КриптоАРМ ГОСТ

Руководство пользователя

Версия выпуска 1.5.2

ОГЛАВЛЕНИЕ

Общие сведения о программном продукте

КриптоАРМ ГОСТ - 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 КриптоАРМ ГОСТ 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.

Функциональность версии 1.5

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; – создание запросов на сертификат; – импорт сертификатов с привязкой к закрытому ключу; – экспорт сертификатов; – удаление сертификатов; – импорт сертификатов из DSS.

[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.

Просмотр и управление журналом операций	– отображение результатов операций, которые производились в приложении.
Работа с файлами в каталоге Документы	– сохранение всех результатов выполнения операций с файлами в централизованном каталоге Документы
Подключение сервисов подписи	– подключение сервисов подписи на базе КриптоПро DSS 2.0 (облачная подпись)

Поддерживаемые криптопровайдеры

Для корректной работы с ГОСТ алгоритмами требуется установка криптопровайдера КриптоПро CSP. В приложении осуществляется поддержка КриптоПро CSP версии 4.0 и выше.

Лицензия на программный продукт

При первой установке приложения активируется временная лицензия сроком на 2 недели. После истечения ознакомительного периода 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 КриптоАРМ ГОСТ можно обратиться в компанию разработчика приложения. Контактные данные компании представлены в разделе Контактная информация.

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 10 64bit/32bit.
- Ubuntu 18.04 64bit.
- Ubuntu 16.04 64bit/32bit.
- CentOS 7.0 64bit/32bit.
- Rosa Fresh 64bit
- Rosa Enterprise Desktop (RED) X3 64bit.
- Гослинукс 6.4 64bit.
- ОС на платформе Альт.
- Ось 2.1 64bit.
- ALT Linux 7.0 Centaurus 64bit/32bit.
- Astra Linux Special Edition, релиз «Смоленск»
- РЕД ОС 7.1 МУРОМ
- Mac OS X 10.10, 10.11, 10.12, 10.13 (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 вместе с приложением устанавливается временный лицензионный ключ сроком на 2 недели.

1. Установка программного продукта

1.1. Установка на платформу Microsoft Windows

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

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

CryptoARM_GOST _vx.x.x_x86.exe (где x.x.x – номер версии) для 32-разрядной ОС).

Откроется мастер установки приложения КриптоАРМ ГОСТ, начальный шаг которого представлен на рис.1.1.1.

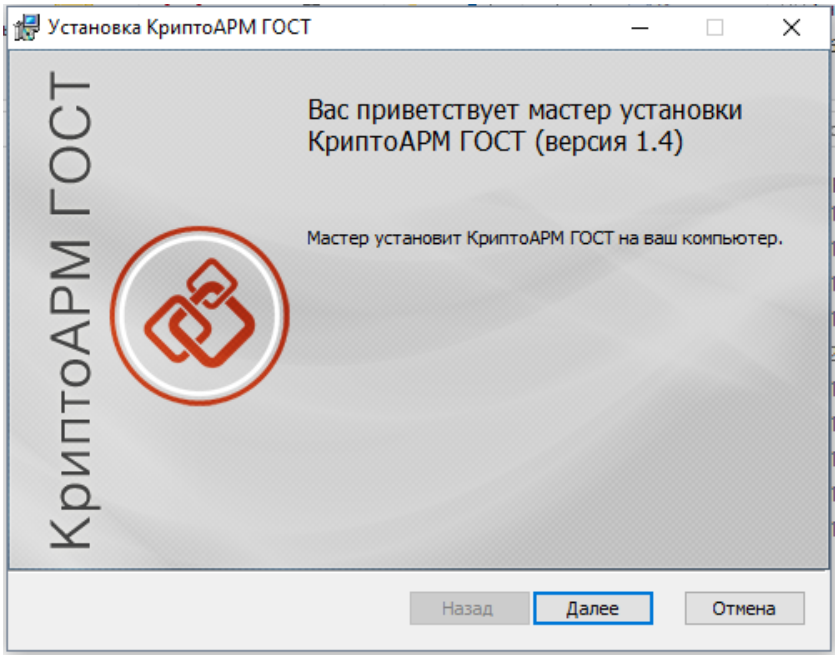


Рис.1.1.1. Начальный шаг мастера установки приложения

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**.

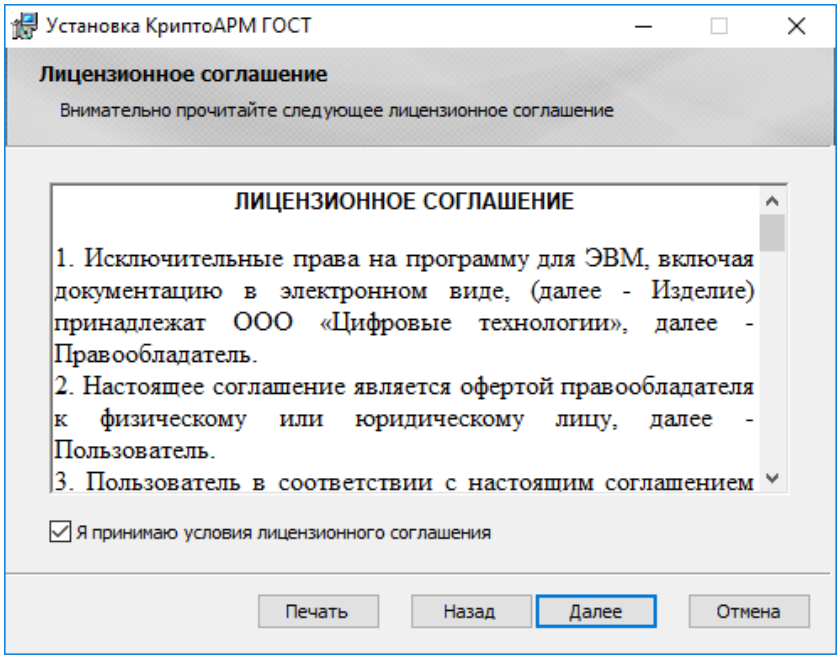


Рис.1.1.2. Условия лицензионного соглашения

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

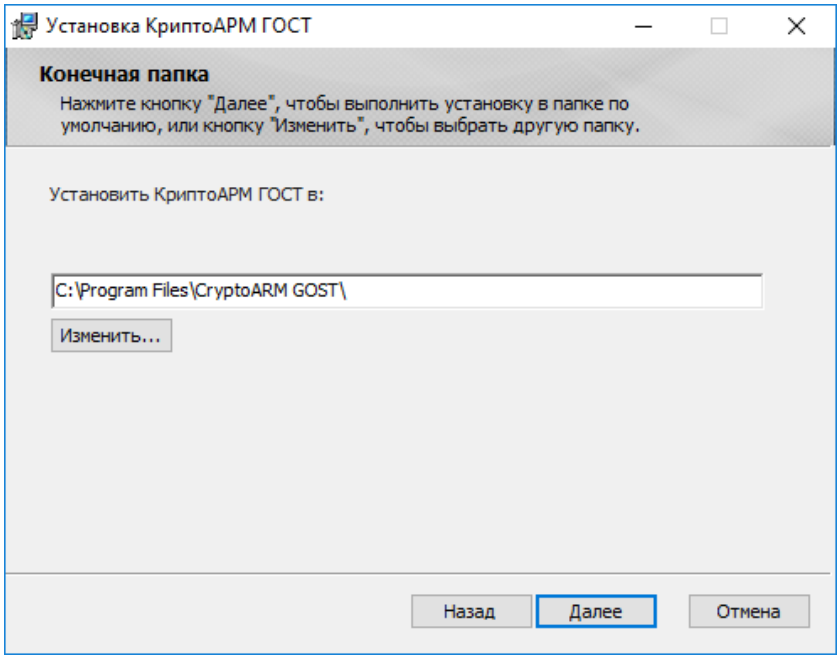


Рис.1.1.3. Выбор каталога установки приложения

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

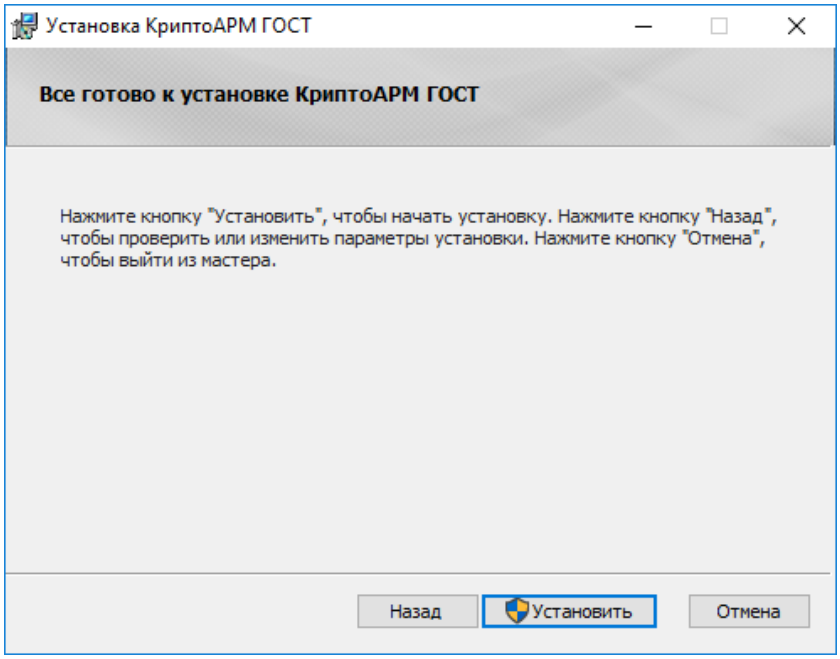


Рис.1.1.4. Выбор каталога установки приложения

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

1.2. Установка на платформу Linux

Установка приложения КриптоАРМ ГОСТ 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/cryptoarm_gost/.

- В режиме графической установки приложения КриптоАРМ ГОСТ запустите на исполнение файл:

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

  CryptoARM_GOST_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 CryptoARM_GOST_vx.x.x_xYY.deb (YY - разрядность ОС) - для ОС, основанных на Debian (Debian/Ubuntu);

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

После установки приложения в меню появится ярлык КриптоАРМ ГОСТ.

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

1.3. Установка на платформу OS X

Дистрибутив приложения КриптоАРМ ГОСТ поставляется в упакованном виде, имеет формат .dmg и представляет собой образ диска, содержащий пакет установки CryptoARM_GOST_vx.x.x_x64.pkg, описание приложения, каталог со скриптами удаления приложения.

Для установки пакета через графический интерфейс откройте двойным щелчком образ диска с дистрибутивом **CryptoARM_GOST_vx.x.x_x64.dmg** (где x.x.x – номер версии).

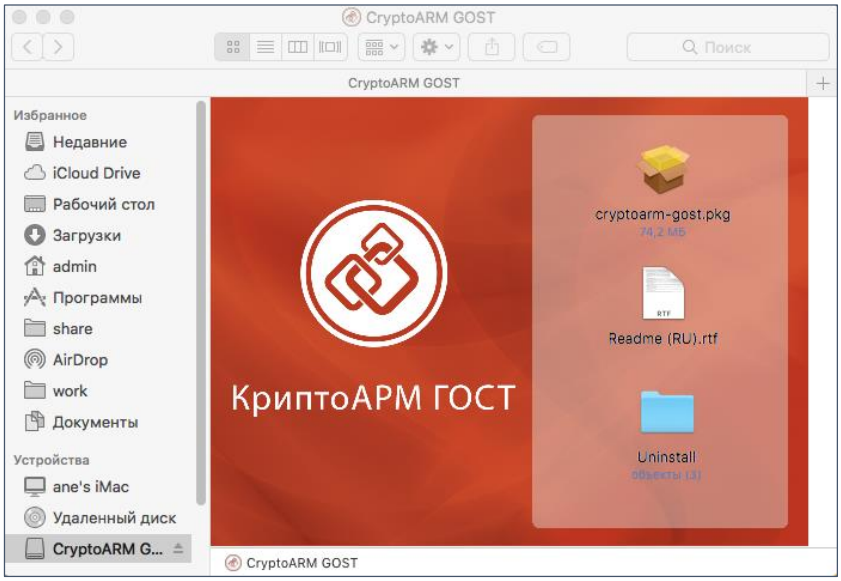


Рис.1.3.1. Состав образа диска

Для установки программы КриптоАРМ ГОСТ запустите на исполнение файл **CryptoARM_GOST_vx.x.x_x64.pkg** (где x.x.x – номер версии). Откроется мастер установки КриптоАРМ ГОСТ. Нажмите кнопку **Продолжить** для продолжения установки. На каждом шаге можно вернуться на предыдущий шаг нажатием **Назад**.

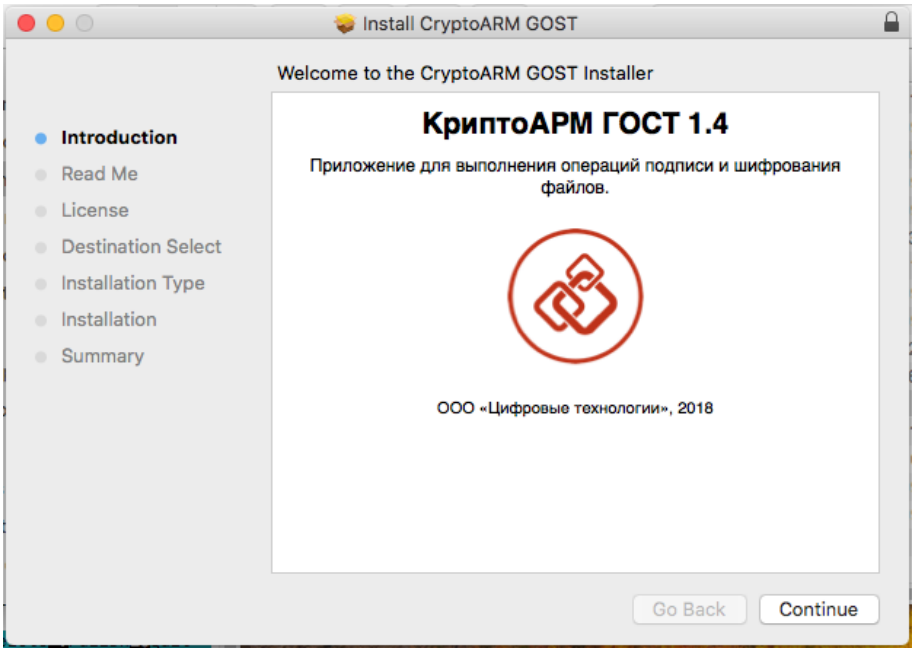


Рис.1.3.2. Начальный шаг мастера установки пакета приложения

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

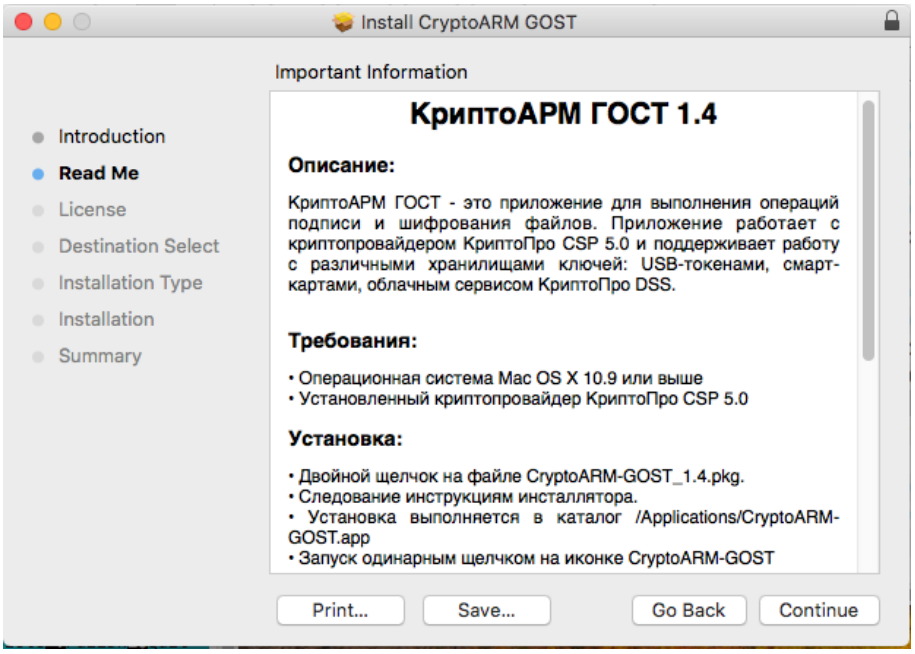


Рис.1.3.3. Просмотр информации о программном продукте

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

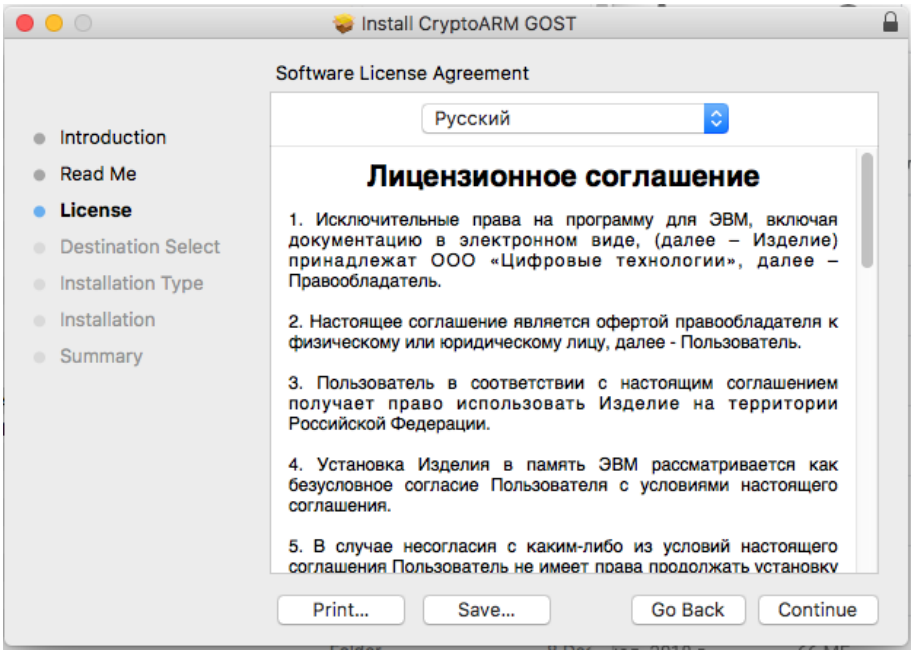


Рис.1.3.4. Просмотр информации о лицензии

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

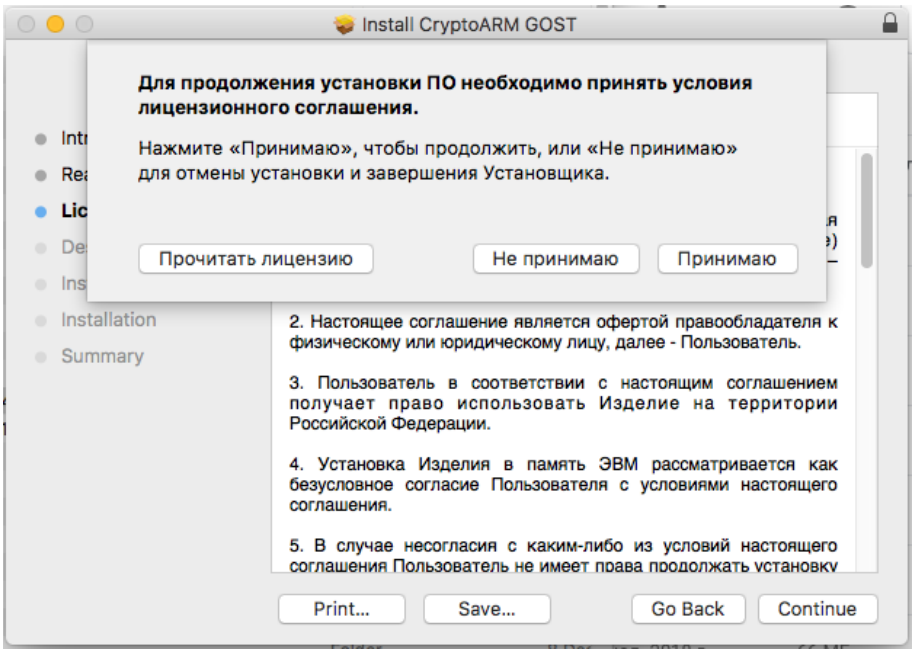


Рис.1.3.5. Соглашение с условиями лицензии

Выберете диск, на который будет установлено приложение (рис.1.3.6) и нажмите **Продолжить**.

Рис.1.3.6. Информация о размещении приложения на жестком диске

На следующем шаге мастера нажмите кнопку **Установить** (рис.1.3.7).

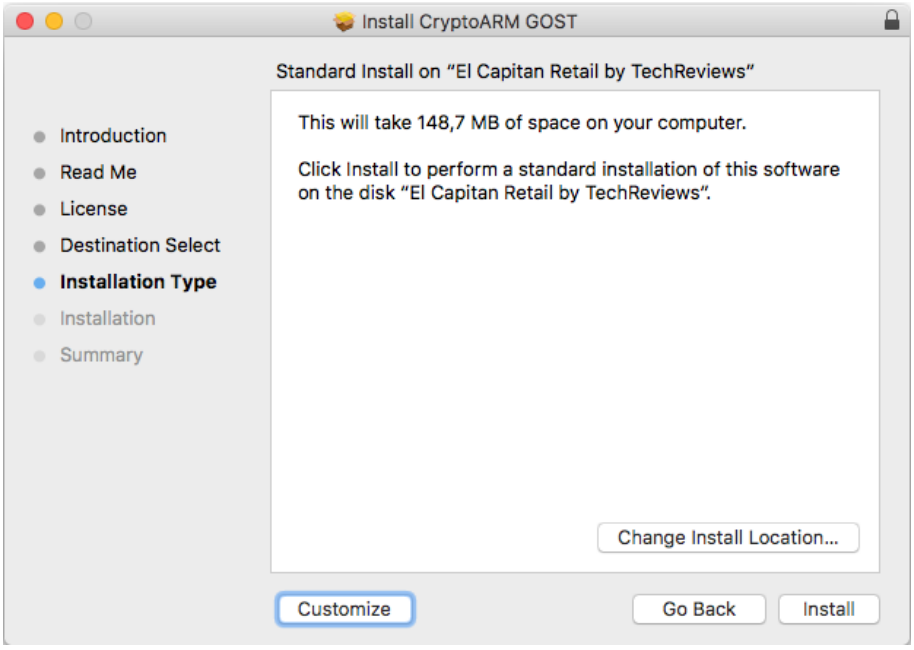


Рис.1.3.7. Подтверждение установки на физический носитель

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

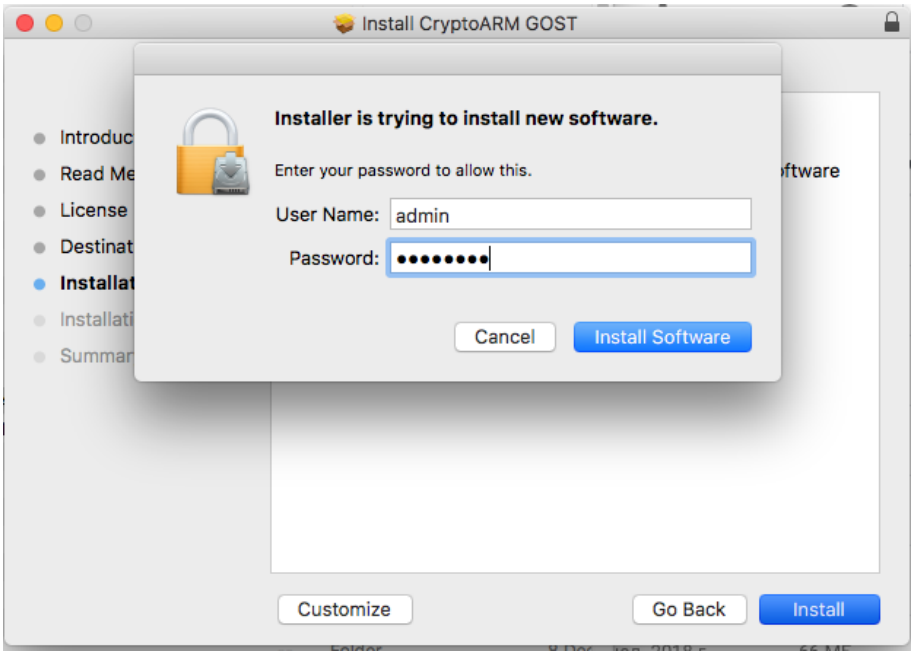


Рис.1.3.8. Информация о размещении приложения на жестком диске

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

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

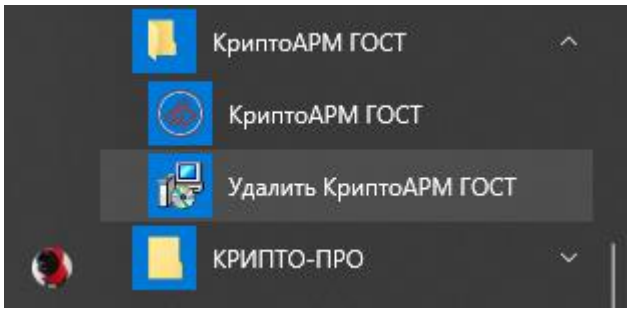
После завершения установки можно отмонтировать диск стандартными средствами ОС.

2. Удаление программного продукта

2.1. Удаление приложения на платформе MS Windows

Удалить приложение КриптоАРМ ГОСТ 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 КриптоАРМ ГОСТ, 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 КриптоАРМ ГОСТ 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, КриптоАРМ ГОСТ**. В списке найдите **Удалить КриптоАРМ ГОСТ** (Uninstall КриптоАРМ ГОСТ) (см. рисунок ниже) и активизируйте команду.



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

2.2. Удаление приложения на платформе Linux

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

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

  sudo dpkg -P cryptoarm-gost - для ОС, основанных на Debian (Debian/Ubuntu);

  sudo rpm -e cryptoarm-gost - для ОС, основанных на RPM;

После выполнения команды приложение будет удалено из операционной системы.

2.3. Удаление приложения на платформе OS X

Для удаления пакета через графический интерфейс откройте двойным щелчком образ диска с дистрибутивом (dmg), а затем двойным щелчком по каталогу **Uninstall**, содержащему скрипты для удаления приложения (рис. 2.3.1). Для удаления приложения из каталога Application запускается **скрипт unistall_cryptoarm_gost**. Для полного удаления приложения (настроек, кэша, лицензий) используется скрипт **full_uninstall_cryptoarm_gost**. Затем ну жно ввести пароль администратора.

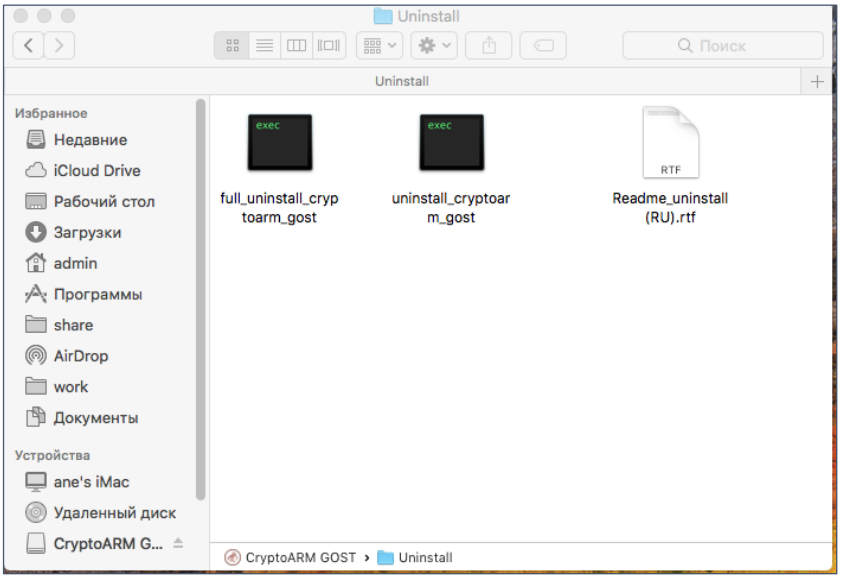


Рис.2.3.1. Каталог скриптов удаления приложения

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

3. Установка лицензии на программный продукт

Для полноценной работы приложения КриптоАРМ ГОСТ необходима установка лицензионного ключа. Лицензионный ключ представляет собой файл, который необходимо расположить в специально созданном каталоге приложения.

Существуют два вида лицензий – постоянная и временная. Временная лицензия предоставляется с ограниченным сроком действия. Для приобретения постоянной лицензии можно обратиться в компанию разработчика.

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

3.1.1. Установка постоянной лицензии

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 разделе сведений о лицензии на КриптоАРМ ГОСТ. 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 установки лицензии. После установки лицензии желательно перезагрузить приложение.

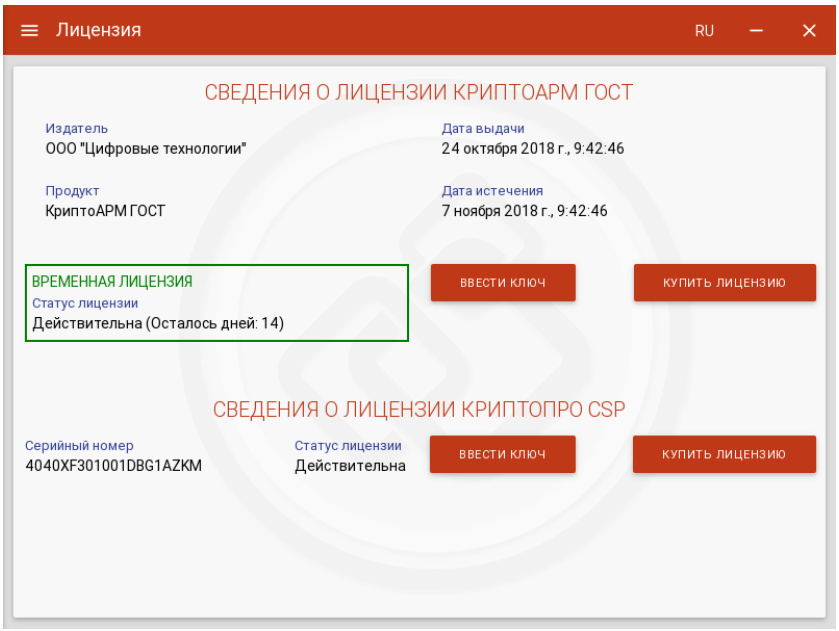


Рис.3.1.1. Страница ввода лицензионного ключа на программный продукт

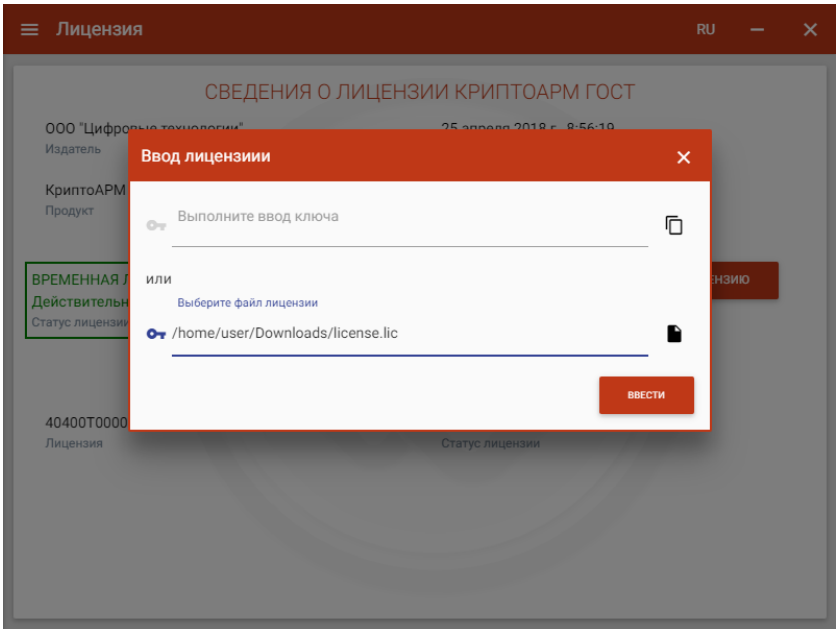


Рис.3.1.2. Диалоговое окно с выбором варианта ввода лицензионного ключа

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.

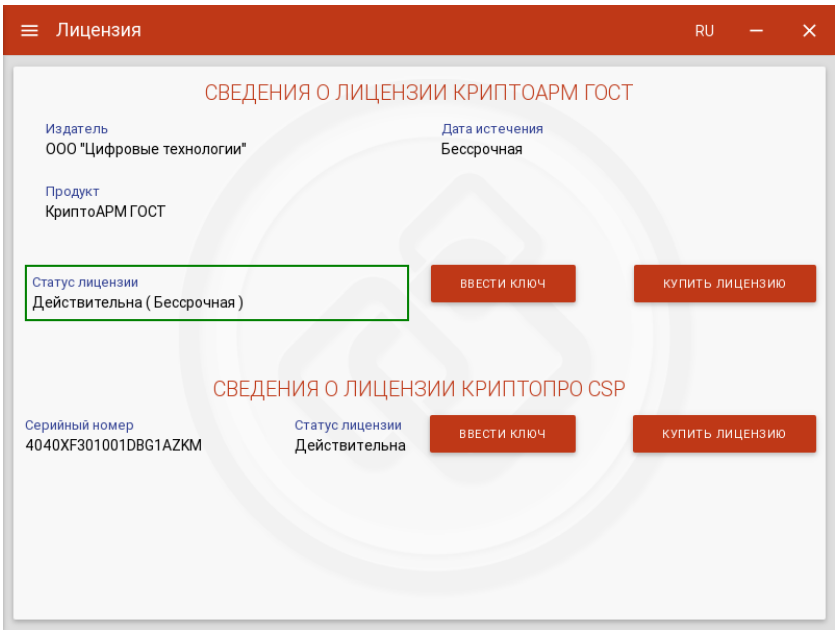


Рис. 3.1.3 Сведения о лицензии

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, выполняющего копирование файла лицензии license.lic в каталог установки:

- Под платформой Windows – каталог

  C:\Users\<имя пользователя>\AppData\Local\Trusted\CryptoARM GOST.

- Под платформой Linux – каталог ./etc/Trusted/CryptoARM GOST/.

Примечание. Для последующей установки лицензии пользователями каталог КриптоАРМ ГОСТ 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».

4.1. Установка криптопровайдера на платформу MS Windows

Для установки КриптоПро CSP 5.0 на платформу Windows можно воспользоваться инструкцией установки КриптоПро CSP более ранних версий, доступной по адресу https://cryptostore.ru/article/instruktsii/kak_ustanovit_criptopro_csp/ .

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-5.0.10874-5.noarch.rpm**

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

alien -kci <файл_пакета>
Например, **alien -kci ./lsb-cprocsp-base-5.0.10874-5.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 или JaCarta 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 библиотеки и пакеты ccid, pcscd и pcsc-lite

Пакеты и драйвера для работы с ключевыми носителями устанавливаются с помощью команд:

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

Для ключевого носителя Рутокен:

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

Для ключевого носителя JaCarta:

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

Для работы с сертификатами, находящимися в «облаке», в систему надо установить следующие пакеты:

sudo alien -kci cprocsp-cptools-gtk- -<...>.deb
sudo alien -kci cprocsp-rdr-cloud-<...>.deb
sudo alien -kci cprocsp-rdr-cloud-gtk-<...>.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.

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 .

4.4. Установка лицензии на программный продукт КриптоПРО CSP

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).

Установка лицензионного ключа может производиться как через пользовательский интерфейс приложения КриптоАРМ ГОСТ, так и с помощью консольных команд для ОС linux и MacOS.

4.4.1. 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.4.4.1 нажать на кнопку **Ввести ключ** в разделе сведений о лицензии на КриптоПРО CSP. В результате должно появиться всплывающее окно ввода лицензии копированием содержимого файла лицензии в текстовое (рис. 4.4.2).

Примечание. При установке лицензии будут запрошены права администратора (Root) на доступ к каталогу установки лицензии.

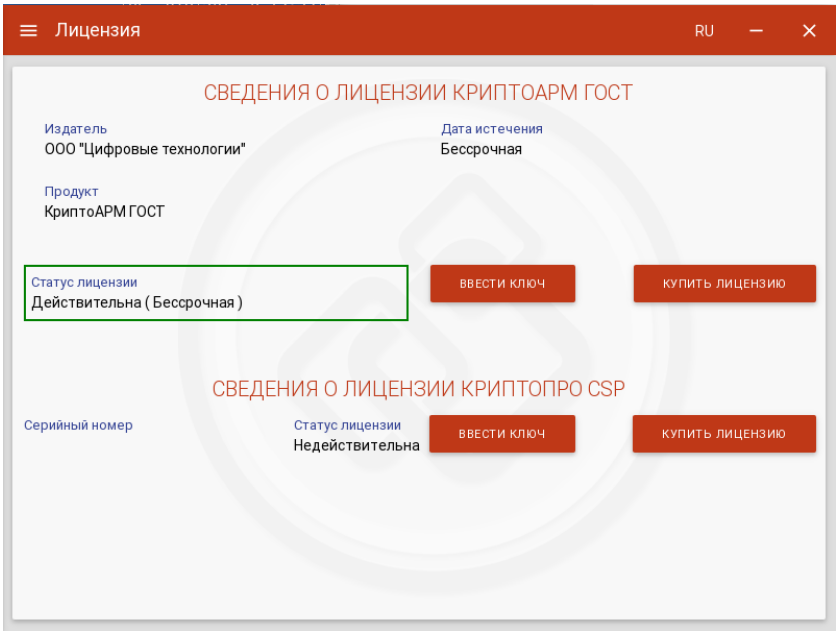


Рис.4.4.1. Страница ввода лицензионного ключа на КриптоПРО CSP

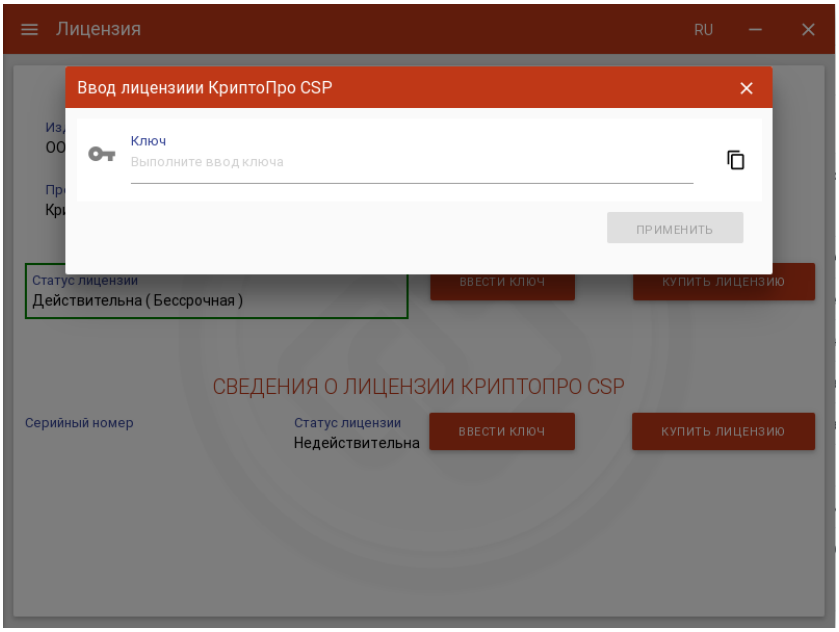


Рис. 4.4.2. Диалоговое окно ввода лицензионного ключа

Если установка лицензионного ключа прошла успешно, то появляется всплывающее сообщение с информацией об этом. На странице **Лицензия** отображается серийный номер и статус лицензии.

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

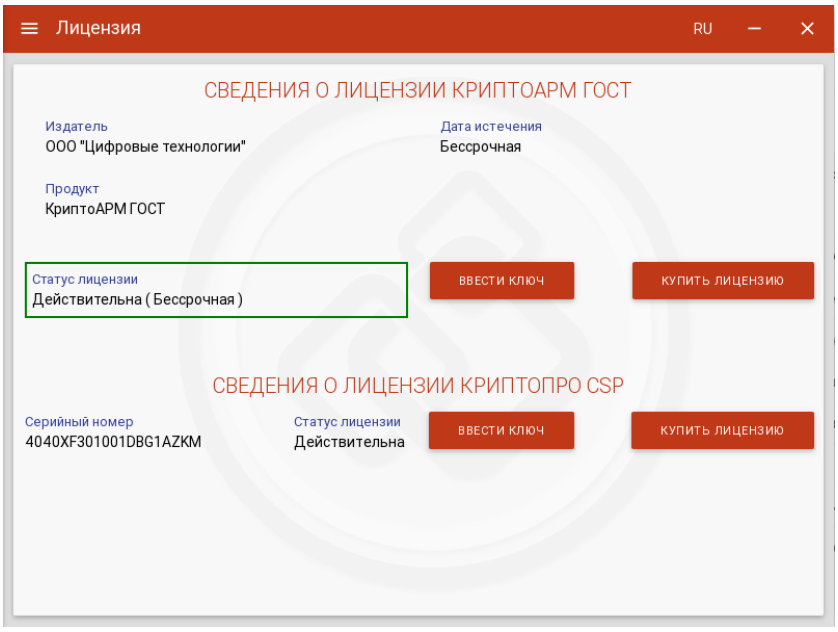


Рис. 4.4.3 Сведения о лицензии

4.4.2. Установка лицензии через командную строку

Установка лицензии на КриптоПРО CSP осуществляется от имени пользователя, имеющего права администратора: под учётной записью root или с использованием команды sudo.

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>

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.

Это можно сделать через программный интерфейс приложения КриптоАРМ ГОСТ или с помощью команд программы КриптоПРО CSP. Установка сертификата с токена через КриптоАРМ ГОСТ описана в разделе **«Установка сертификата из ключевого контейнера».**

Установка с помощью программы КриптоПРО CSP 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.

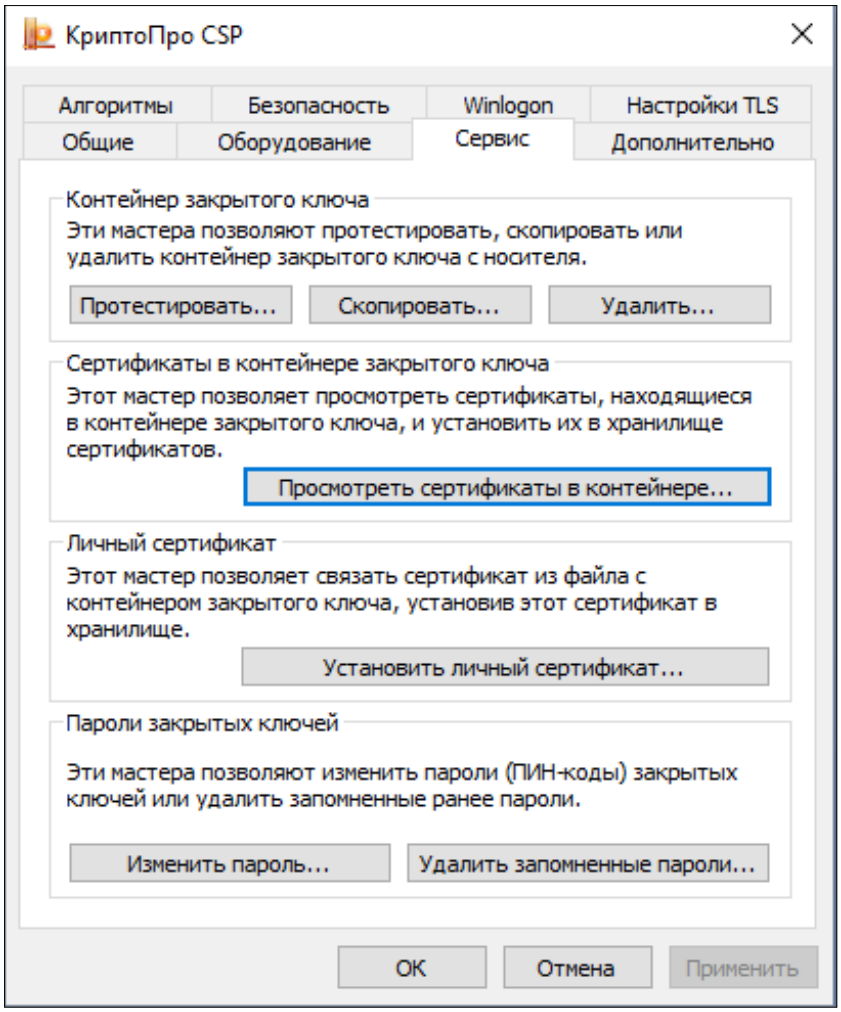


Рис.6.1.1. Диалог настроек криптопровайдера. Вкладка Сервис

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

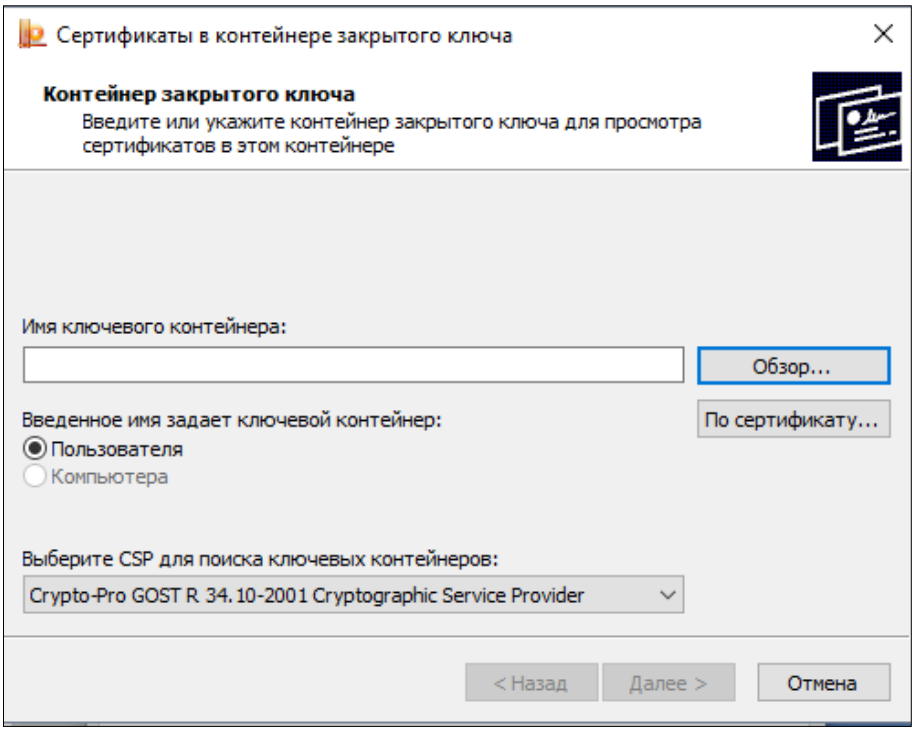


Рис.6.1.2. Диалог поиска ключевого контейнера

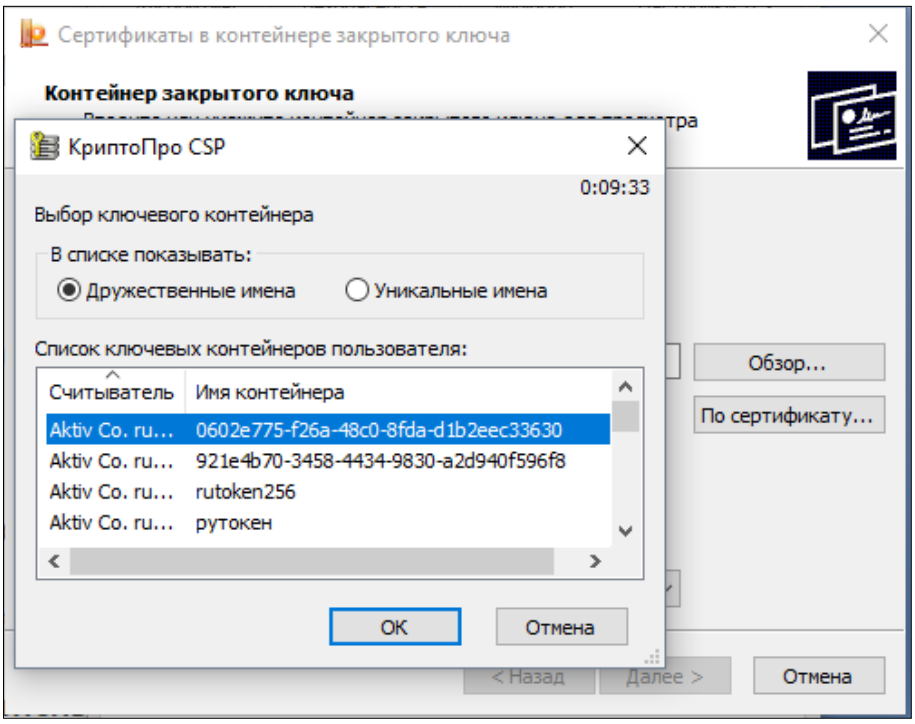


Рис.6.1.3. Выбор ключевого контейнера

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

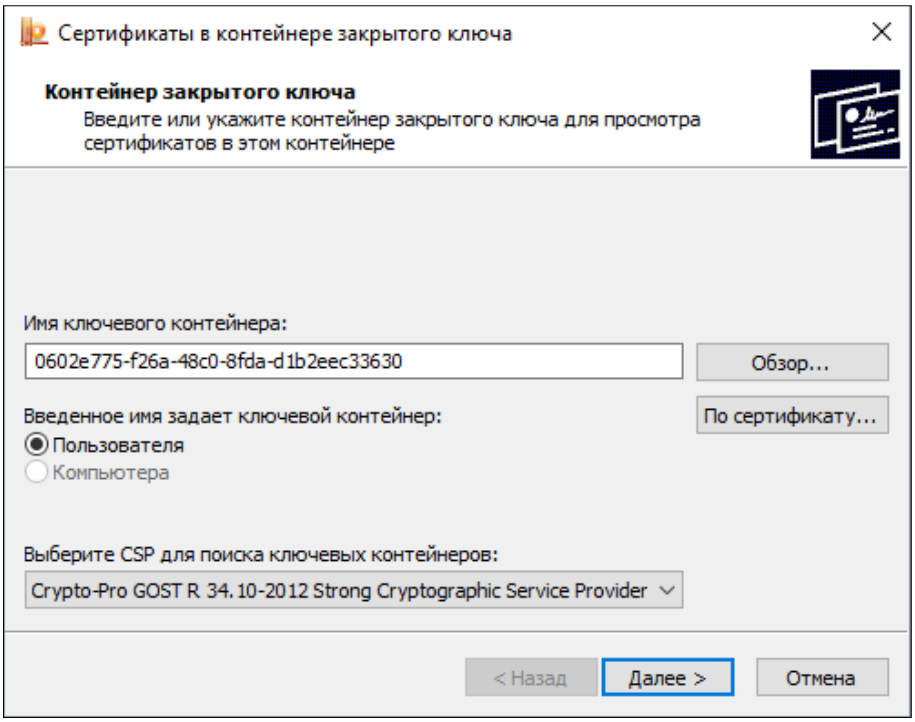


Рис.6.1.4. Просмотр содержимого контейнера

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**.

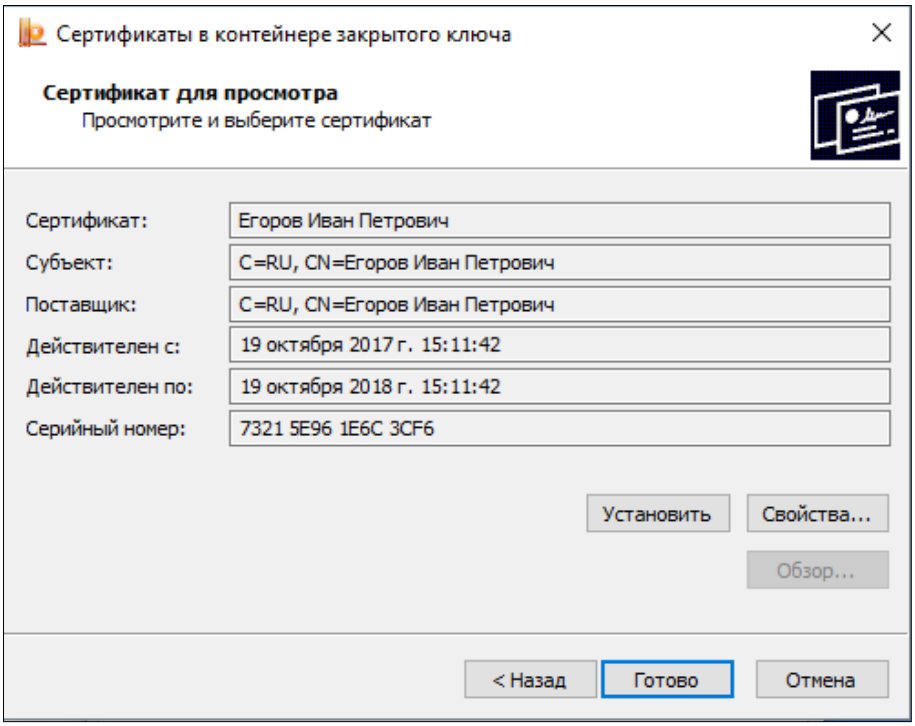


Рис.6.1.5. Сведения о сертификате внутри контейнера

После успешной установки сертификата можно открыть приложение КриптоАРМ ГОСТ 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 КриптоАРМ ГОСТ 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 КриптоАРМ ГОСТ, 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.

Установить сертификаты можно через программный интерфейс приложения КриптоАРМ ГОСТ или с помощью команд программы КриптоПРО CSP. Установка сертификата с через КриптоАРМ ГОСТ описана в пункте **«**Управление сертификатами и ключами**»** в разделе «Импорт сертификата».

Установка корневого, промежуточных и списка отозванных сертификатов с помощью программы КриптоПРО CSP для Linux и OS X 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 КриптоАРМ ГОСТ начинается со стартовой страницы (рис.8.1.1), на которой расположены кнопки перехода к мастерам приложения.

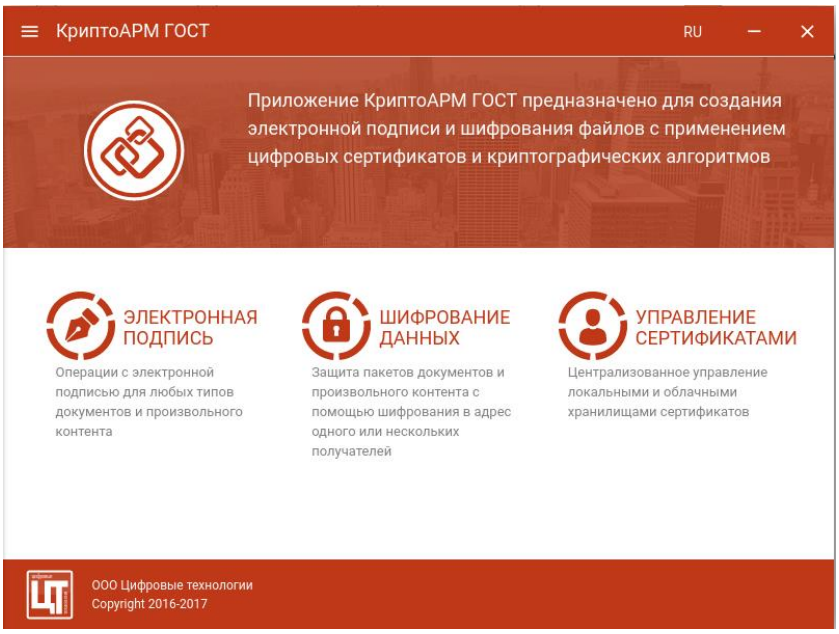


Рис.8.1.1. Главное окно приложения

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

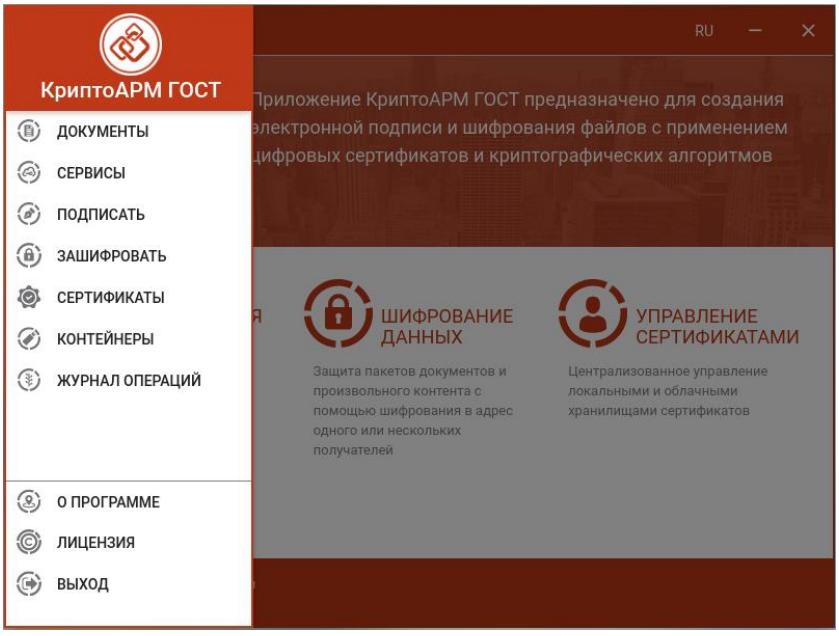


Рис.7.1.2. Основное меню приложения

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 файлы журнала операций и каталог с документами. В файле **settings.json** сохраняются пользовательские настройки.

8.2. Диагностика неполадок при запуске приложения

При обнаружении проблем, затрудняющих дальнейшую работу приложения КриптоАРМ ГОСТ, запускается мастер диагностики приложения. В мастере подробно описываются возникшие неполадки и способы их решения.

8.2.1. Отсутствует СКЗИ КриптоПро CSP

Приложение КриптоАРМ ГОСТ не работает без установленного в системе СКЗИ КриптоПро CSP 5.0. В таком случае при запуске приложения будет предупреждающее сообщение (рис. 8.2.1)

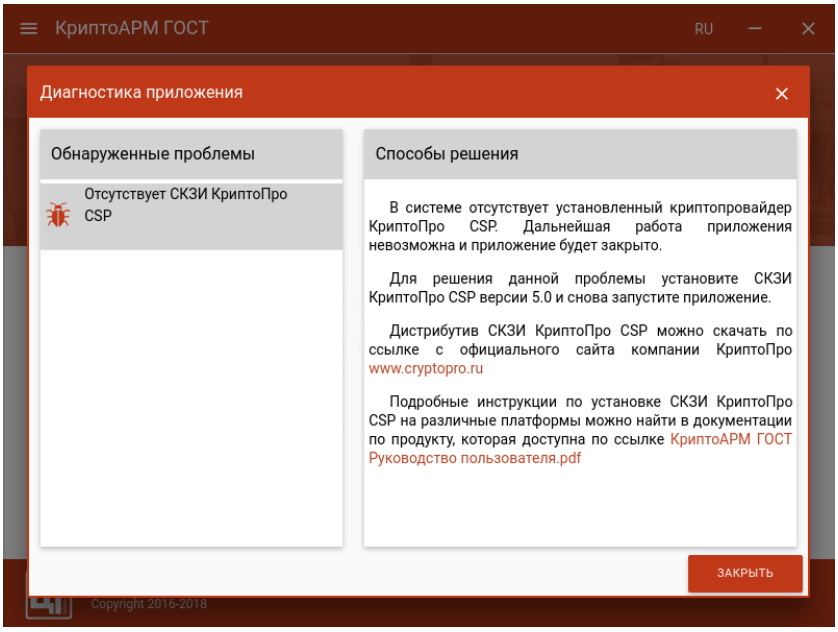


Рис. 8.2.1 Сообщение об отсутствии СКЗИ КриптоПро CSP

Дальнейшая работа приложения невозможна. Приложение можно только закрыть.

Инструкция по установке СКЗИ КриптоПро CSP описана в п. 4 «Установка криптопровайдера КриптоПро CSP».

8.2.2. Отсутствует лицензия на КриптоАРМ ГОСТ

Без установленной лицензии на программный продукт КриптоАРМ ГОСТ при запуске приложения возникает предупреждающее сообщение (рис. 8.2.2).

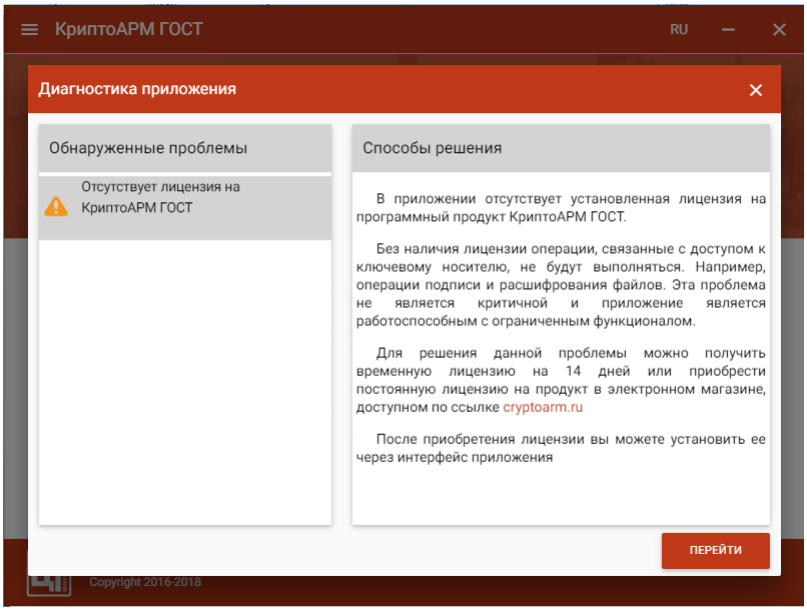


Рис. 8.2.2 Сообщение об отсутствии лицензии на КриптоАРМ ГОСТ

По кнопке **Перейти** происходит переход на вкладку **Лицензия**, где можно установить лицензию.

При закрытии мастера диагностики приложение остается работоспособным, но с ограниченным функционалом. Без лицензии не будут выполняться операции, связанные с доступом к закрытому ключу (например, подпись и расшифрование).

Инструкция по установке лицензии в приложении КриптоАРМ ГОСТ описана в п. 3 «Установка лицензии на программный продукт» данного руководства.

8.2.3. Не обнаружены сертификаты с привязкой к ключевому контейнеру

При отсутствии в личном хранилище сертификатов, с привязкой к закрытому ключу, при запуске приложения возникает предупреждающее сообщение (рис. 8.2.3)

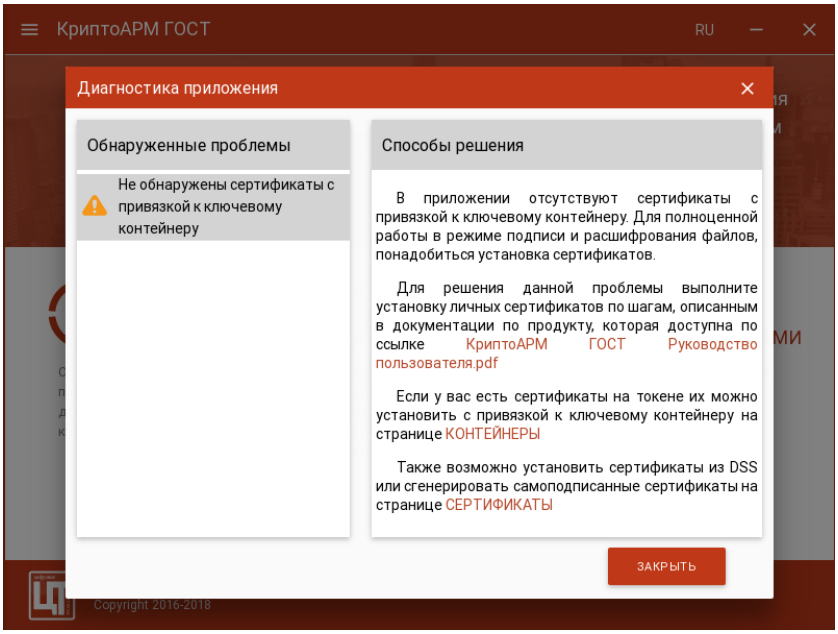


Рис. 8.2.3 Сообщение об отсутствии сертификатов с привязкой к закрытому ключу

Добавить личный сертификат можно несколькими способами:

- установить со стороннего носителя;
- установить из DSS (только для КриптоПРО CSP 5);
- сгенерировать запрос на сертификат и установить полученный сертификат;
- сгенерировать самоподписанный сертификат.

Установить личный сертификат со стороннего носителя можно одним из следующих способов:

1) Используя вкладку **Контейнеры**, если сертификат и закрытый ключ находятся на ключевом носителе (Рутокен, JaCarta). Для перехода на вкладку нужно вставить в компьютер ключевой носитель и нажать кнопку **Перейти**. Инструкция по установке сертификата из контейнера описана в п. 8.11 «Установка сертификата из ключевого контейнера».
2) Используя инструкцию в п. «Перенос контейнера закрытого ключа под требуемую операционную систему», если сертификат и контейнер расположены в другой операционной системе
3) Используя инструкцию из п. «Установка сертификата с токена с сохранением привязки к закрытому ключу», если сертификат и закрытый ключ находятся на ключевом носителе (Рутокен, JaCarta), но по каким-то причинам не удалось установить сертификат на вкладке **Контейнеры.**

Установить сертификат из DSS можно, перейдя по ссылке на страницу **Сертификаты**, выбрав пункт контекстного меню «Импорт из DSS».

Сгенерировать запрос на сертификат или создать самоподписанный сертификат можно, перейдя по ссылке в окне диагностики приложения на вкладку **Сертификаты.** Подробнее описано в пункте «Управление сертификатами и ключами» в разделе «Создание запроса на сертификат» и «Создание самоподписанного сертификата»

8.2.4. Не загружен модуль Trusted Crypto

Приложение КриптоАРМ ГОСТ не работает без модуля Trusted Crypto. В таком случае при запуске приложения будет предупреждающее сообщение (рис. 8.2.4)

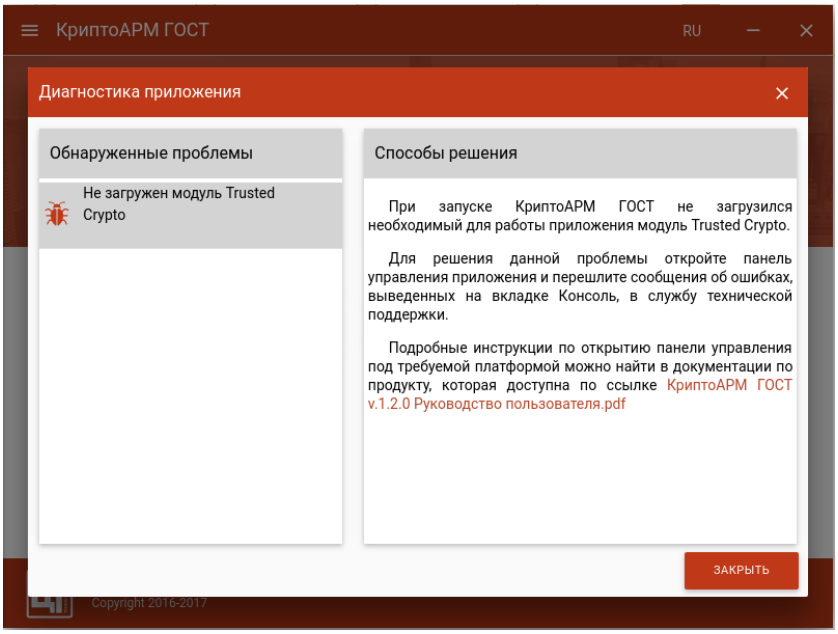


Рис. 8.2.4 Сообщение об ошибке в модуле Trusted Crypto

Дальнейшая работа приложения невозможна. Приложение можно только закрыть.

Для решения данной проблемы необходимо запустить приложение в консольном режиме, скопировать информацию об ошибке и связаться со специалистами технической поддержки продукта КриптоАРМ ГОСТ. Инструкция по включению консольного режима описана в п. 9 «Включение режима логирования и консоль управления» данного руководства.

8.3. Создание электронной подписи

Представление мастера подписания/проверки подписи (рис. 8.3.1) 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.

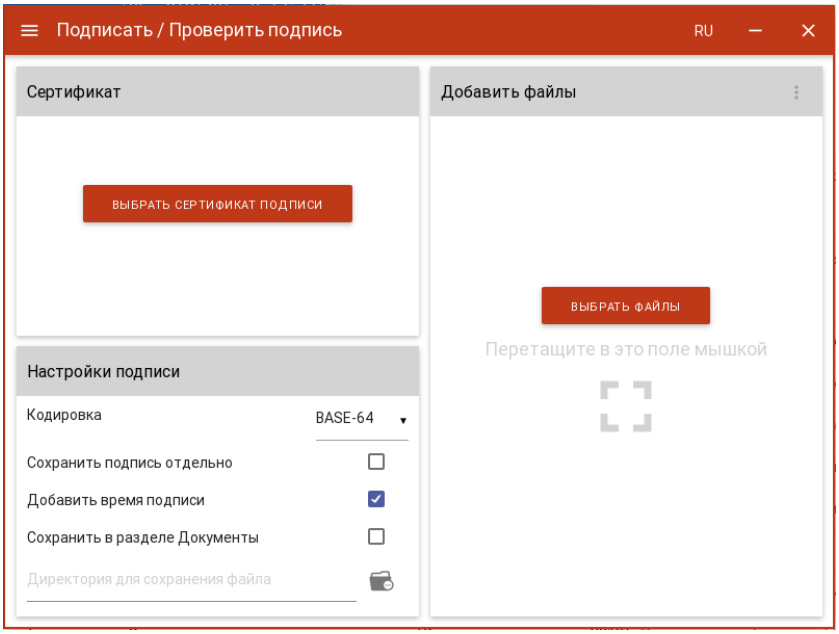


Рис.8.3.1. Страница создания/проверки электронной подписи файлов

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;
- **Сохранить в разделе Документы** – при установленном флажке результат операции сохраняется в каталог Documents, расположенный в папке пользователя в каталоге /Trusted/CryptoARM GOST/. Если флаг не установлен и не выбрана директория для сохранения файла, то файл сохраняется рядом с исходным файлом. При выбранной директории файл сохраняется в данной директории.

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.8.3.2) 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.

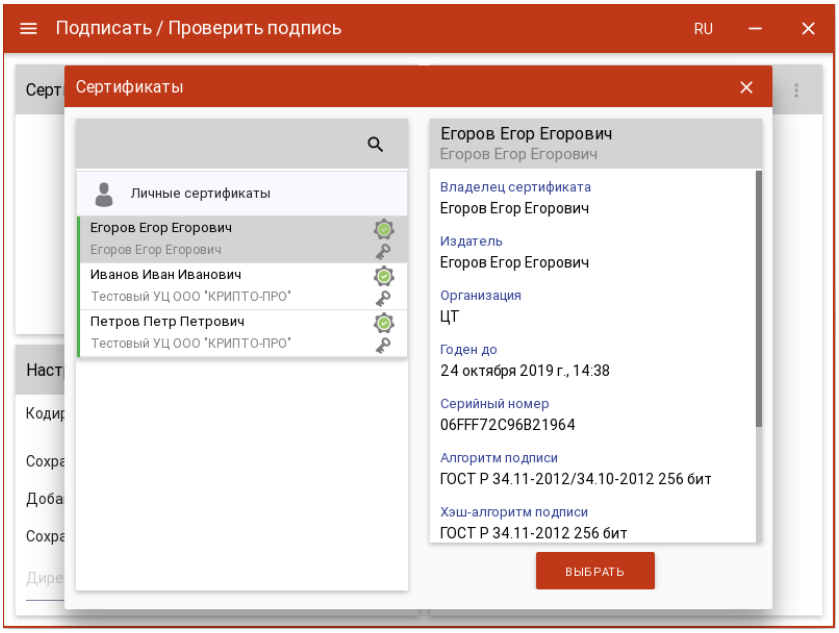


Рис.8.3.2. Диалоговое окно выбора сертификата подписчика

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. 8.3.3) 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.

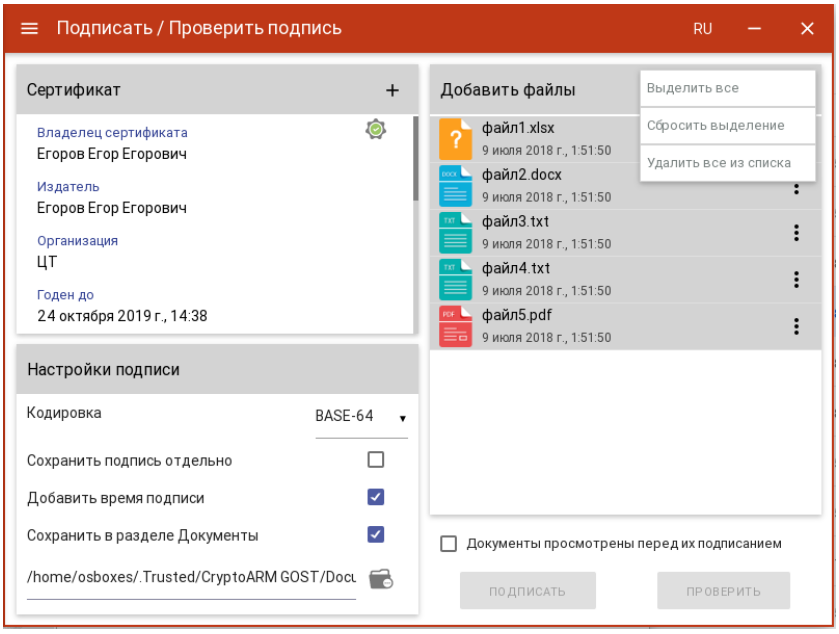


Рис. 8.3.3. Контекстное меню управления списком файлов

В списке отображается наименование файла с расширением и дата его создания. Для каждого элемента списка доступно контекстное меню (рис. 8.3.4), 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.

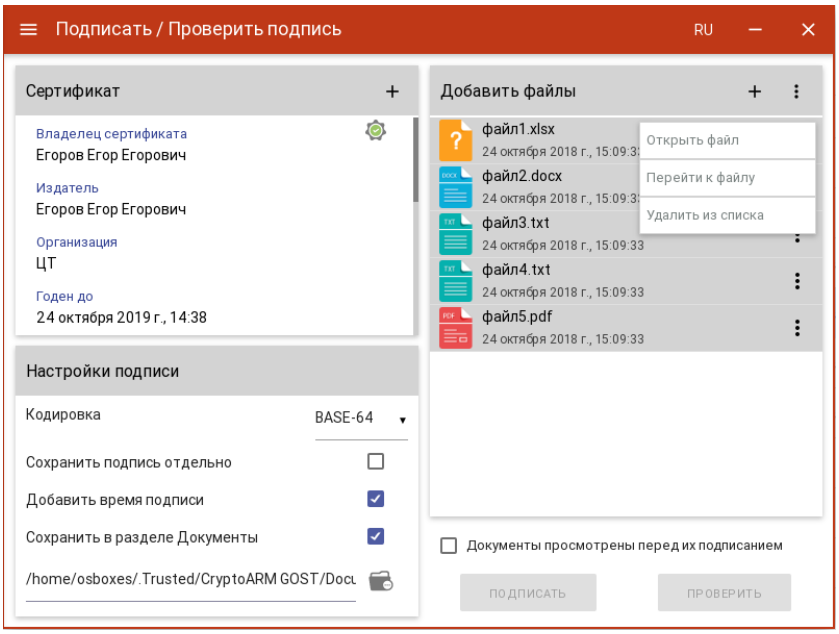


Рис. 8.3.4. Контекстное меню элемента списка (файла)

Подпись файлов. При условии выбора сертификата подписчика, файлов для подписи и установленного флага, что документы просмотрены перед подписанием, в мастере становится доступной кнопка **Подписать** (рис.8.3.5).

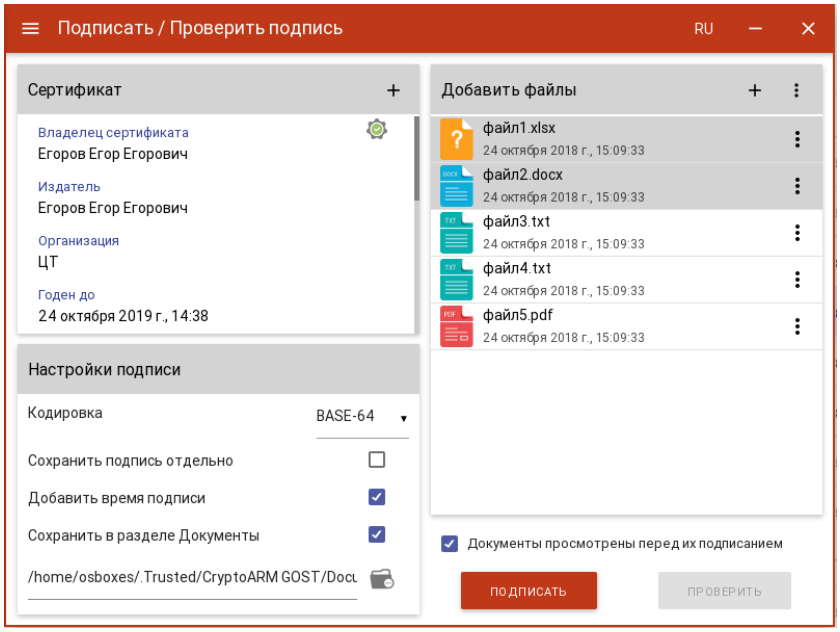


Рис.8.3.5. Подпись файлов

Нажатие на кнопку **Подписать** запускает процесс подписи. Выбранные файлы подписываются по очереди. Для подписанных файлов меняется иконка, наименование, дата создания. Сразу происходит проверка подписи, результат которой отображается в виде индикатора на иконке подписанного файла.

Если в настройках стоит флаг «Сохранить в разделе Документы», то подписанные файлы они сохраняются в каталог /Trusted/CryptoARM GOST/Documents в папке пользователя, и доступны в пункте меню **Документы**.

Для подписанных файлов становятся доступны кнопки **Проверить** и **Снять** проверки и снятия подписи (рис. 8.3.6).

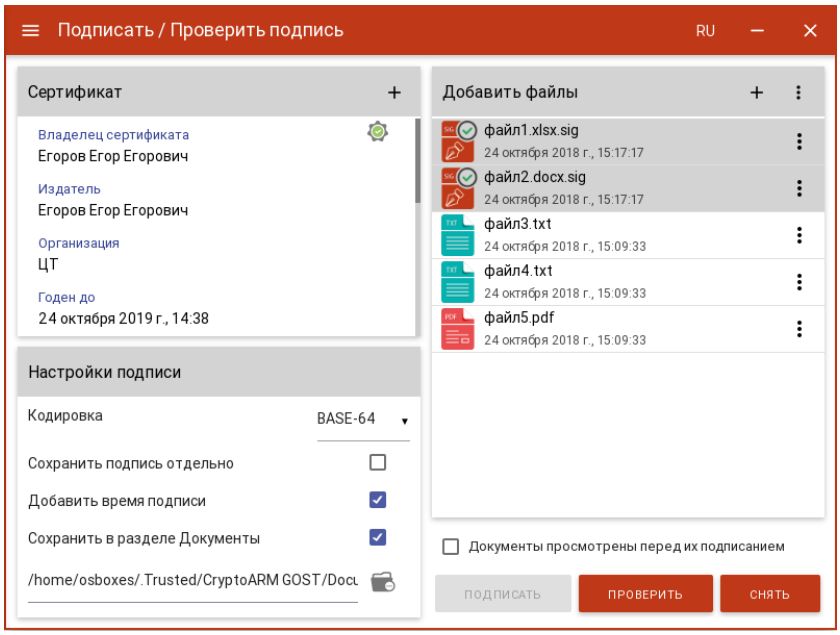


Рис.8.3.6. Подписанные файлы

8.4. Проверка электронной подписи

Для проверки подписи достаточно выбрать проверяемые файлы - файлы с расширением **.sig**, которые содержат электронную подпись. 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 на иконке для каждого файла (рис. 8.4.1): зеленый - подпись действительна; красный - подпись недействительна.

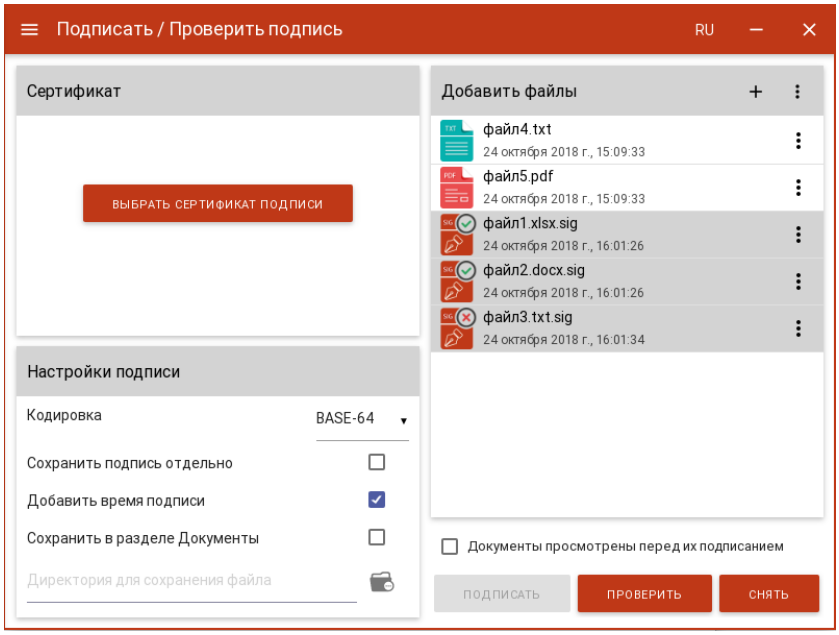


Рис. 8.4.1. Результат проверки подписи файлов

При выделении одного подписанного файла в левой области отображается информация о подписи, как показано на рис. 8.4.2.

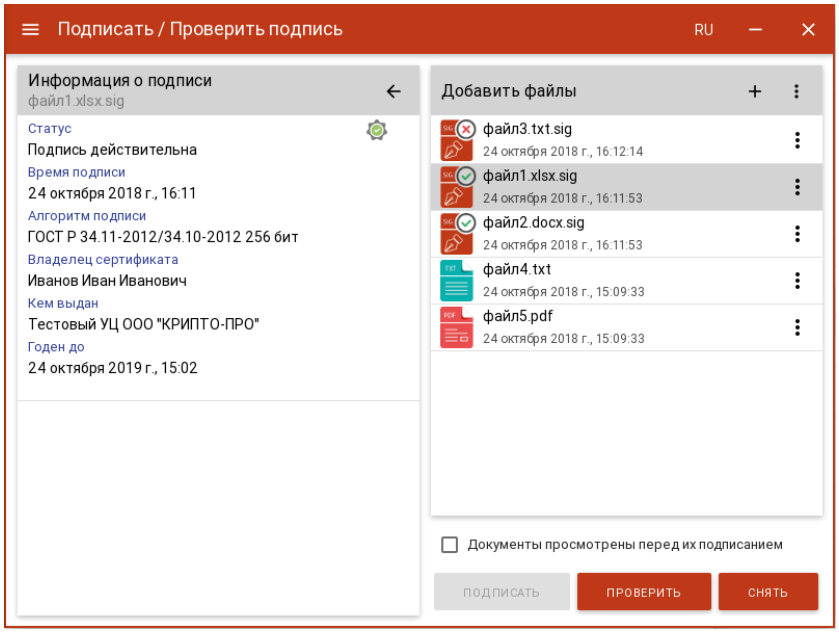


Рис. 8.4.2. Отображение информации о подписи

При нажатии на область с информацией о подписи открывается информация о цепочке сертификации (цепочке доверия) и сведения о выбранном сертификате в этой цепочке (рис.8.4.3).

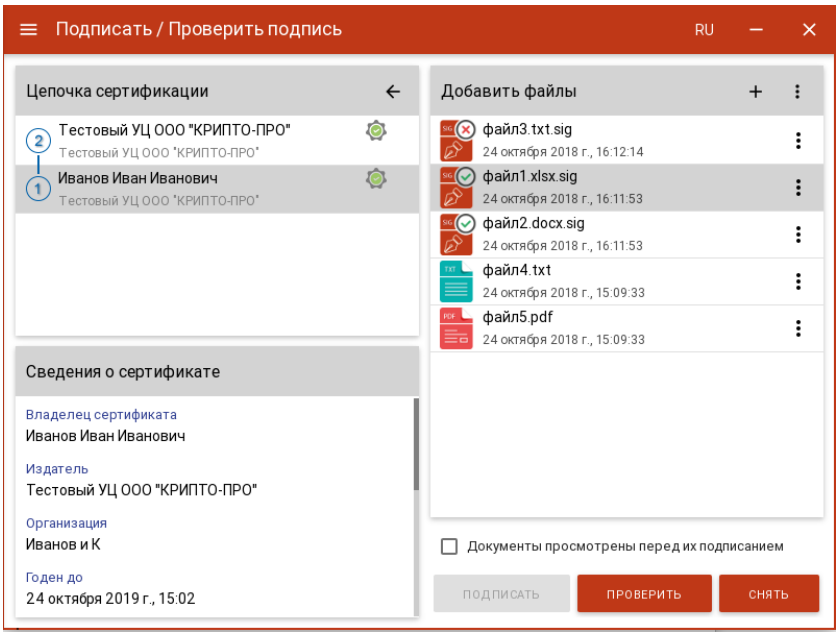


Рис. 8.4.3. Отображение цепочки сертификации подписанного файла

8.5. Снятие электронной подписи

Для снятия подписи достаточно выбрать подписанные файлы - файлы с расширением **.sig**, которые содержат электронную подпись и нажать на кнопку **Снять** (рис. 8.5.1).

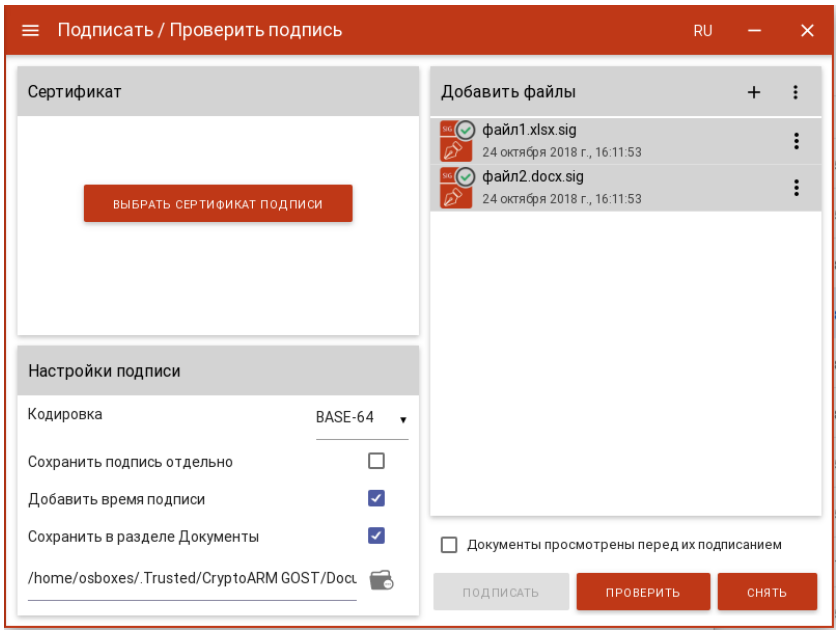


Рис. 8.5.1. Выделенные файлы для снятия подписи

При снятии подписи у файлов меняется иконка, наименование, дата создания. Если в настройках подписи установлен флаг «Сохранить в разделе Документы», то файлы сохраняются в каталог с документами в папке пользователя /.Truste/CryptoARM GOST/Documents/ (рис. 8.5.2).

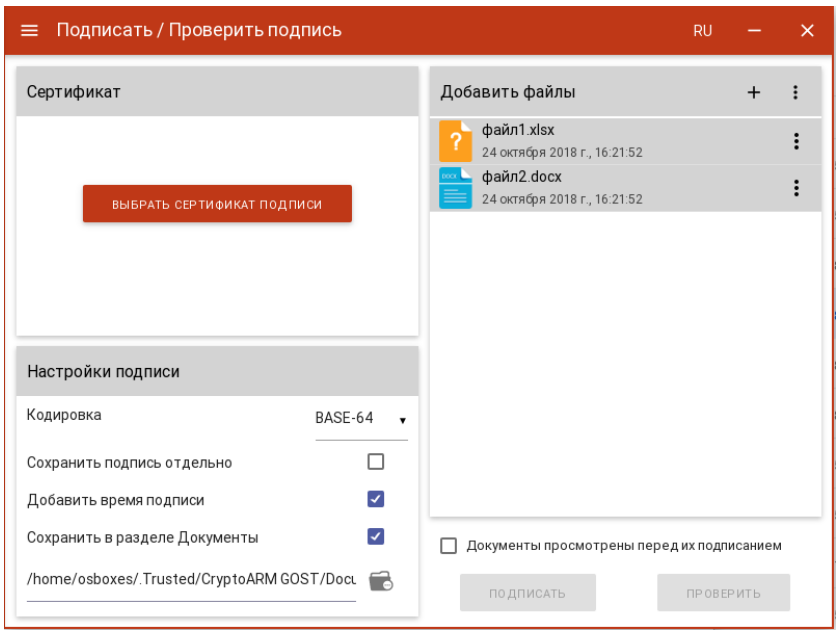


Рис. 8.5.2. Результат снятия подписи с файлов

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

8.6. Добавление подписи

Приложение КриптоАРМ ГОСТ позволяет добавлять электронные подписи к уже подписанному файлу. Добавление подписи осуществляется по нажатию на кнопку **Подписать** (рис. 8.6.1), при условии, что выбран сертификат подписчика, файлы, содержащие электронную подпись (файлы с расширением **.sig)** и установлен флаг, что документы просмотрены перед подписанием .

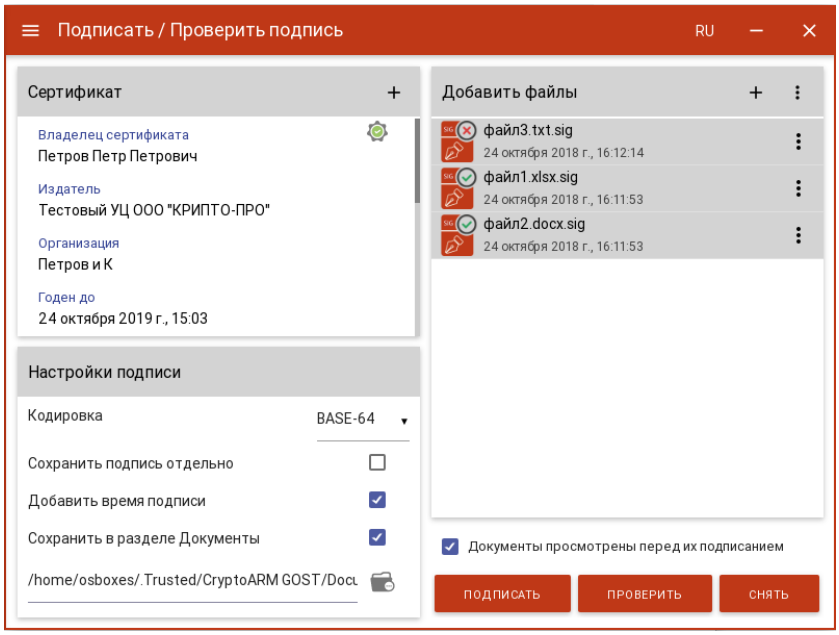


Рис. 8.6.1. Добавление электронной подписи к уже подписанным файлам

Для всех добавленных подписей настройки подписи используются по-умолчанию, как для первой подписи (рис. 8.6.2).

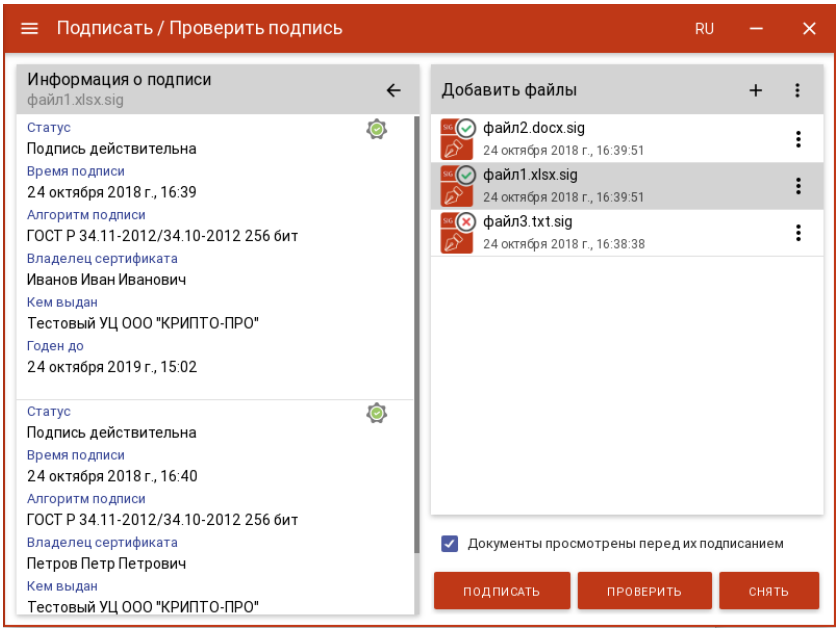


Рис. 8.6.2. Отображение информации о нескольких подписях файла

8.7. Шифрование файлов

Представление мастера шифрования/расшифрования (рис. 8.7.1) имеет три функциональных элемента: слева располагаются области выбора сертификатов получателей, настройки шифрования, справа - область формирования списка файлов для выполнения операций.

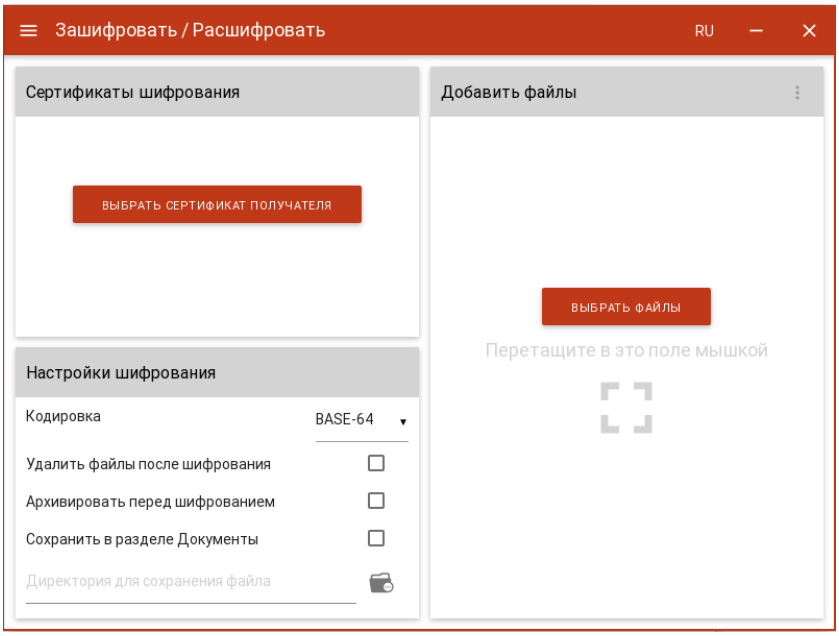


Рис. 8.7.1. Страница шифрования / расшифрования файлов

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.

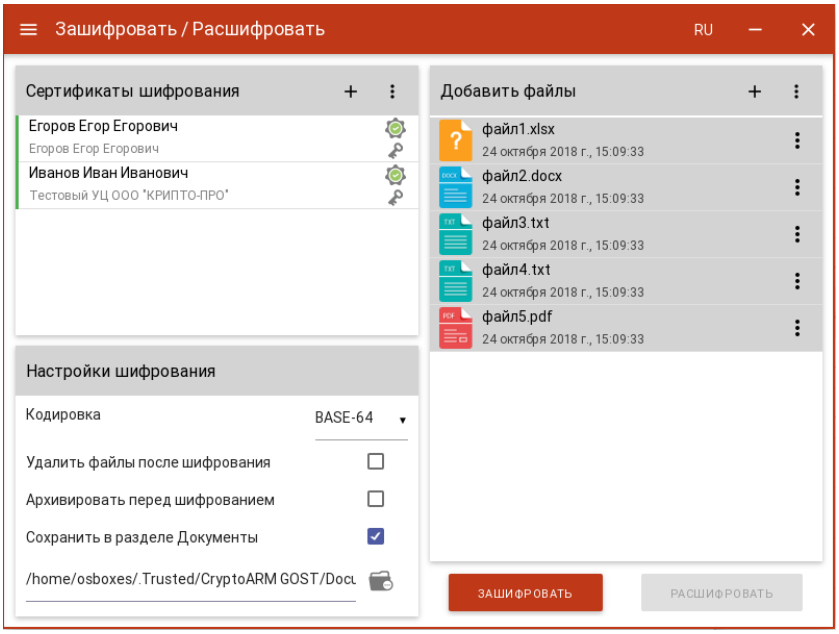


Рис. 8.7.2. Выбор файлов для шифрования

Выбранные файлы заносятся в правую область и представляют собой одноуровневый список. Для данного списка доступно контекстное меню в заголовке функционального элемента (рис. 8.7.3), 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.

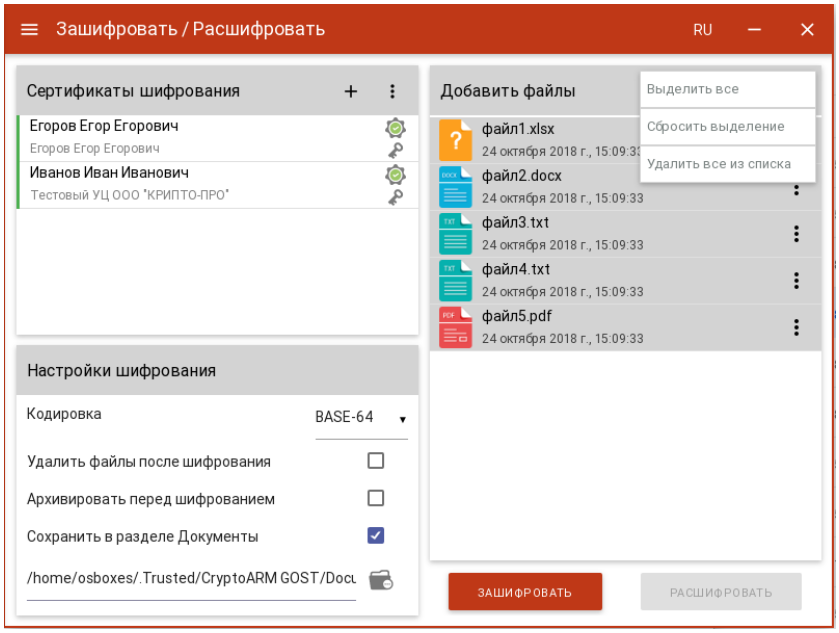


Рис. 8.7.3. Общее меню для выделенной группы файлов

В списке отображается наименование файла с расширением и дата его создания. Для каждого элемента списка доступно контекстное меню (рис. 8.7.4), 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.

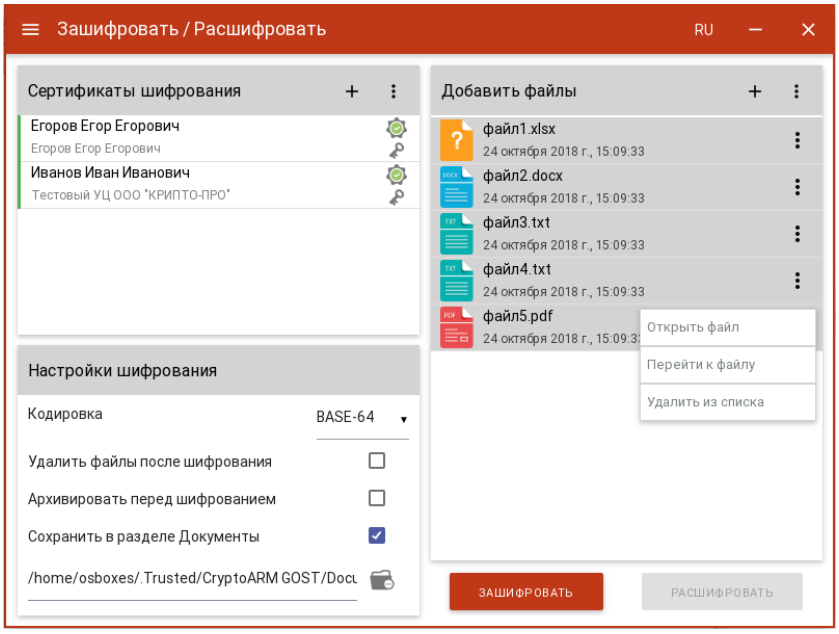


Рис. 8.7.4. Контекстное меню отдельного файла

ВЫБОР СЕРТИФИКАТОВ ПОЛУЧАТЕЛЕЙ. Для того, чтобы выполнить шифрование необходимо выбрать цифровые сертификаты получателей шифрованных файлов (рис. 8.7.5). 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. 8.7.6).

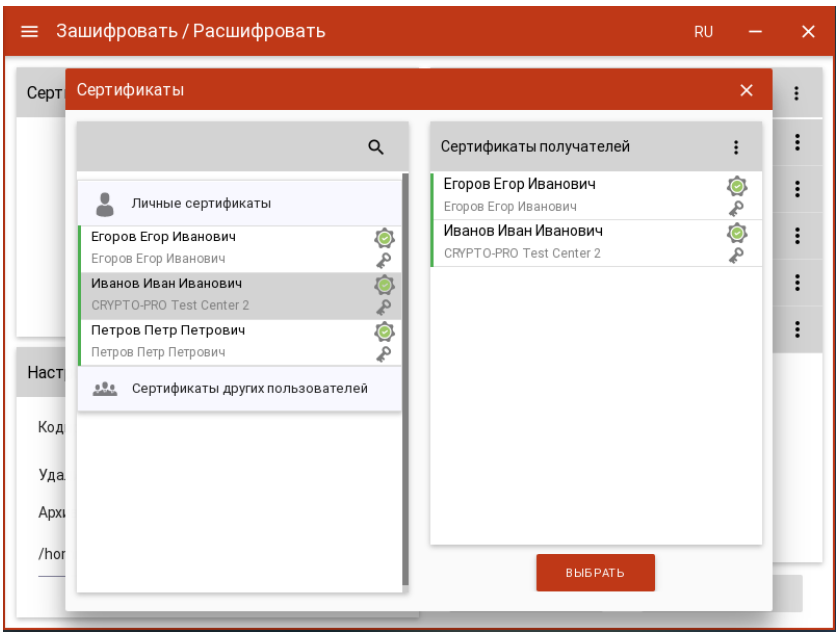


Рис. 8.7.5. Выбор сертификатов получателей

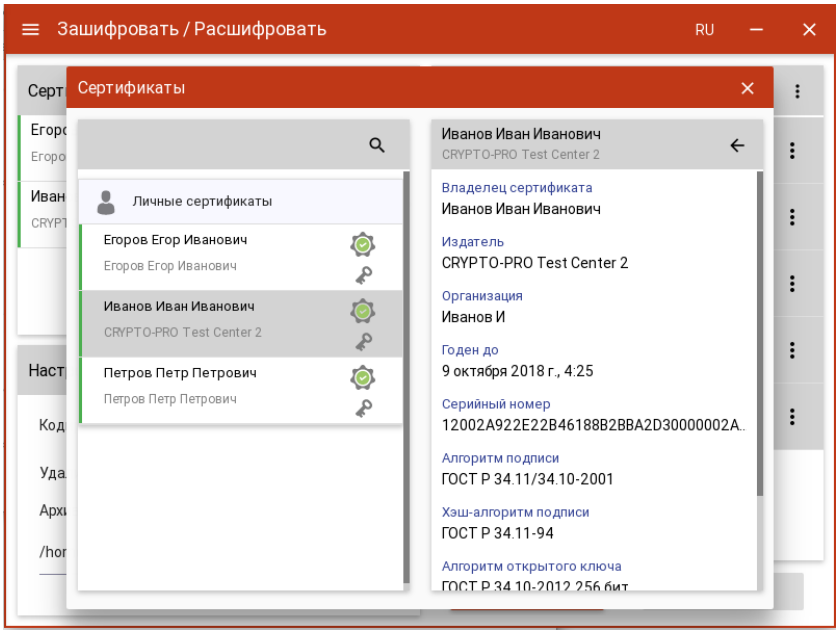


Рис.8.7.6. Детальная информация о сертификате получателя

Удалить сертификаты из списка получателей можно по одному двойным щелчком мыши по сертификату в правом списке, или, очистить весь список, с помощью контекстного меню в правом списке (рис. 8.7.7).

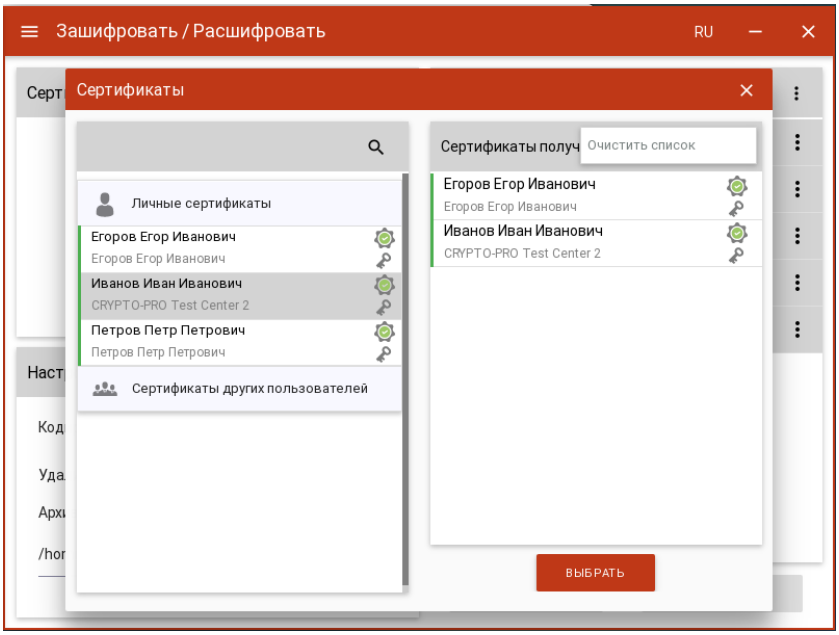


Рис. 8.7.7. Очистка списка сертификатов получателей

Если список сертификатов получателей заполнен, то его можно зафиксировать нажатием на кнопку **Выбрать** (рис. 8.7.8). Допускается изменение списка сертификатов получателей с помощью кнопки и контекстного меню в верхней части элемента.

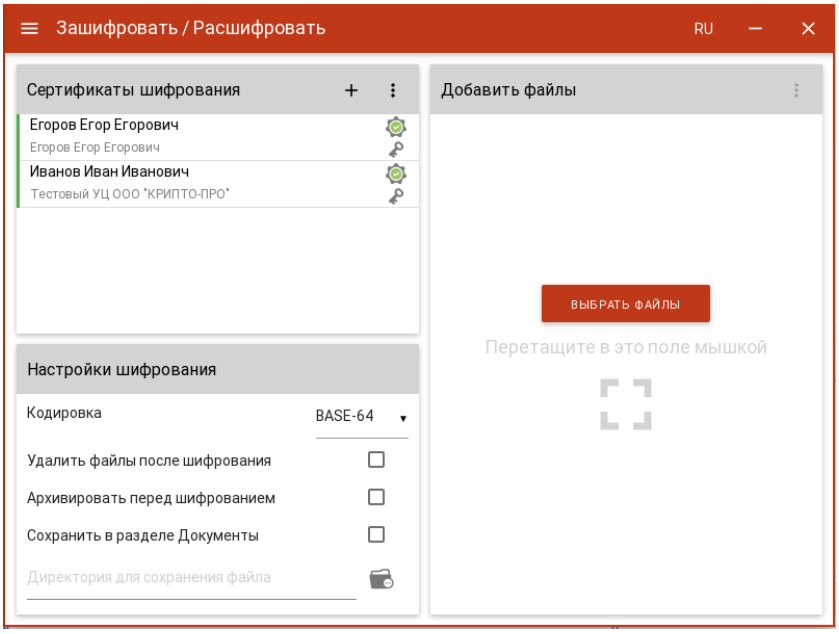


Рис. 8.7.8. Сформированный список получателей

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.
- **Сохранить в разделе Документы** – при установке флага файл сохраняется в каталог Documents, расположенный в папке пользователя в каталоге /Trusted/CryptoARM GOST/. При другой выбранной директории зашифрованный файл сохраняется в данной директории. Если директория не задана, то файл сохраняется рядом с исходным.

ШИФРОВАНИЕ ФАЙЛОВ. При условии выбора сертификатов получателей и шифруемых файлов в мастере становится доступной кнопка **Зашифровать** (рис. 8.7.2). 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. 8.7.9).

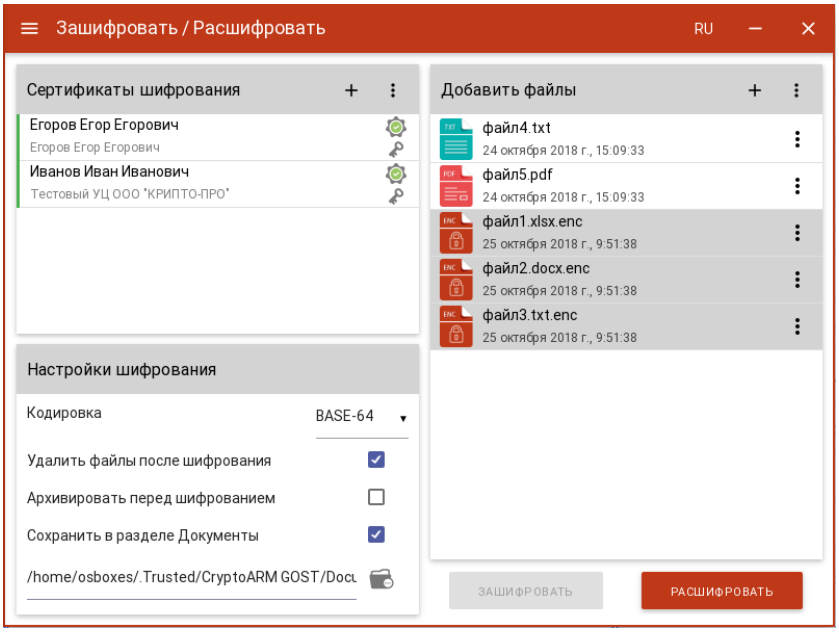


Рис. 8.7.9. Мастер расшифрования файлов

8.8. 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.

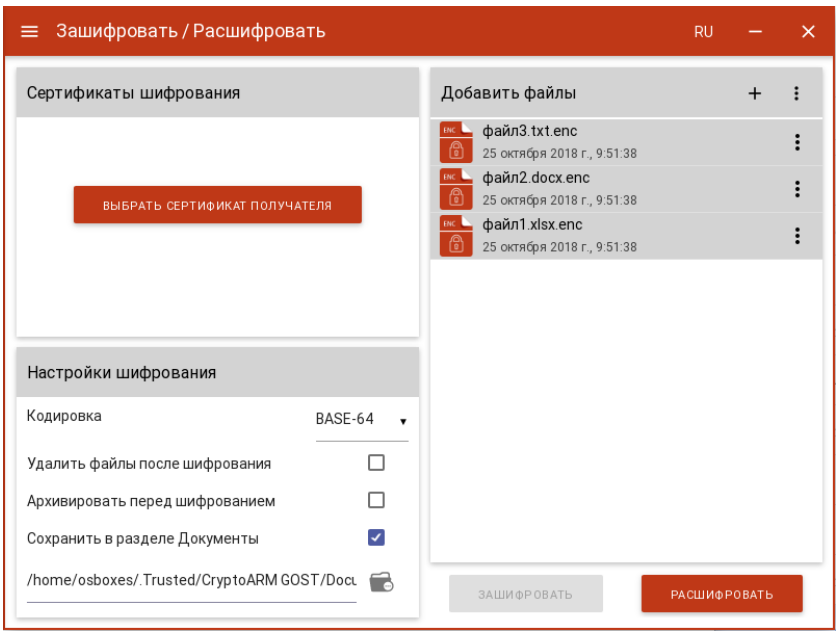


Рис. 8.8.1. Мастер расшифрования файлов

При расшифровании у файлов меняется иконка, наименование, дата создания. Если в настройках шифрования не задан каталог для сохранения файлов, они сохраняются в каталог Documents в папке пользователя в директории /Trusted/CryptoARM GOST/.

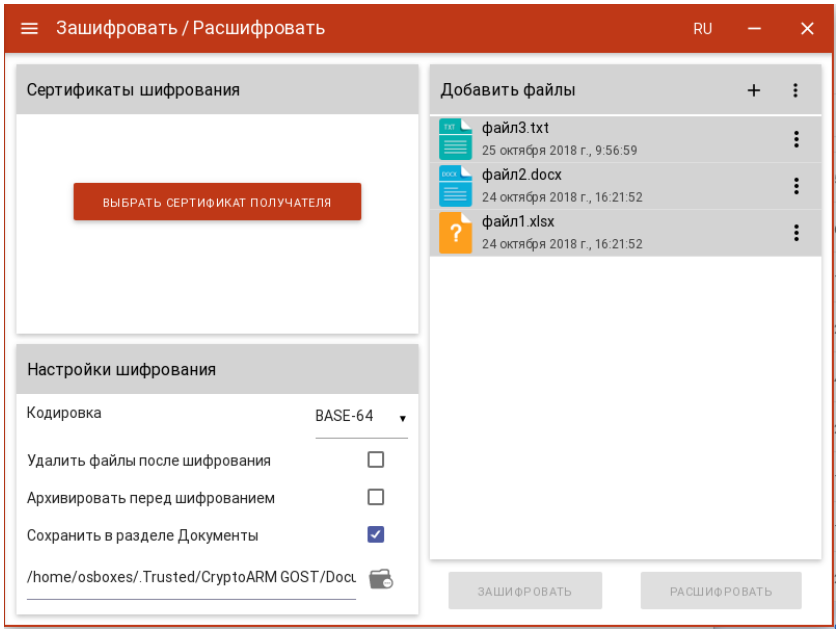


Рис. 8.8.2. Результат операции расшифрования

8.9. Управление сертификатами и ключами

Для управления сертификатами и ключами в приложении добавлено отдельное представление списка сертификатов. В левой области представления отображаются разделы, соответствующие категориям сертификатов (рис. 8.9.1). В правой области отображается информация о выделенном сертификате.

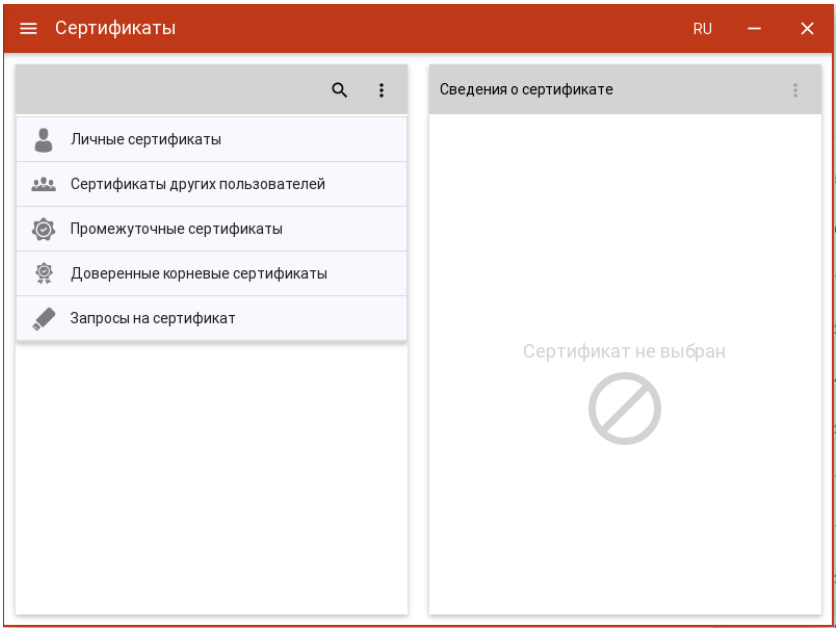


Рис. 8.9.1. Категории сертификатов

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. 8.9.2). Информация о сертификате представлена на двух вкладках: **Сведения о сертификате** и **Цепочка сертификации**.

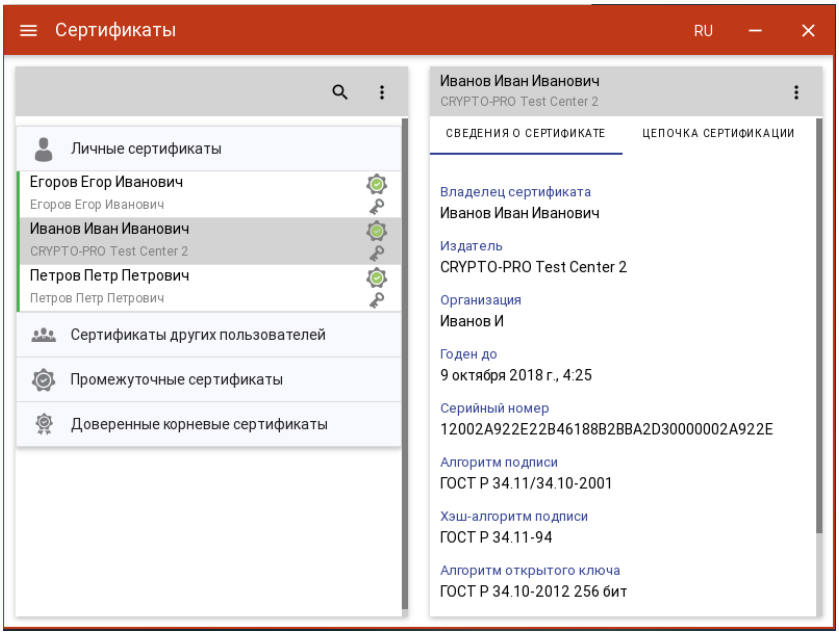


Рис. 8.9.2. Отображение сведений о выбранном сертификате

На вкладке **Цепочка сертификации** отображается общий статус построения цепочки доверия и приводится «дерево» сертификации, как показано на рис. 8.9.3.

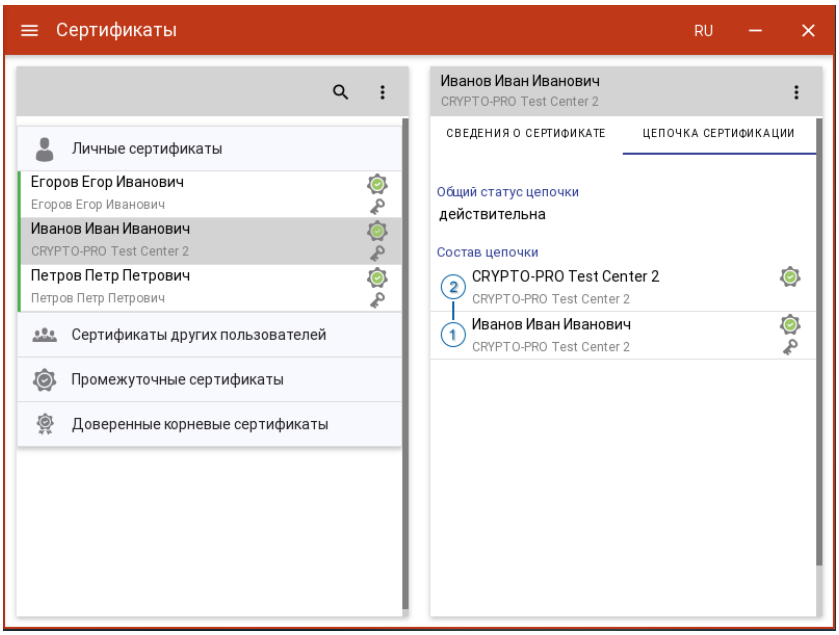


Рис. 8.9.3. Представление цепочки сертификации (цепочки доверия)

Импорт сертификата из файла. Для выполнения импорта нового сертификата в хранилище можно воспользоваться контекстным меню - выбрать операцию **Импорт из файла** (рис. 8.9.4). В

появившемся диалоговом окне нужно выбрать файл сертификата (поддерживаются кодировки BASE64 и DER).

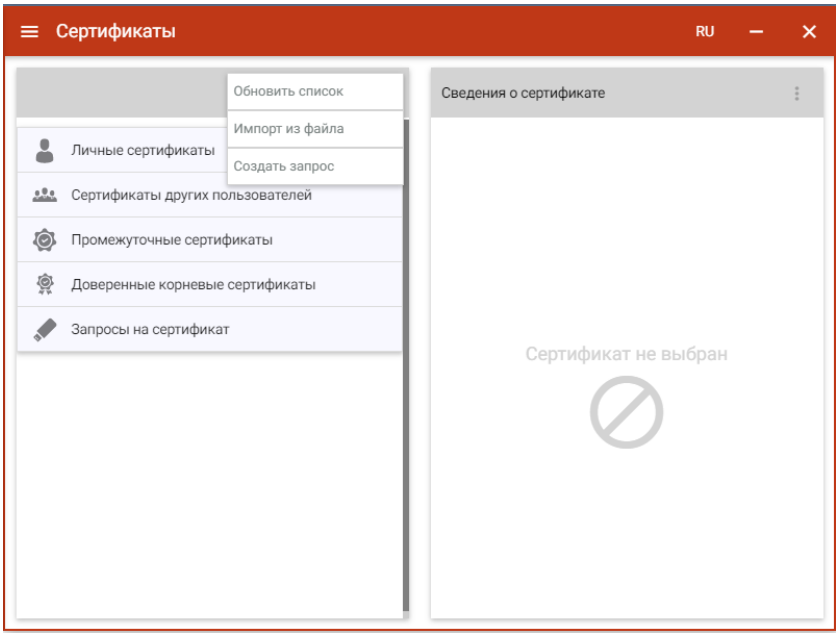


Рис.8.9.4. Меню импорта сертификата

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 КриптоАРМ ГОСТ (рис. 8.9.5).

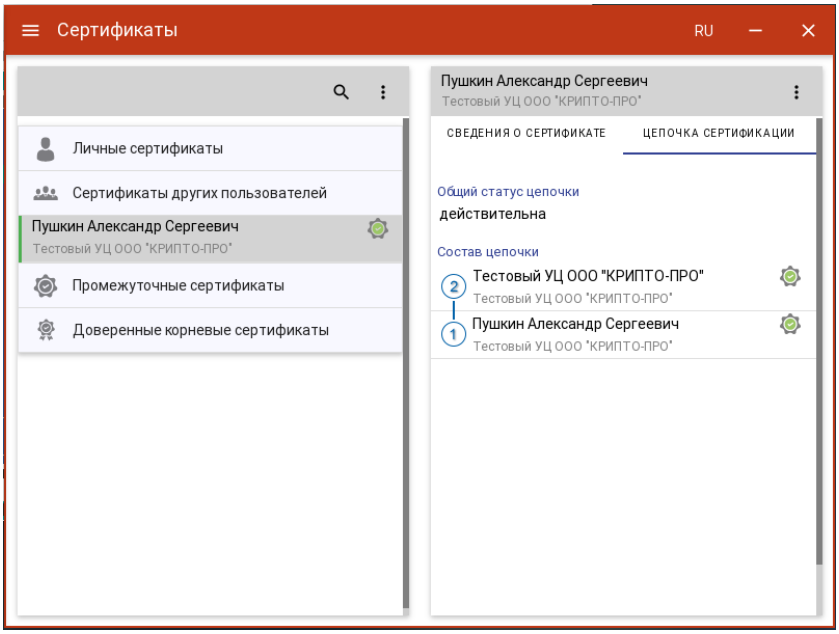


Рис. 8.9.5. Отображение импортированного сертификата

Импорт сертификата из DSS (доступно только для КриптоПро CSP 5). Для выполнения импорта сертификата из DSS в хранилище можно воспользоваться контекстным меню - выбрать операцию **Импорт из DSS** (рис. 8.9.6).

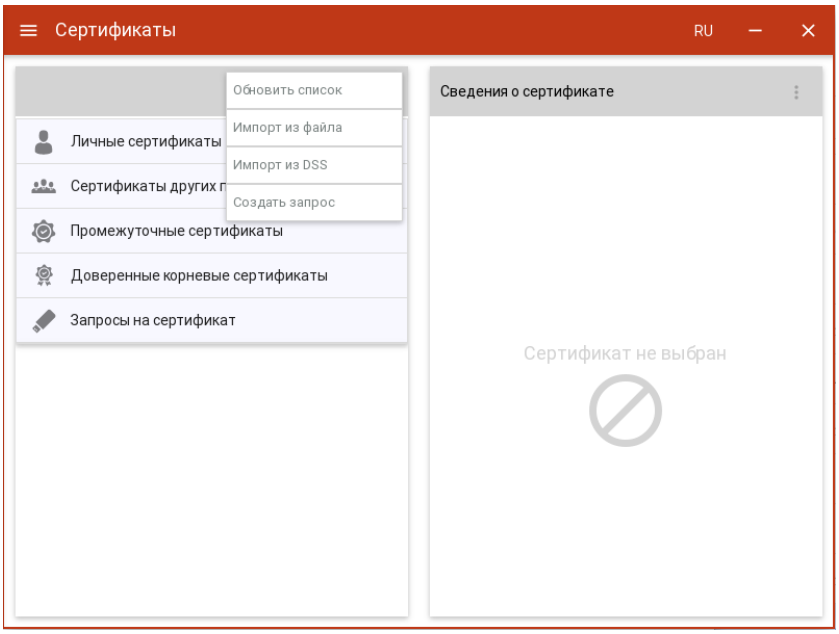


Рис.8.9.6. Меню импорта сертификата

В открывшемся окне указываются адреса серверов авторизации и DSS (рис. 8.9.7). По-умолчанию указаны адреса тестовых серверов КриптоПРО DSS.

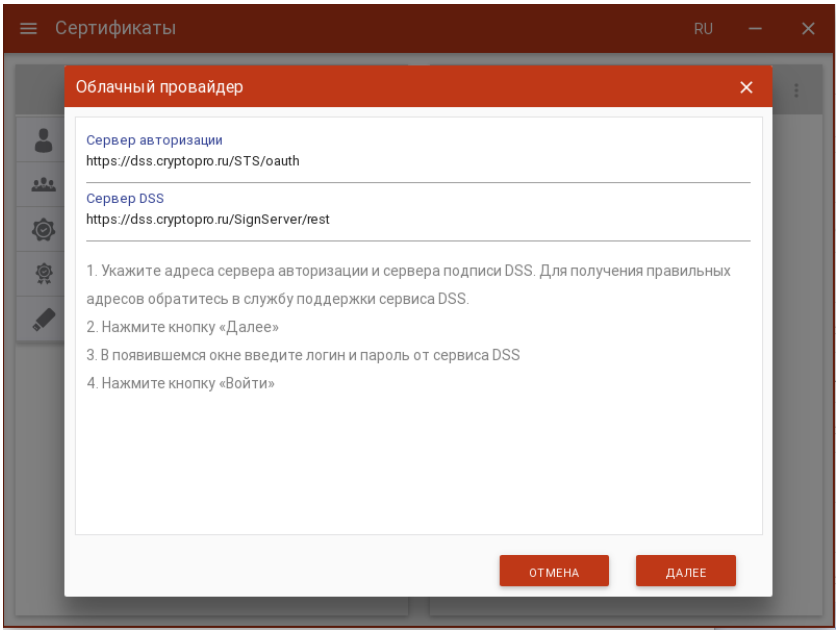


Рис.8.9.7. Настройка адреса серверов DSS

На следующем шаге нужно ввести логин и пароля для входа на сервис DSS (рис. 8.9.8)

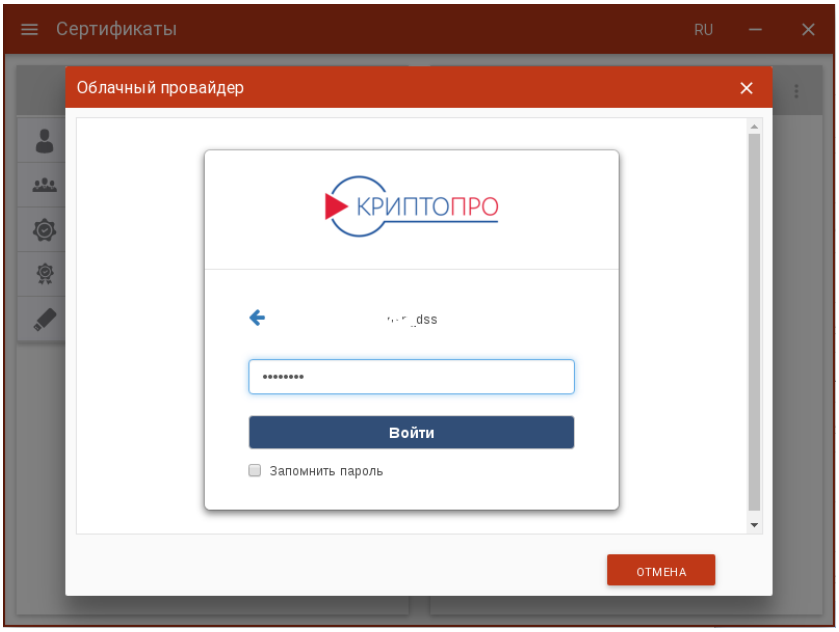


Рис.8.9.8. Ввод данных для авторизации на сервис DSS

При успешном импорте сертификаты DSS автоматически помещаются в хранилище личных сертификатов (рис. 8.9.9).

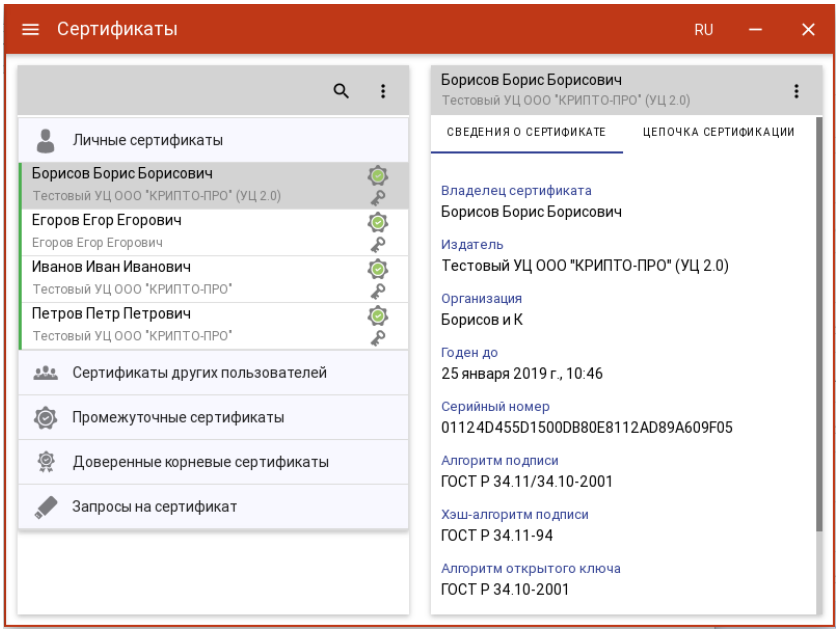


Рис. 8.9.9. Отображение импортированного DSS сертификата

ЭКСПОРТ СЕРТИФИКАТА В ФАЙЛ. Для экспорта сертификата в файл в контекстном меню сертификата нужно выбрать пункт **Экспортировать** (рис. 8.9.10). Если у сертификата экспортируемый закрытый ключ, то такой сертификат можно экспортировать вместе с закрытым ключом.

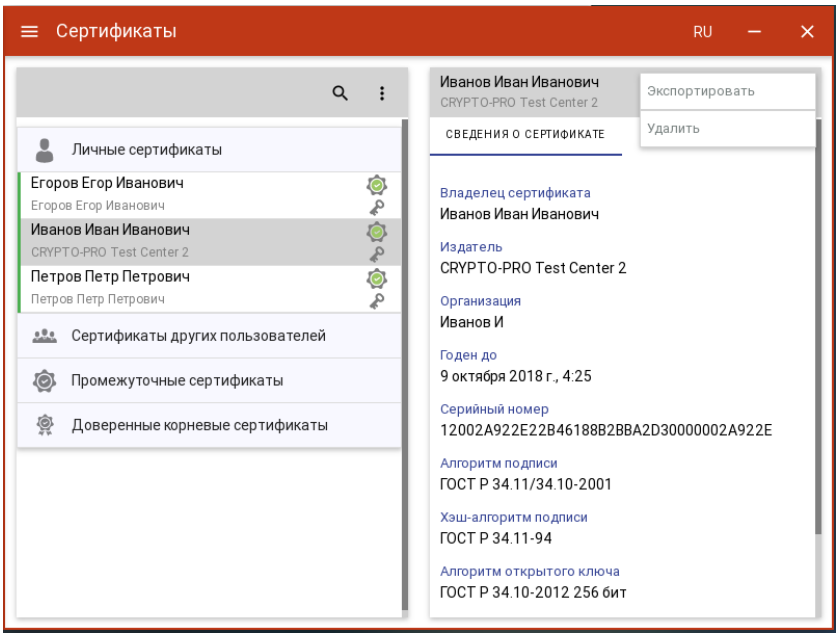


Рис. 8.9.10. Меню экспорта сертификата

При экспорте сертификата с не экспортируемым закрытым ключом появляется окно, в котором можно выбрать только кодировку файла сертификата (рис. 8.9.11).

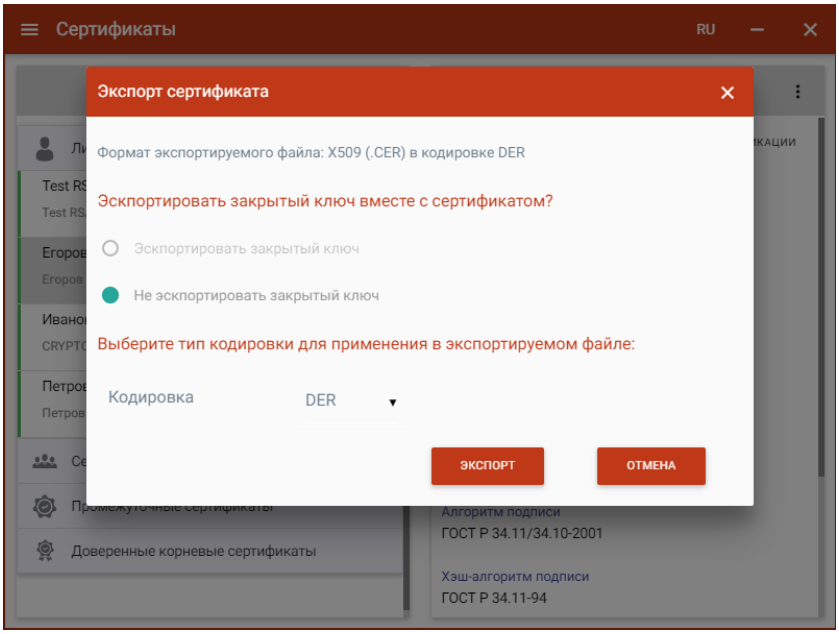


Рис. 8.9.11. Выбор кодировки файла сертификата

После нажатия кнопки **Экспорт**, в появившемся диалогом окне указать путь и имя файла, куда будет сохранен сертификат (по-умолчанию, файл export.cer).

При экспорте сертификата с экспортируемым закрытым ключом в появившемся диалоговом окне можно выбрать способ экспорта сертификата:

- экспортировать только сертификат без закрытого ключа. В таком случае нужно только выбрать кодировку файла сертификата (рис. 8.9.12).
- Экспортировать сертификат вместе с закрытым ключом. В таком случае надо указать пароль для защиты закрытого ключа (рис. 8.9.13).

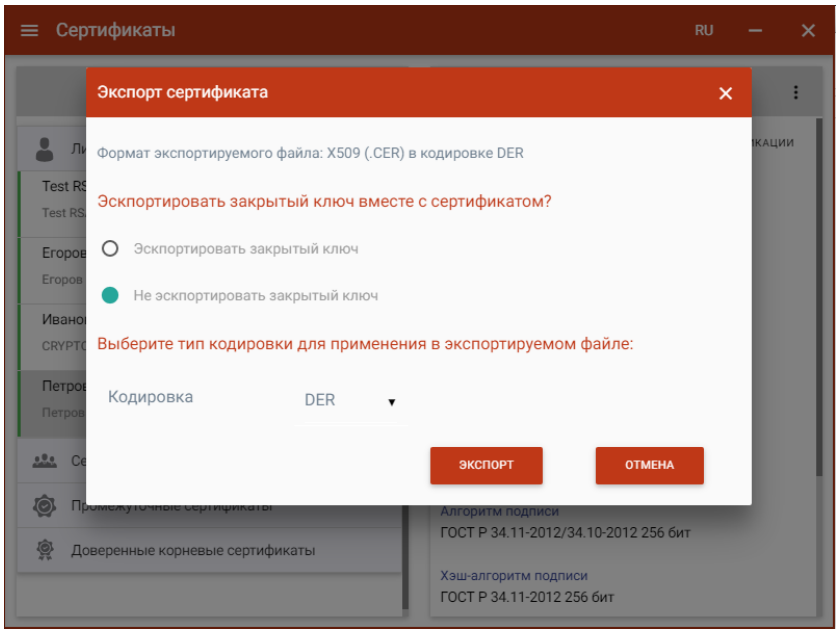


Рис. 8.9.12. Выбор способа экспорта сертификата

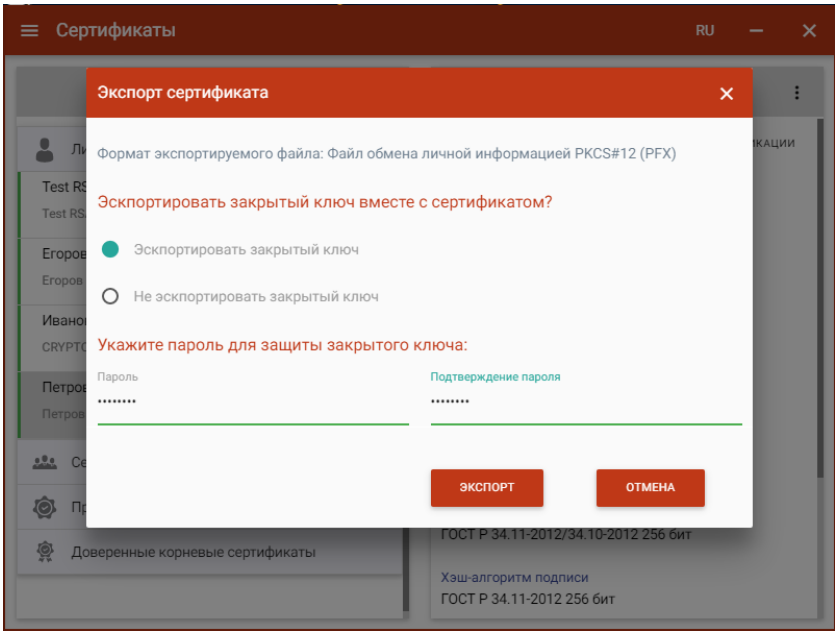


Рис. 8.9.13. Экспорт сертификата вместе с закрытым ключом

После нажатия кнопки **Экспорт**, в появившемся диалогом окне указать путь и имя файла, куда будет сохранен сертификат (по-умолчанию, файл export.pfx).

По окончании операции возникнет сообщение об успешном экспорте сертификата.

Примечание: если контейнер экспортируемого сертификата защищен паролем, то при экспорте сертификата вместе с закрытым ключом необходимо будет вводить пароль к ключевому контейнеру (рис. 8.9.14).

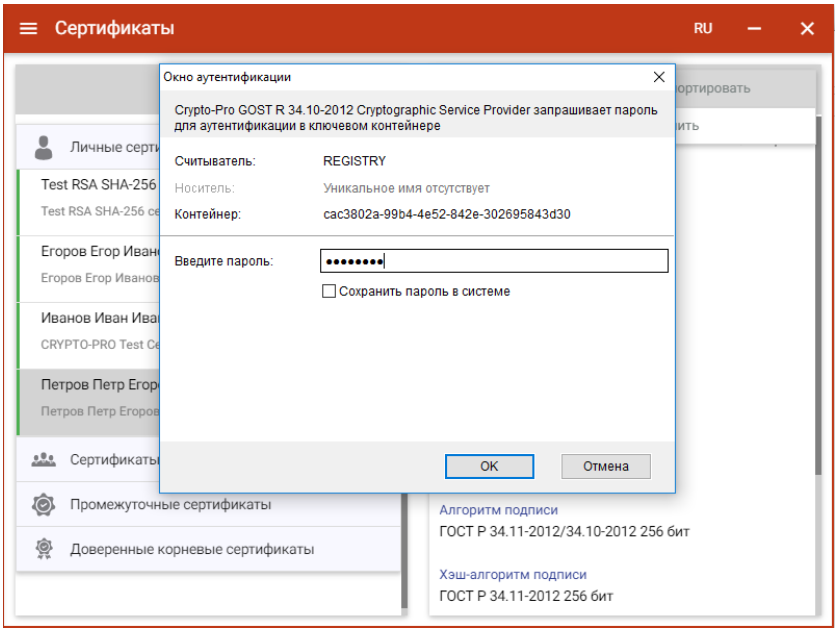


Рис. 8.9.14. Ввод пароля к ключевому контейнеру

УДАЛЕНИЕ СЕРТИФИКАТА. Для удаления сертификата в контекстном меню сертификата нужно выбрать пункт **Удалить** (рис. 8.9.15).

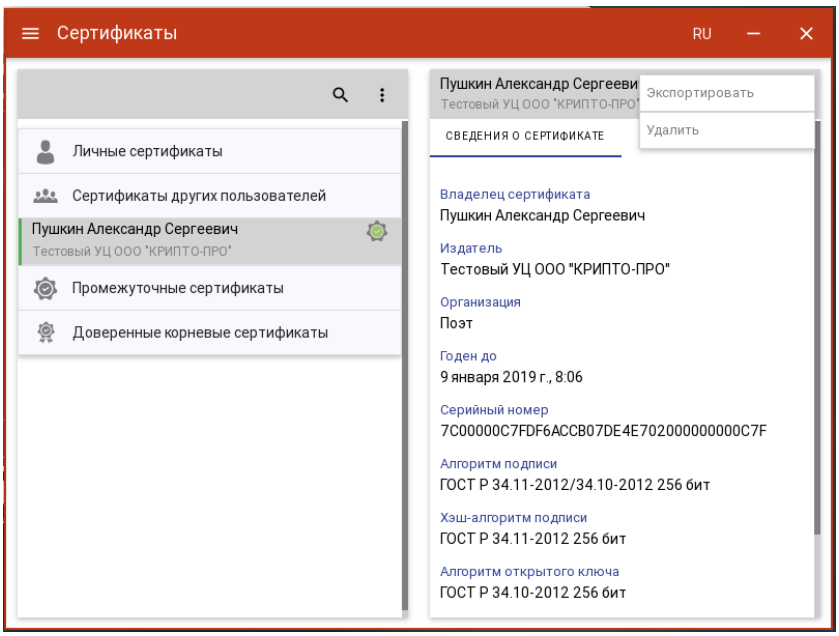


Рис. 8.9.15. Меню удаления сертификата

В появившемся диалоговом окне нажать **Удалить** для подтверждения удаления (рис. 8.9.16)

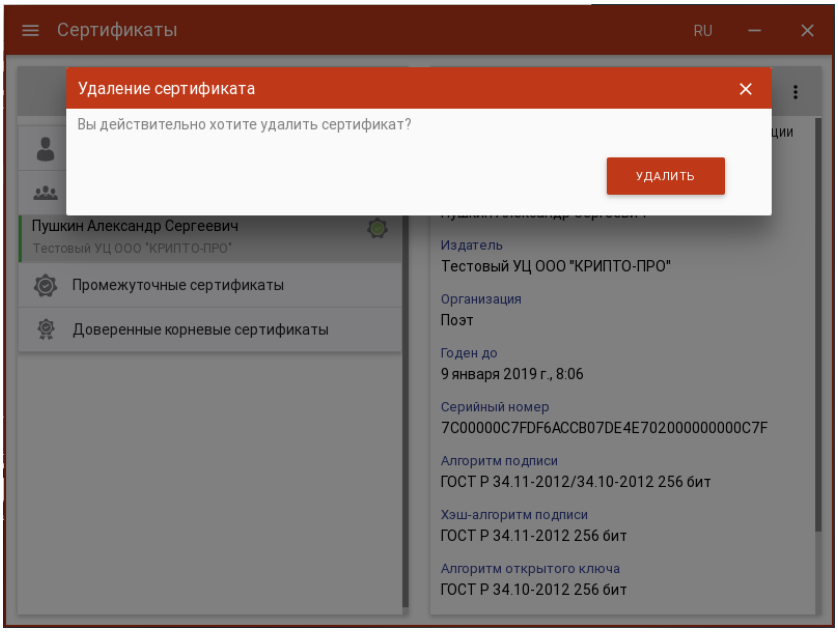


Рис. 8.9.16 Подтверждение удаления сертификата

Если у сертификата есть привязка к закрытому ключу, то при удалении сертификата возможно удаление закрытого ключа. Для удаления сертификат вместе с закрытым ключом в диалоговом окне надо поставить «галочку» **Удалить связанный с сертификатом контейнер** и нажать кнопку **Удалить** (рис. 8.9.17).

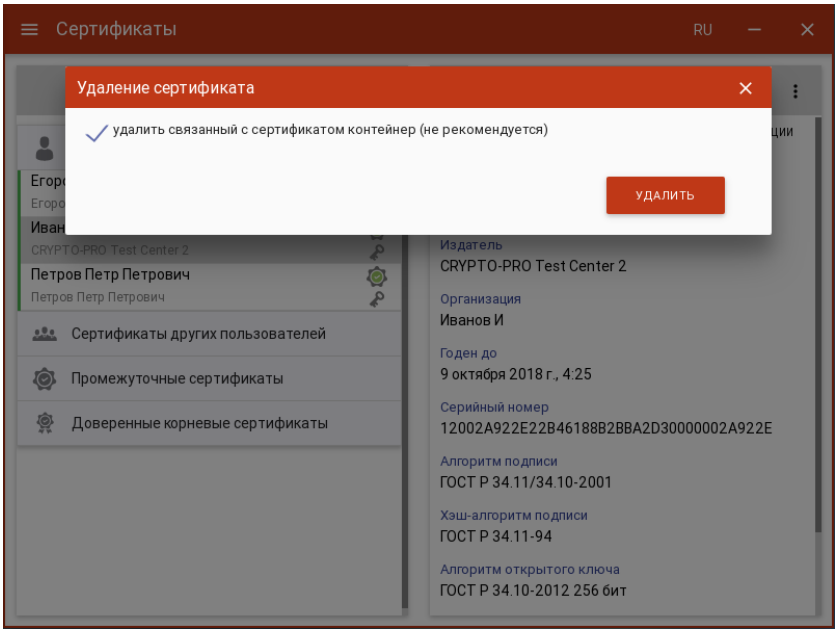


Рис. 8.9.17 Подтверждение удаления сертификата с закрытым ключом

Примечание. Не рекомендуется удалять контейнер закрытого ключа, так как он не подлежит восстановлению.

СОЗДАНИЕ ЗАПРОСА НА СЕРТИФИКАТ. Для создания запроса на сертификат в контекстном меню списка сертификатов следует выбрать операцию **Создать запрос** (рис. 8.9.18).

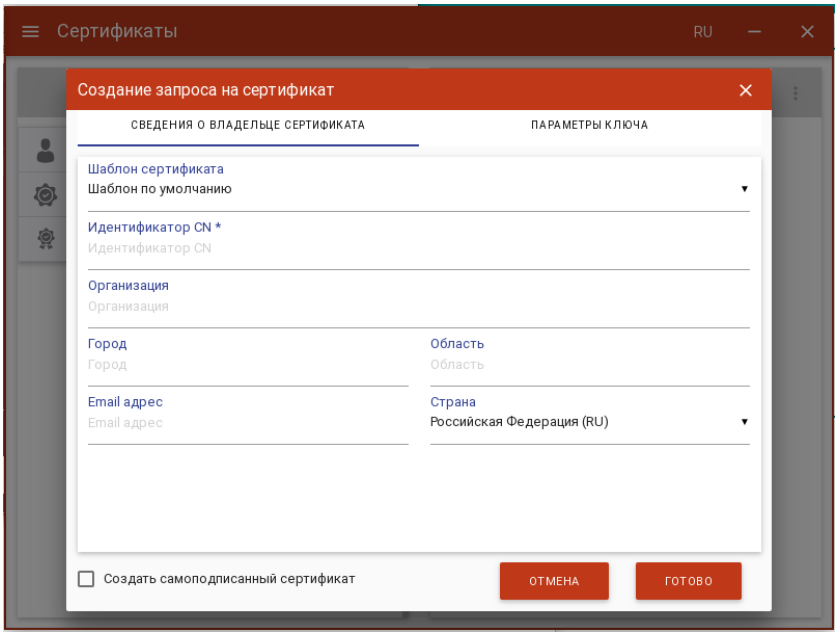


Рис. 8.9.18. Создание запроса на сертификат

Опции необходимых сведений для генерации запроса распределены на две вкладки: **Сведения о владельце сертификата** и **Параметры ключа**.

В параметрах субъекта указывается:

– Шаблон сертификата (рис. 8.9.19);

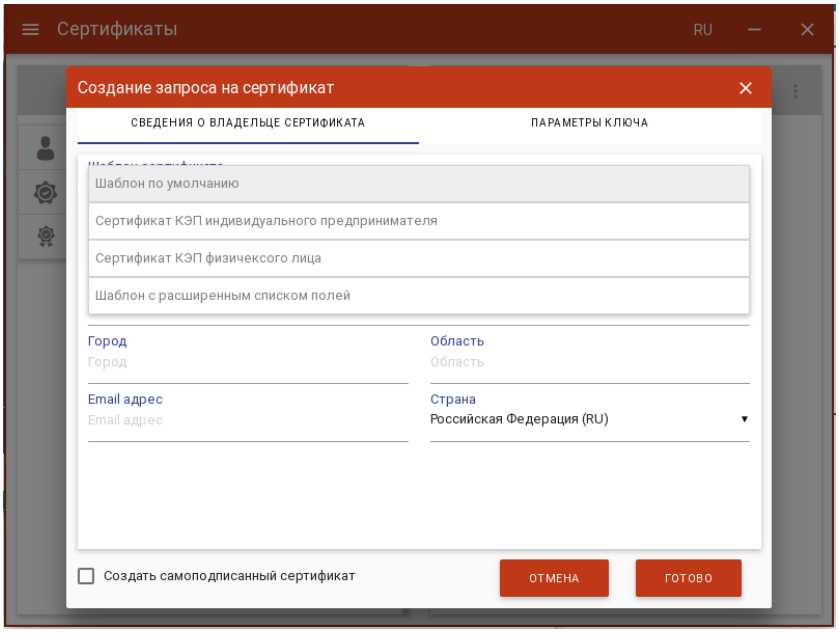


Рис. 8.9.19. Выбор шаблона сертификата

– Основная информация, в которой, согласно выбранному на предыдущем шаге шаблону, необходимо указать идентификационную информацию о владельце сертификата (рис. 8.9.20).

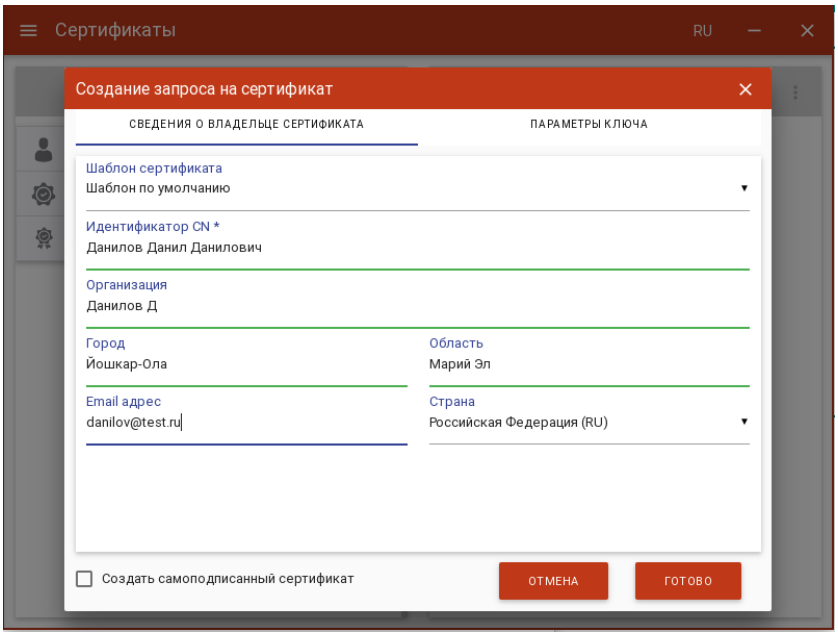


Рис. 8.9.20. Информация о владельце сертификата

– При установке флага **Создать самоподписанный сертификат** происходит создание сертификата и его автоматическая установка в личное хранилище пользователя. Запросы на самоподписанные сертификаты не создаются.

В параметрах ключа указывается:

– Алгоритм ключа (рис. 8.9.21);

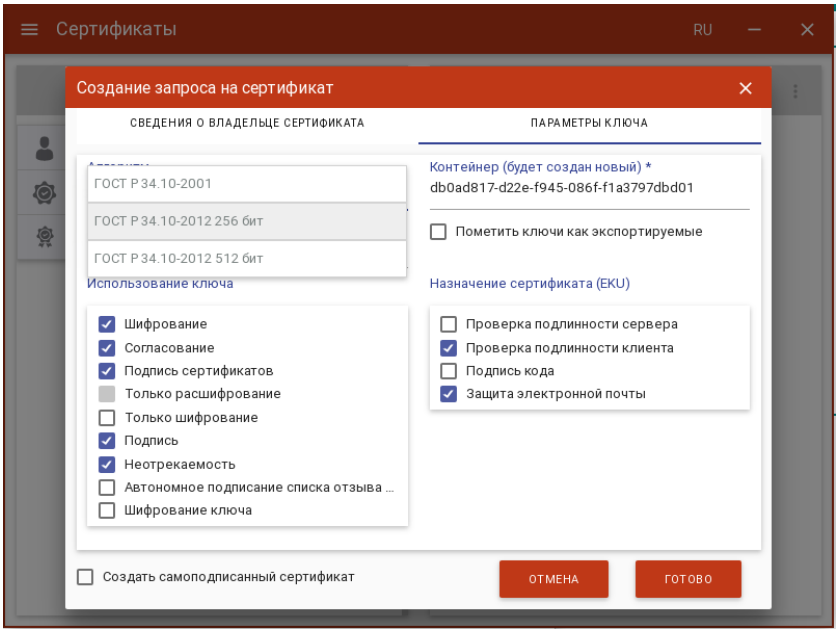


Рис. 8.9.21. Выбор алгоритма ключа

– Назначение ключа (рис. 8.9.22);

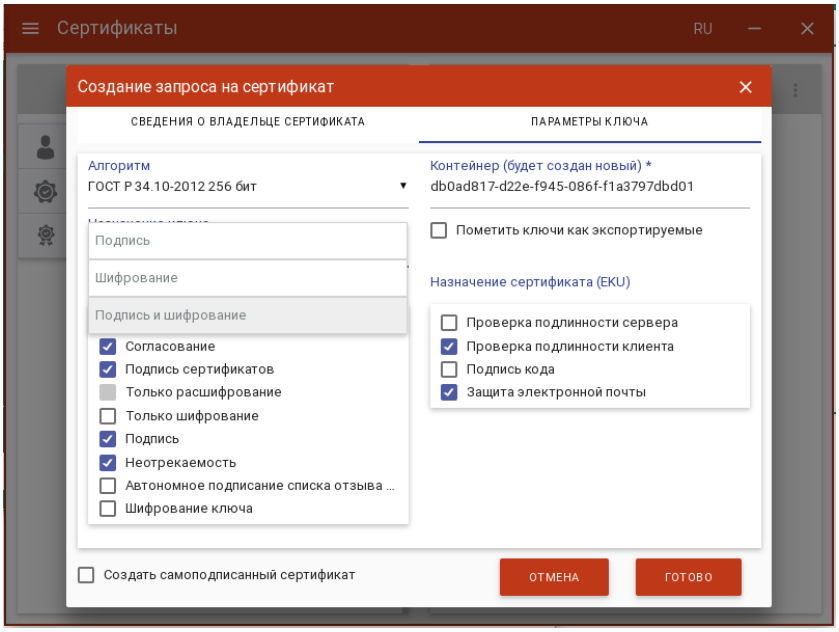


Рис. 8.9.22. Выбор назначения ключа

– Использование ключа (рис. 8.9.23);

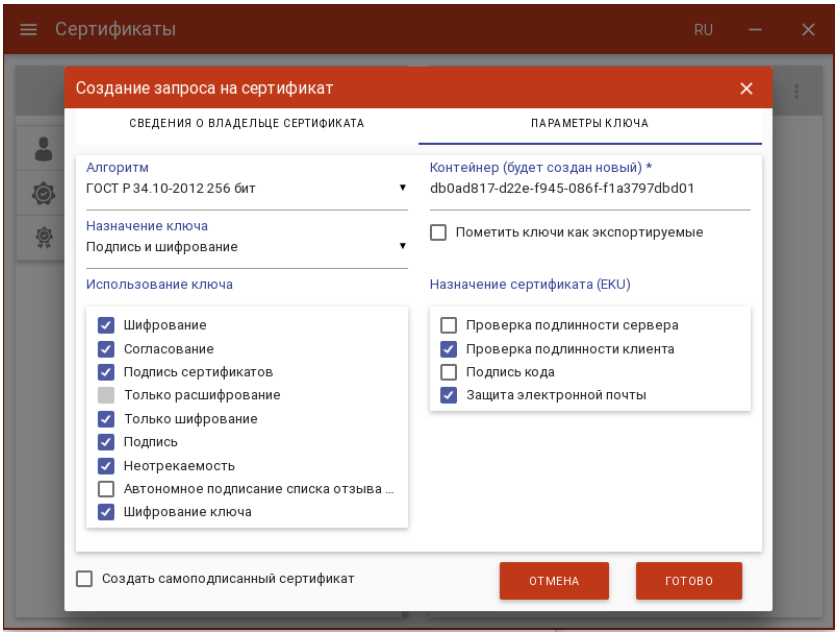


Рис. 8.9.23. Выбор использования ключа

- Контейнер - сертификат будет создан на основе нового ключевого набора. Можно задать свое имя ключевого набора или оставить созданное автоматически.
- Пометить ключи как экспортируемые. Если отметить этот флаг, то можно проводить экспорт сертификата вместе с закрытым ключом.
- Назначение сертификата (EKU).

На основе указанных данных по кнопке **Готово** будет сформирован запрос на сертификат. Для ГОСТ сертификата выберите ключевой носитель для хранения контейнера (Реестр, диск, токен). На запрос системы установите пароль на данный контейнер и подтвердите его. После завершения операции возникнет окно с информацией о ее результатах

Запрос сохраняется в файл «<CN сертификата>_<алгоритм >_<дата генерации>.req» в папке пользователя в каталоге \.Trusted\CryptoARM GOST\CSR и отображается на вкладке **Запросы на сертификат** (рис. 8.9.24).

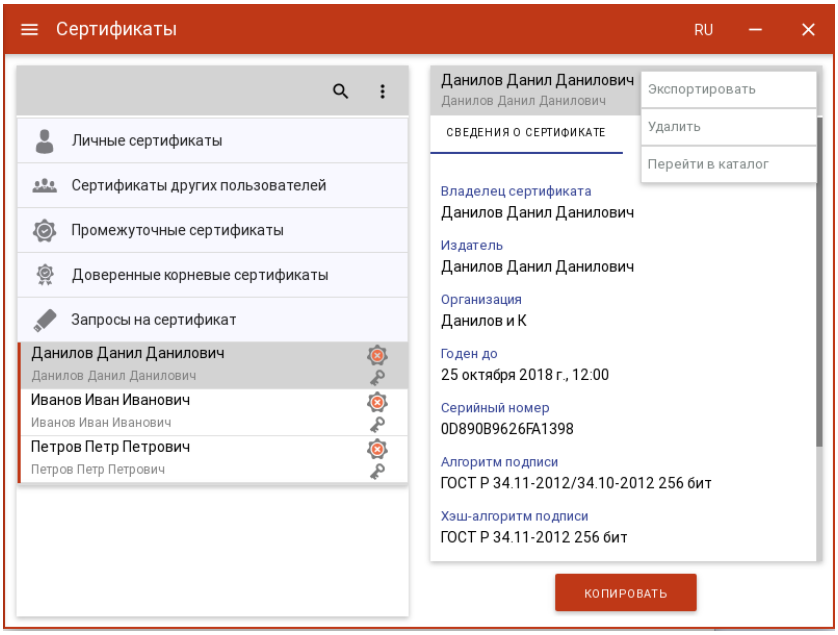


Рис. 8.9.24 Форма просмотра запроса на сертификат

Для запроса доступны следующие операции:

- **Экспортировать** – для сохранения сертификата в файл;
- **Удалить** – для удаления запроса из списка, при этом файл запроса не удаляется из папки;
- **Перейти в каталог** – для открытия каталога в файловом менеджере, где располагается файл запроса;
- **Копировать** – для создания нового запроса по шаблону. Открывается форма создания запроса на сертификат, в полях которого автоматически заполнены поля из шаблона выбранного запроса. Можно скорректировать нужные сведения и создать запрос.

Созданный файл запроса на сертификат следует направить на рассмотрение в Удостоверяющий центр (УЦ). Полученный из УЦ сертификат следует импортировать для работы с данным сертификатом в приложении.

СОЗДАНИЕ САМОПОДПИСАННОГО СЕРТИФИКАТА. Для создания самоподписанного сертификата на форме **Создать запрос** следует поставить флаг **Создание самоподписанного сертификата** (рис. 8.9.25).

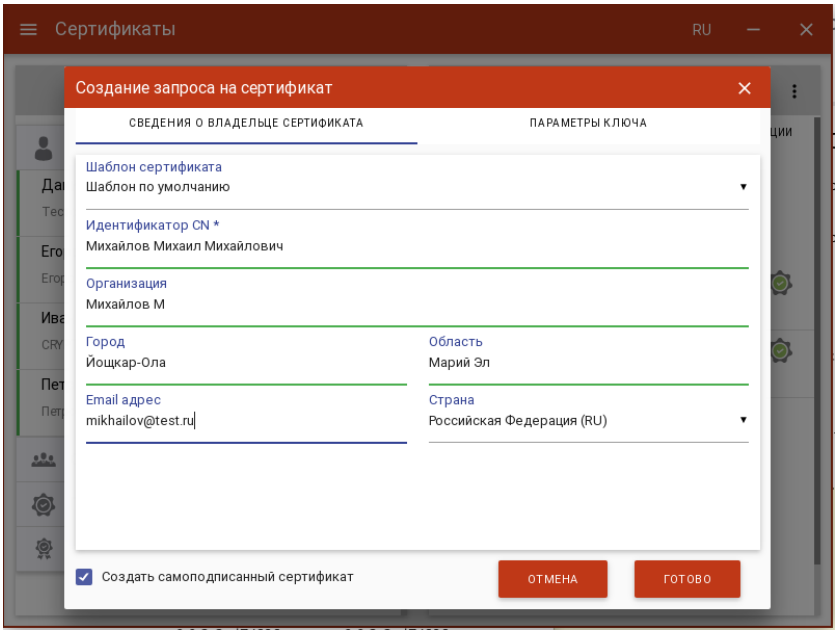


Рис. 8.9.25. Создание самоподписанного сертификата

На основе указанных данных по кнопке **Готово** будет сформирован самоподписанный сертифкат. Для ГОСТ сертификата выберите ключевой носитель для хранения контейнера (Реестр, диск, токен). На запрос системы установите пароль на данный контейнер и подтвердите его. После завершения операции возникнет окно с информацией о ее результатах. Сертификат будет в списке Личных сертификатов (рис. 8.9.26)

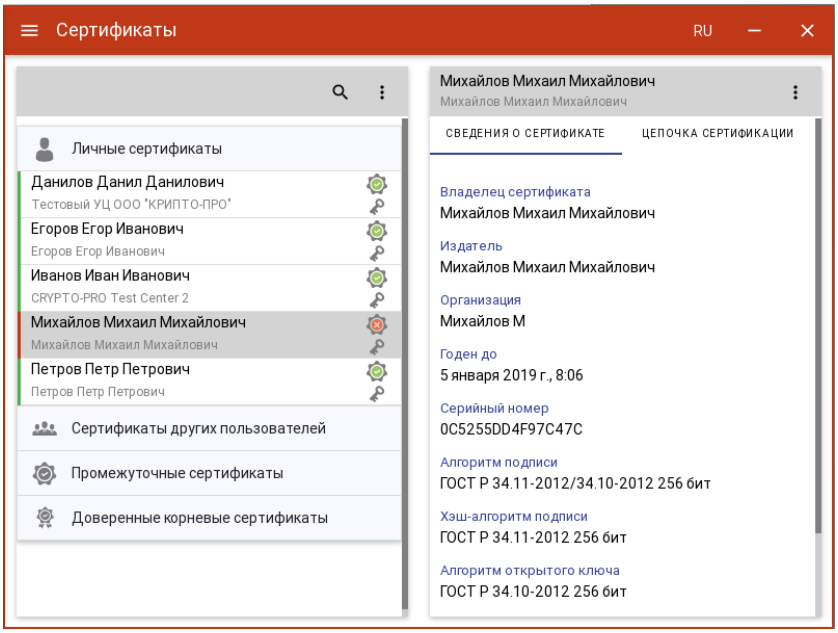


Рис. 8.9.26. Список Личных сертификатов

При генерации самоподписанного сертификата запрос на сертификат не создается.

СПИСКИ ОТЗЫВА СЕРТИФИКАТОВ (COC). Для работы со списками отзыва сертификатов в мастере управления сертификатами добавлен раздел **Списки отзыва сертификатов** (рис. 8.9.27).

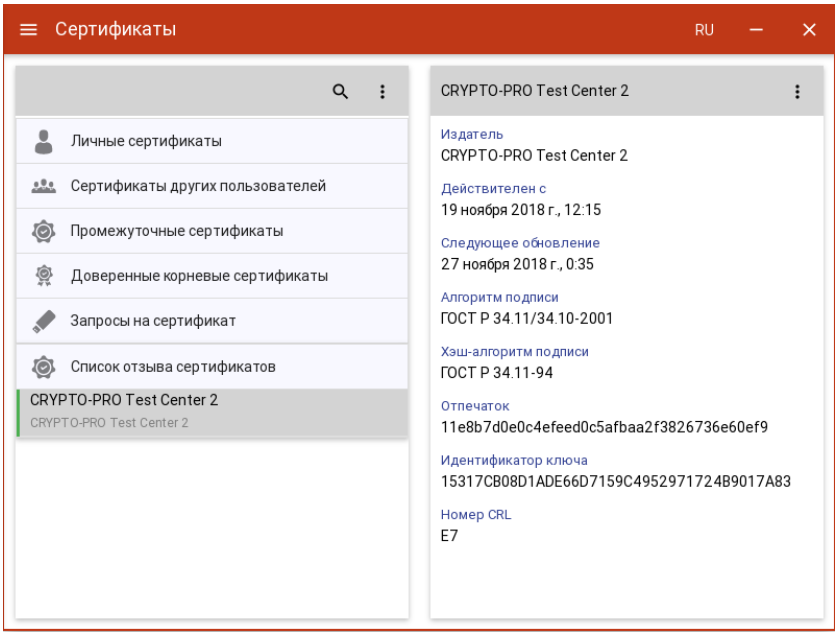


Рис. 8.9.27. Списки отзыва сертификатов

Если раздел не отображается в списке, значит в хранилище нет импортированных списков отзыва сертификатов.

Для импорта списка отзыва надо выбрать в контекстном меню Импорт из файла и выбрать файл списка отзыва (рис. 8.9.28)

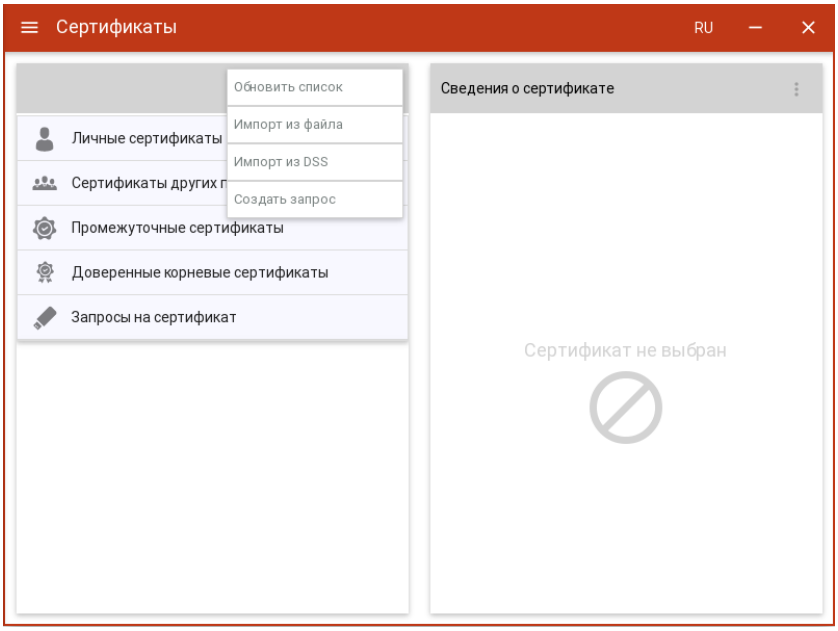


Рис. 8.9.28. Импорт списка отзыва сертификатов

Импортированный список отображается в разделе **Список отзыва сертификатов** (рис. 8.9.27).

Выбранный СОС можно экспортировать или удалить, выбрав соответствующий пункт меню на форме просмотра СОС (рис. 8.9.29).

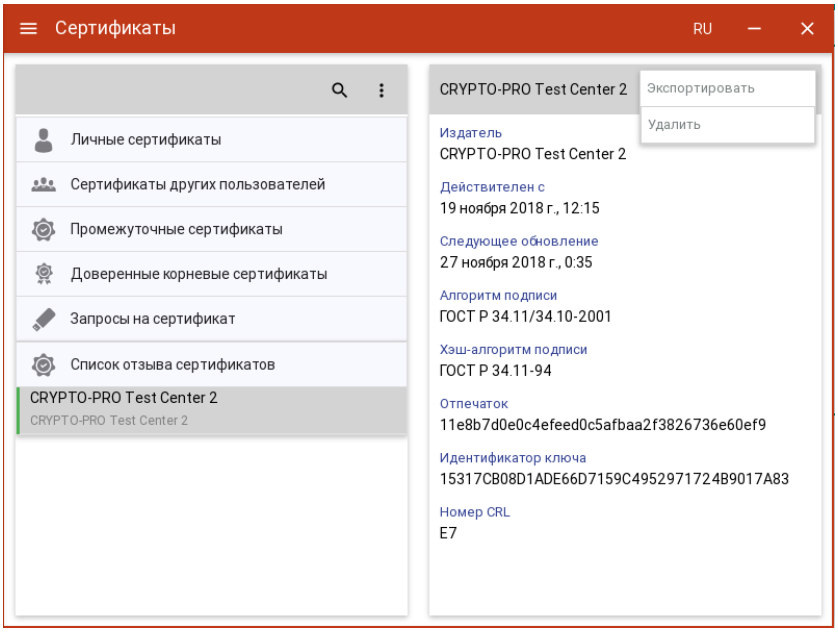


Рис. 8.9.29. Контекстное меню СОС

Экспорт СОС. При выборе Экспортировать в контекстном меню списка отзыва сертификатов открывается форма выбора кодировки файла (рис. 8.9.30). При нажатии на **Экспорт** следует выбрать директорию для сохранения и задать имя файла СОС.

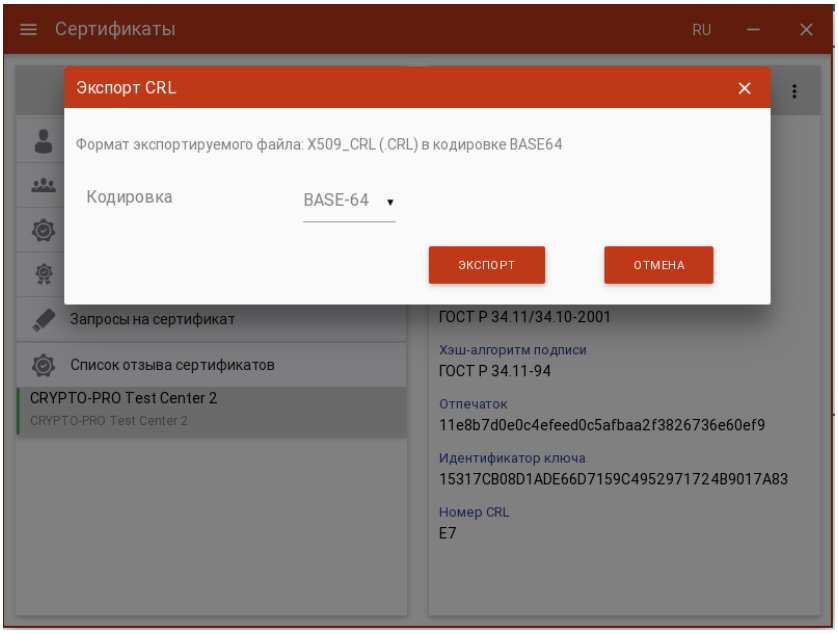


Рис. 8.9.30. Выбор кодировки экспортируемого СОС

Удаление СОС. Для удаления СОС надо выбрать пункт контекстного меню **Удалить** и подтвердить удаление в соответствующем окне (рис. 8.9.31).

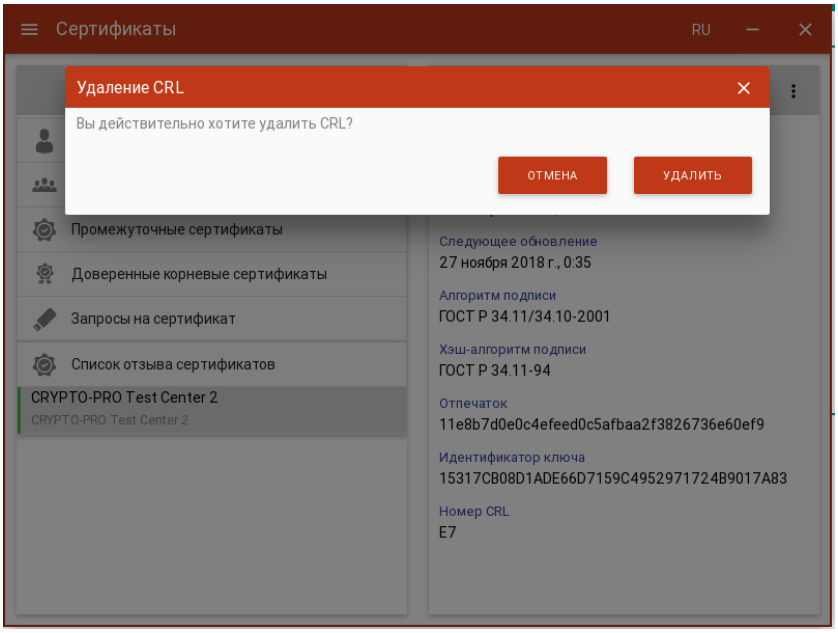


Рис. 8.9.31. Подтверждение удаления СОС

8.10. Поиск сертификата

В элементах пользовательского интерфейса, где процесс выполнения операции учитывает выбор сертификата из списка, реализована функция поиска сертификатов (рис. 8.10.1). 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».

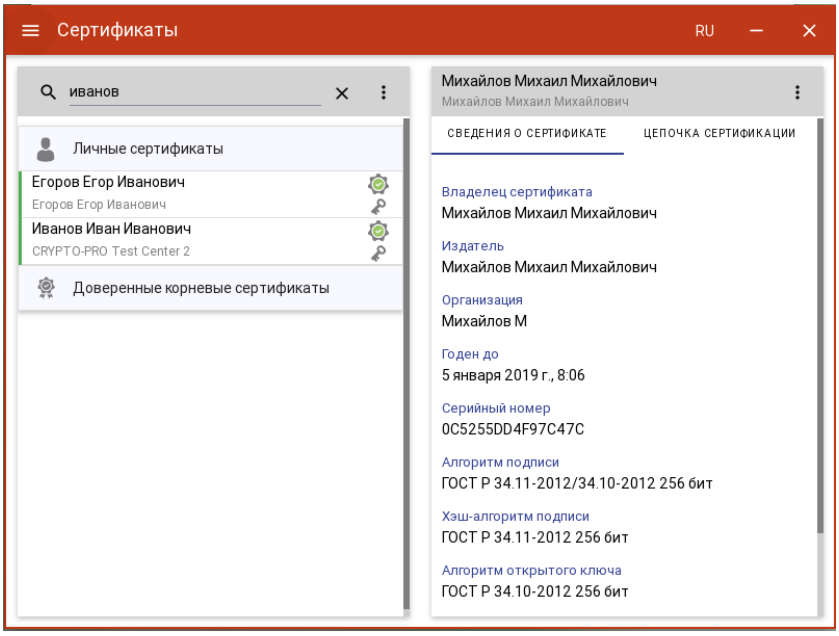


Рис. 8.10.1. Поиск сертификата

8.11. Установка сертификата из ключевого контейнера

Для установки сертификата из ключевого контейнера в приложении добавлено отдельное представление **Контейнеры**. В левой области представления отображаются все подключенные хранилища контейнеров закрытых ключей. В правой области отображается информация о сертификате в выделенном контейнере (рис. 8.11.1).

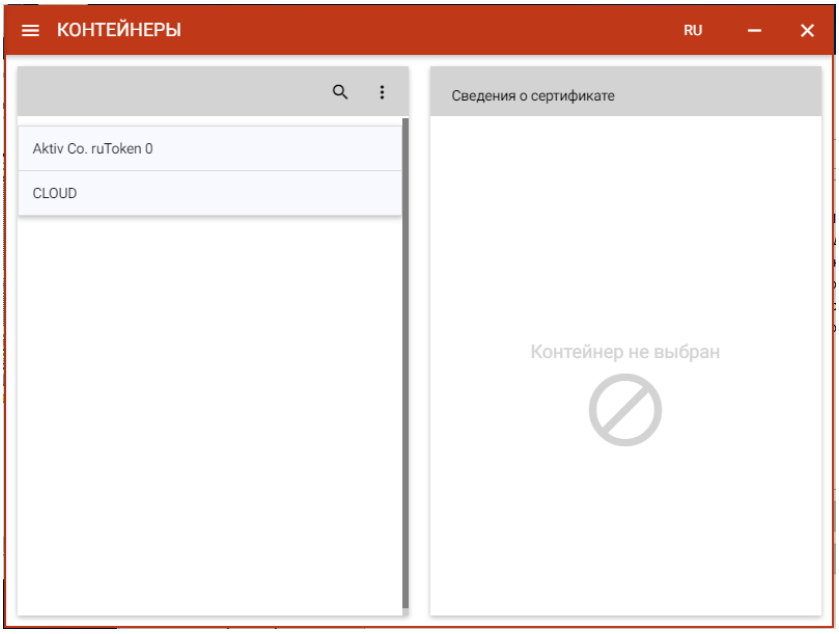


Рис. 8.11.1. Хранилища контейнеров закрытых ключей

В каждом из хранилищ отображаются контейнеры закрытых ключей. В случае отсутствия контейнеров в хранилище, оно может быть скрыто как пустое.

После выбора контейнера отображается информация о находящемся в нем сертификате (рис. 8.11.2).

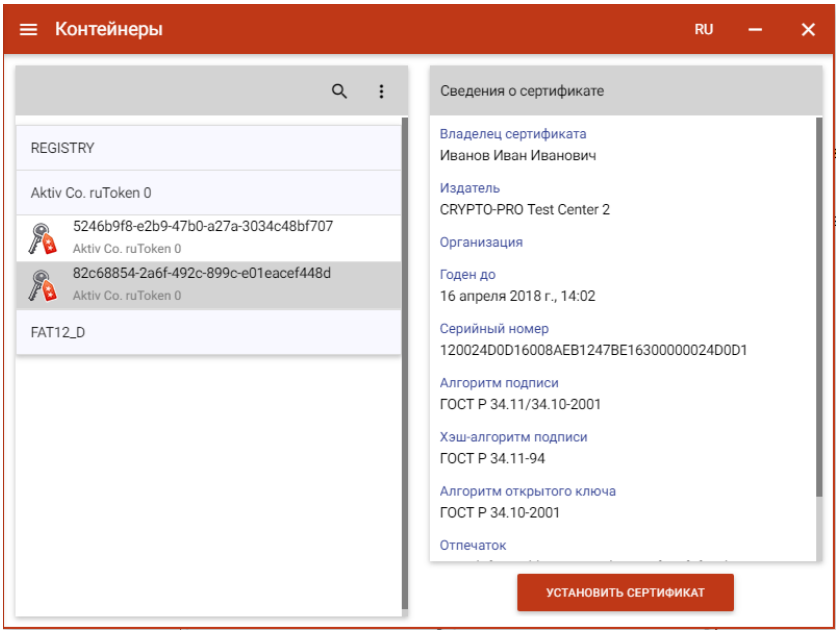


Рис. 8.11.2 Информация о сертификате в контейнере

По кнопке **Установить сертификат** происходит установка сертификата в Личное хранилище сертификатов. Данный сертификат становится доступен для выполнения операций подписи, шифрования и расшифрования.

8.12. Документы

Для сохранения результатов выполнения операций подписи, снятия подписи, шифрования и расшифрования используется каталог Документы. Каталог с документами располагается в каталоге пользователя в папке \.Trusted\CryptoARM GOST\Documents\. Просмотреть документы в каталоге можно, выбрав пункт меню «Документы» (рис. 8.12.1).

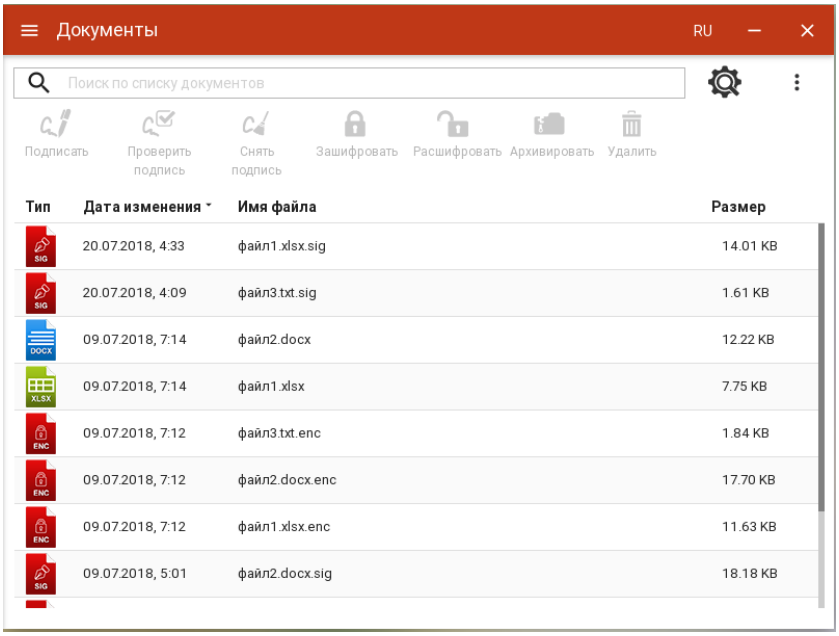


Рис. 8.12.1 Список документов

При выделении записей в списке становятся доступны кнопки для выполнения операций с данными документами (рис. 8.12.2)

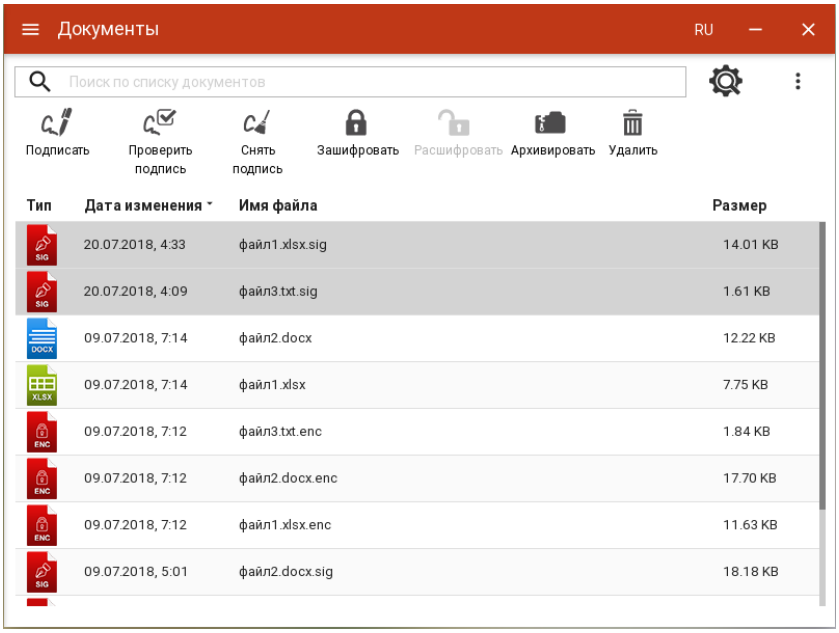


Рис. 8.12.2 Список документов

При нажатии на кнопку будет выполнена соответствующая операция:

- **Подписать** - выделенные документы передаются в качестве входных файлов в мастер подписи/проверки подписи для создания подписи;
- **Проверить подпись** - выделенные документы передаются в мастер подписи/проверки подписи, где выполняется проверка имеющихся подписей файлов;
- **Снять подпись** - выделенные документы передаются в мастер подписи/проверки подписи, где выполняется снятие подписи с файлов;
- **Зашифровать** - выделенные документы передаются в качестве входных файлов в мастер шифрования/расшифрования для операции шифрования файлов;
- **Расшифровать** - выделенные документы передаются в качестве входных файлов в мастер шифрования/расшифрования для операции расшифрования;
- **Архивировать** - выделенные файлы упаковываются в архив и сохраняются в каталог с документами. В качестве имени используется формат: Arhive_dd.mm.yyy_hh.mm.rar. Если в настройках указано ограничение на размер архива, то создается многотомный архив с последовательной нумерацией каждого нового тома.
- **Открытие настроек параметров архивации** - вызывает открытие диалогового окна задания настроек архивирования;
- **Удалить** - выделенные файлы физически удаляются из каталога с документами.

Для списка документов доступно **контекстное меню** (рис. 8.12.3), состоящее из пунктов:

- **Обновить** - выполняется обновление списка документов;
- **Выделить все** – выполняется выделение всех записей в списке документов;
- **Перейти в каталог** - выполняется открытие каталога документов.

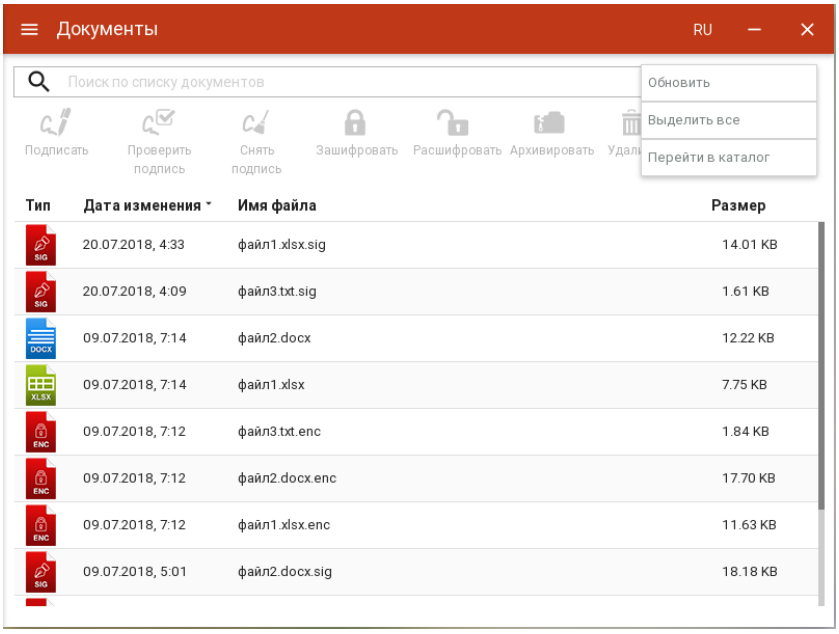


Рис. 8.12.3 Контекстное меню списка документов

ПОИСК ЗАПИСЕЙ В СПИСКЕ ДОКУМЕНТОВ. В представлении Документы реализован поиск записей по символьному совпадению (рис. 8.12.4)

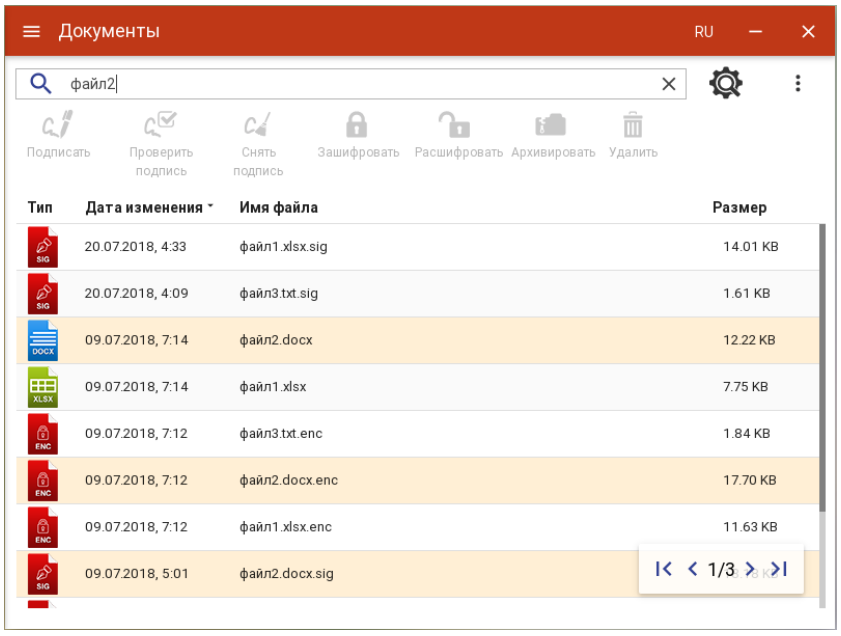


Рис. 8.13.4. Поиск записей в сипске документов

ФИЛЬТРАЦИЯ СПИСКА ДОКУМЕНТОВ. Для открытия окна настроек критериев фильтра на панели управления имеется кнопка  . При нажатии на кнопку открывается окно настроек фильтрации (рис. 8.12.5).

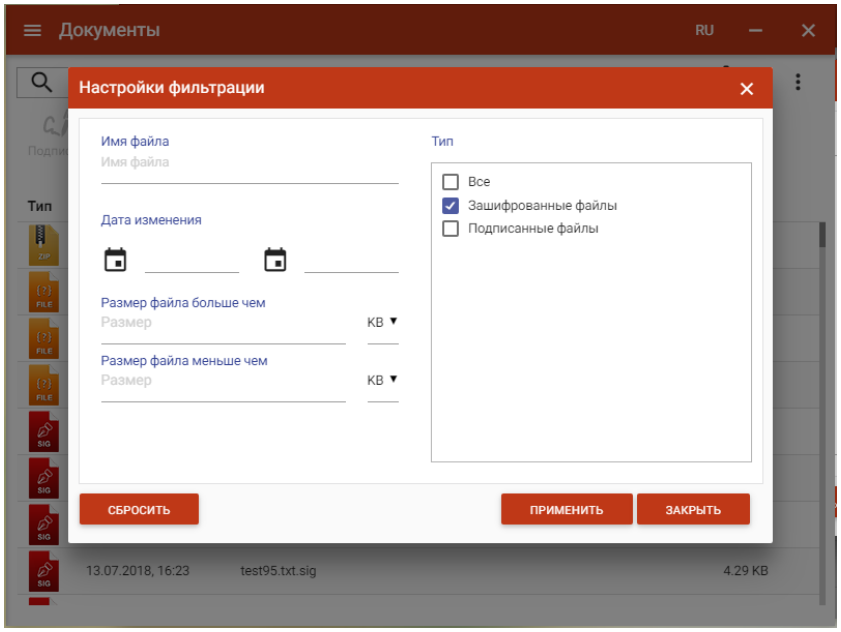


Рис. 8.12.5. Настройки критериев фильтра документов

Применение фильтрации выполняется по нажатию кнопки “Применить”. В зависимости от выставленных критериев фильтра в списке документов остаются только те записи, которые удовлетворяют (суммарно) этим критериям. Кнопка открытия окна настроек фильтрации имеет вид  (рис. 8.12.6).

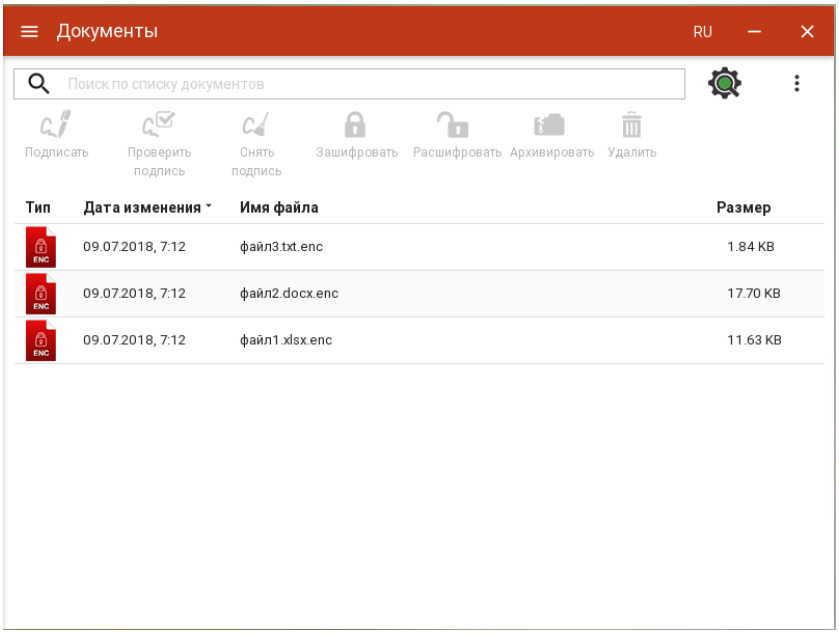


Рис. 8.12.6. Результат применения фильтрации документов

Для сброса заданных критериев фильтрации служит кнопка «Сбросить» в окне настроек фильтрации (рис. 8.12.5).

8.13. Журнал операций

Журнал операций предназначен для отображения операций, выполняемых пользователем (рис. 8.13.1).

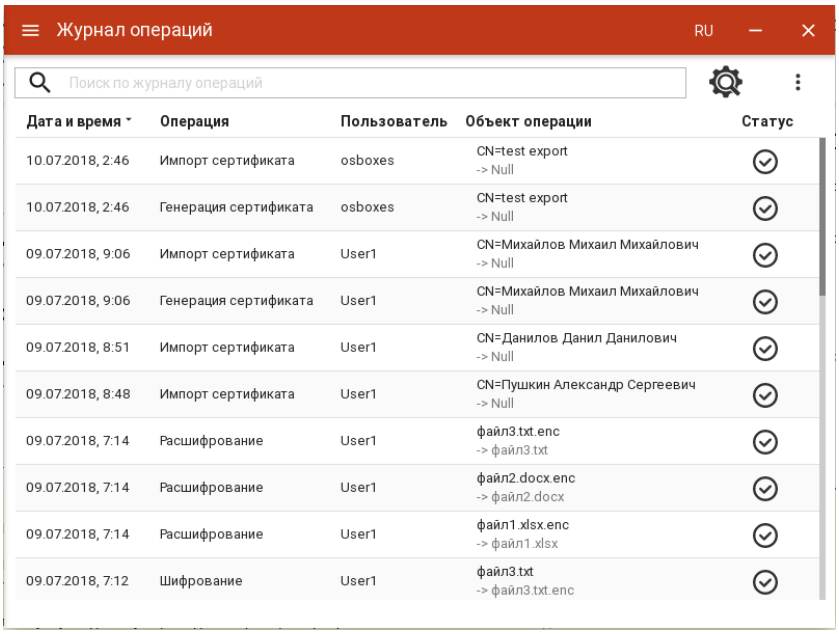


Рис. 8.13.1 Журнал операций

В журнале отображаются следующие типы операций:

- подпись;
- снятие подписи;
- шифрование;
- расшифрование;
- генерация сертификата;
- генерация запроса на сертификат;
- импорт сертификата;
- импорт сертификата в формате pkcs#12;
- удаление сертификата;
- удаление контейнера.

Текущая версия журнала операций записывается в файл cryptoarm_gost_operations[порядковый номер журнала].log, который находится в папке пользователя в директории \.Trusted\CryptoARM_Gost\ под Windows и \.Trusted\CryptoARM_Gost\ под OSX и Linux.

По мере накопления записей в журнале операций выполняется автоматический переход к новому файлу журнала со следующим порядковым номером.

При работе с журналом операций предусмотрен режим загрузки ранее сохраненной в архив его части для просмотра, поиска и фильтрации записей. Для этого используется пункт “Загрузить архивный журнал” контекстного меню журнала (рис.8.13.2)

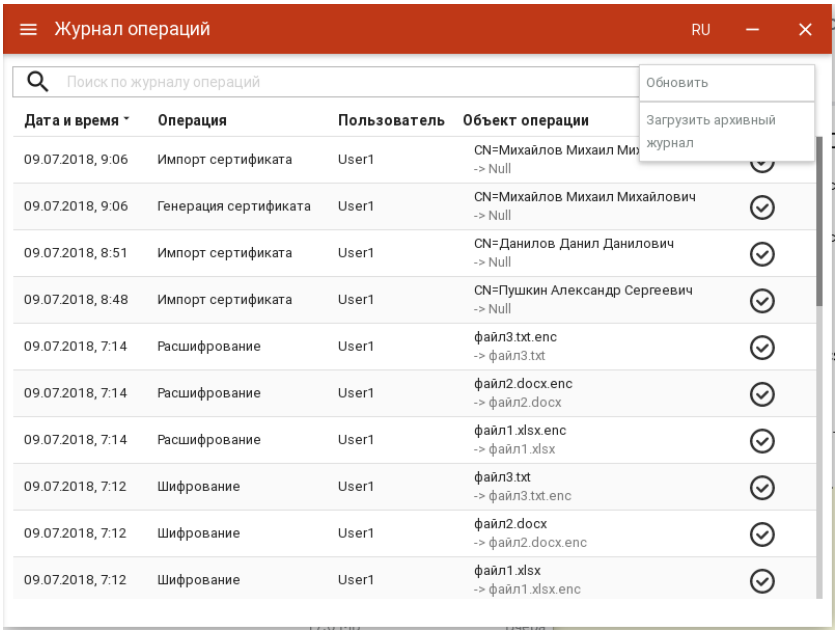


Рис. 8.13.2 Контекстное меню журнала операций

По кнопке «Обновить» контекстного меню происходит обновление записей в журнале операций.

Для возврата к текущему журналу операций используется пункт контекстного меню архивного журнала «Вернуться к текущему журналу» (рис. 8.13.3)

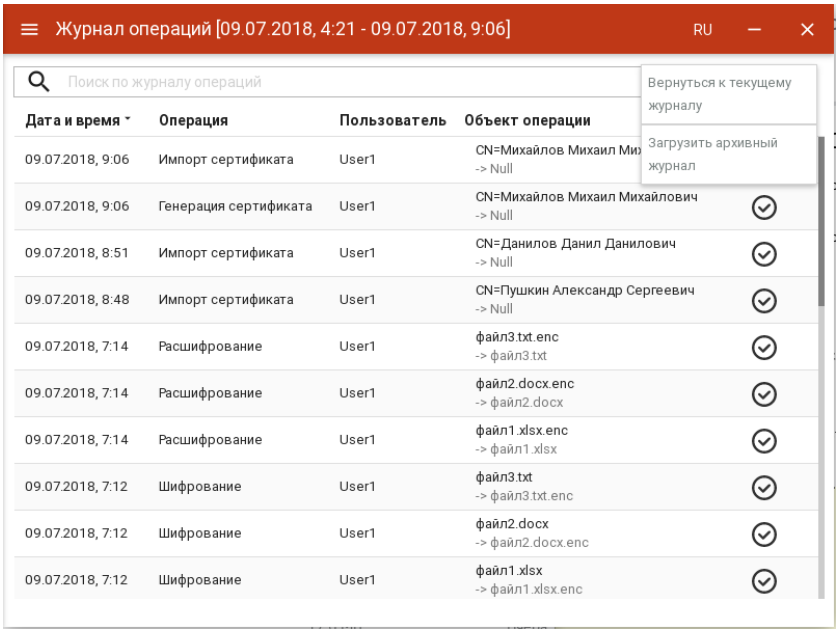


Рис. 8.13.3. Контекстное меню архивного журанала операций

ПОИСК ЗАПИСЕЙ В ЖУРНАЛЕ ОПЕРАЦИЙ. В приложении реализован поиск записей журнала операций по символьному совпадению (рис. 8.13.4)

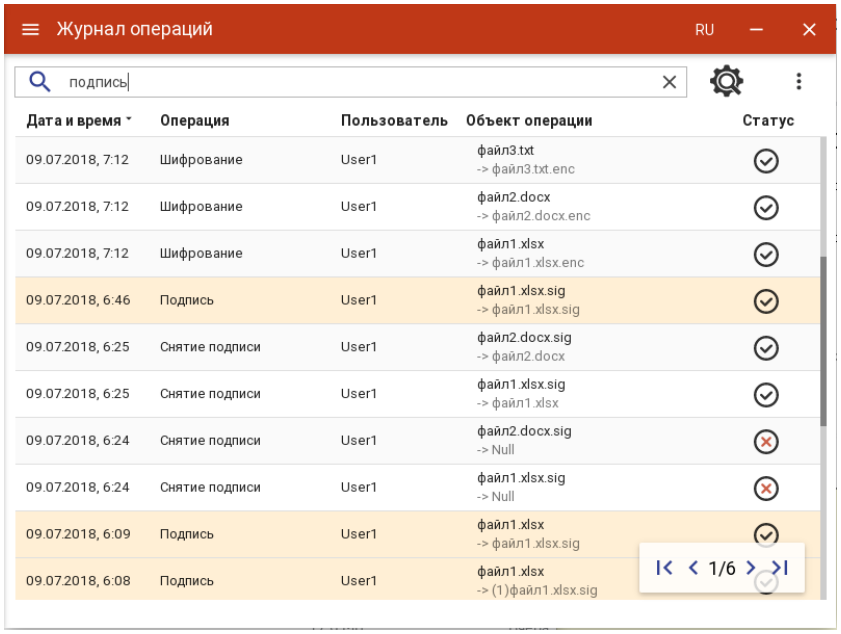


Рис. 8.13.4. Поиск записей в журнале операций

ФИЛЬТРАЦИЯ ЖУРНАЛА ОПЕРАЦИЙ. Для открытия окна настроек критериев фильтра на панели управления имеется кнопка  . При нажатии на кнопку открывается окно настроек фильтрации (рис. 8.13.5).

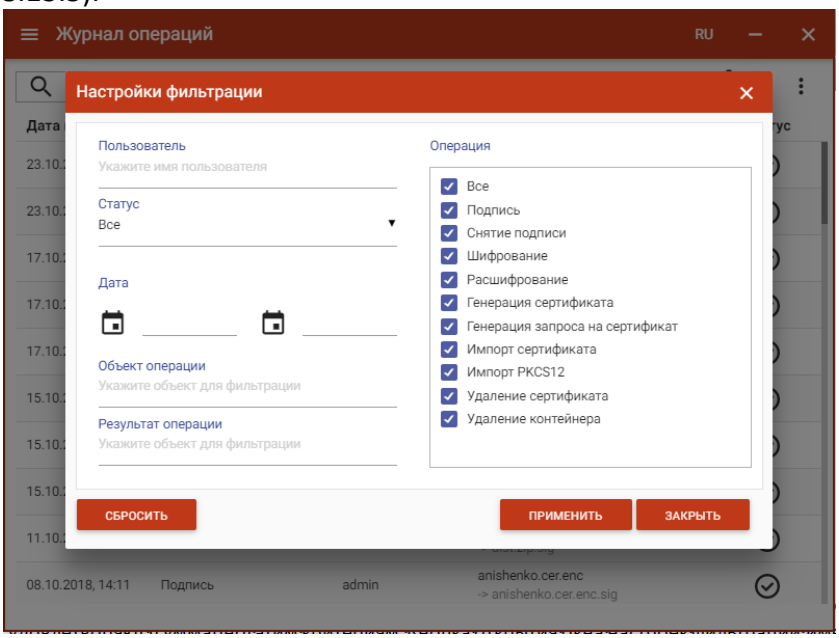


Рис. 8.13.5. Настройки критериев фильтра журнала операций

Применение фильтрации выполняется по нажатию кнопки “Применить”. В зависимости от выставленных критериев фильтра в журнале остаются только те записи, которые удовлетворяют (суммарно) этим критериям. Кнопка открытия окна настроек фильтрации имеет вид  (рис. 8.13.6).

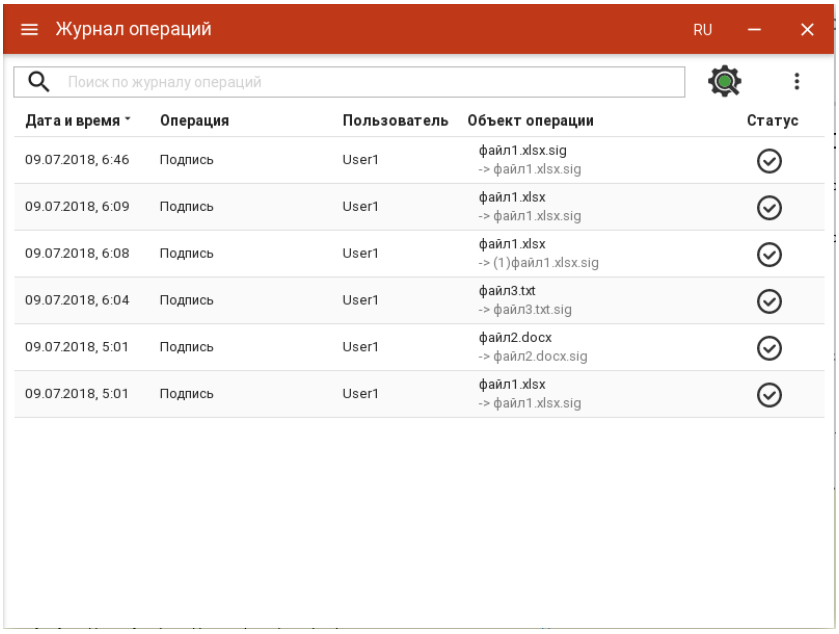


Рис. 8.13.6. Результат применения фильтрации журнала операций

Для сброса заданных критериев фильтрации служит кнопка «Сбросить» в окне настроек фильтрации (рис. 8.13.5).

8.14. Сервисы подписи

В приложении КриптоАРМ ГОСТ организуется интерфейс подключения внешних сервисов, развернутых на основе КриптоПро DSS.

Управление сервисами осуществляется на форме **Сервисы** (рис. 8.14.1).

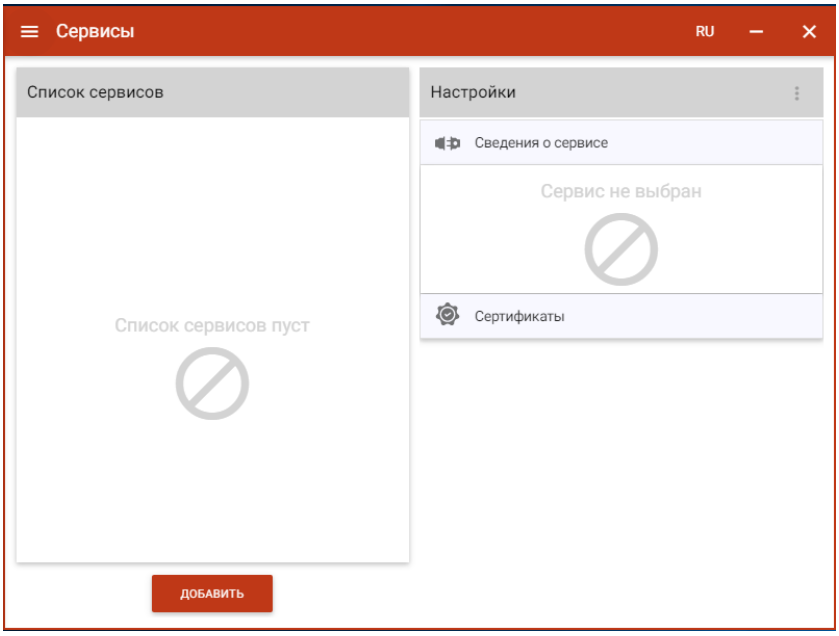


Рис. 8.14.1. Форма управления сервисами подписи

В левой области отображается список подключенных сервисов. В правой области отображается информация о выделенном сервисе.

Создание нового подключения к сервису. При нажатии на кнопку **Добавить** открывается форма ввода параметров подключения: описание, адрес сервера авторизации и адрес сервера подписи (рис. 8.14.2). По умолчанию введены данные для подключения к тестовому сервису подписи КртптоПро DSS.

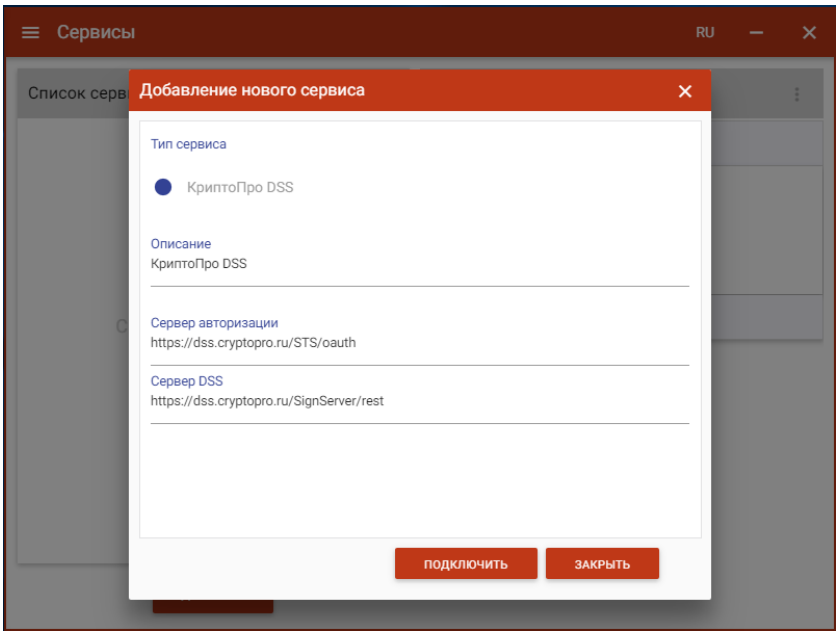


Рис. 8.14.2. Форма ввода параметров подключения к сервису подписи

После нажатия на кнопку **Подключить** и ввода данных для авторизации на сервер DSS происходит создание подключения к сервису. В списке сервисов появляется элемент, при выборе которого открывается детальная информация о настройках подключения (рис.8.14.3) и сертификатах пользователя (в том случае если они доступны для данного пользователя) (рис.8.14.4).

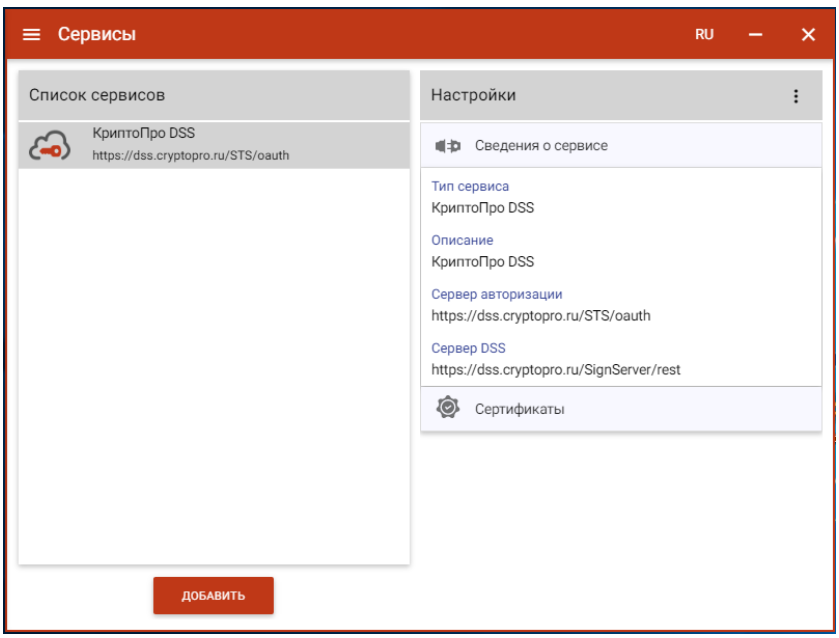


Рис. 8.14.3. Информация о настройках подключения к сервису

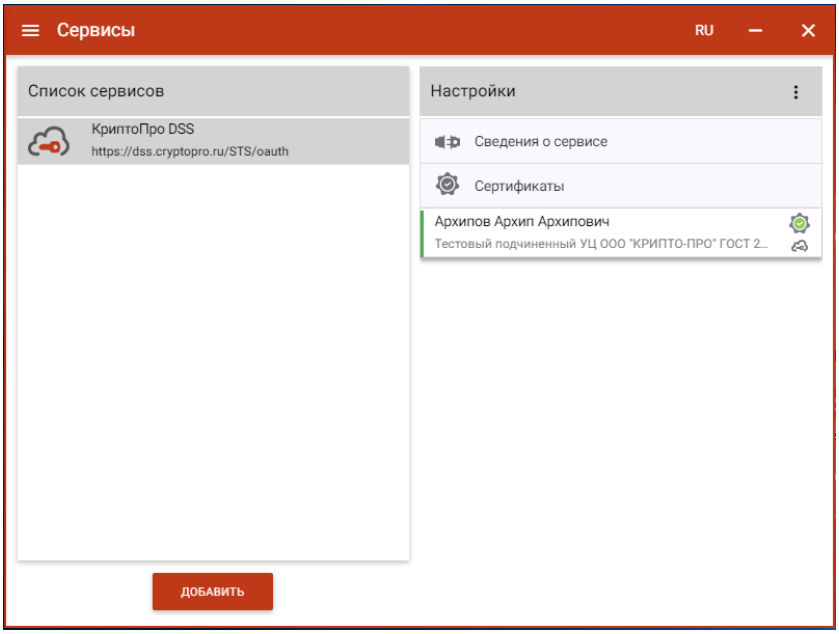


Рис. 8.14.4. Информация о сертификатах пользователя

Для управления подключенным сервисом доступны соответствующие операции в контекстном меню (рис. 8.14.5).

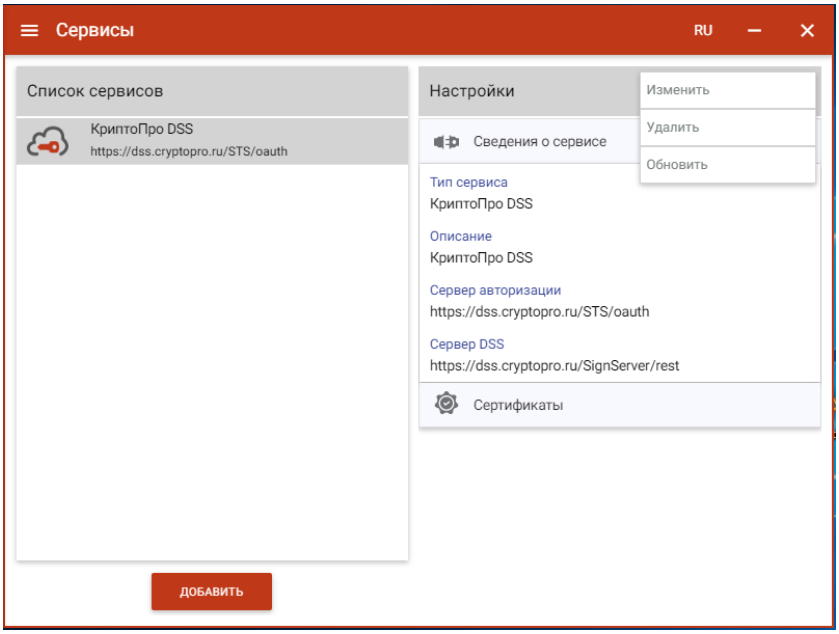


Рис. 8.14.5. Контекстное меню сервиса подписи

Изменение параметров подключения. При выборе в контекстном меню приложения пункта **Изменить** открывается форма редактирования настроек подключения (рис. 8.14.6)

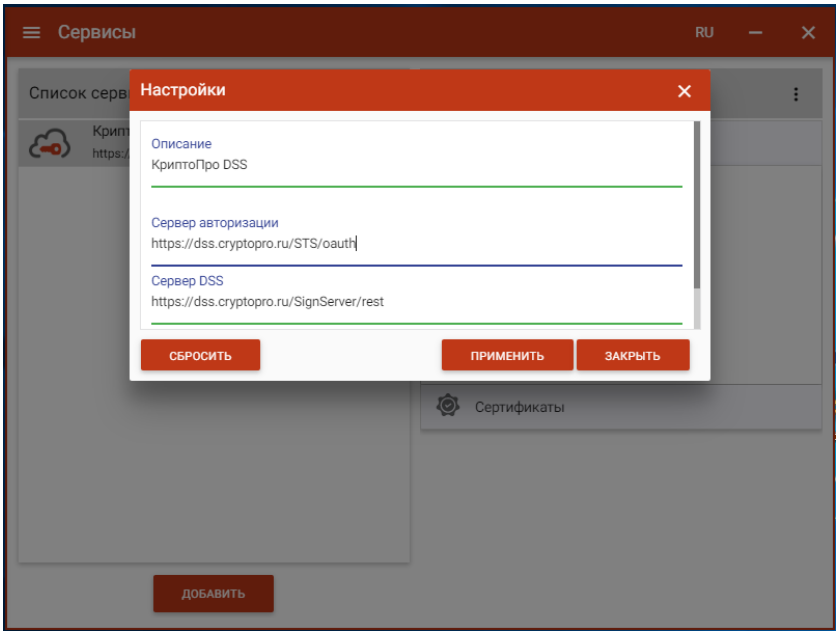


Рис. 8.14.6. Редактирование настроек сервиса

Для редактирования настроек доступны следующие операции:

- **Сбросить** – возвращает данные полей, которые были до редактирования;
- **Применить** – сохраняет изменения и закрывает окно редактирования
- **Закрыть** – закрывает окно редактирования без сохранения изменений.

Удаление подключения. При выборе в контекстном меню приложения пункта **Удалить** открывается окно для подтверждения удаления (рис. 8.14.7)

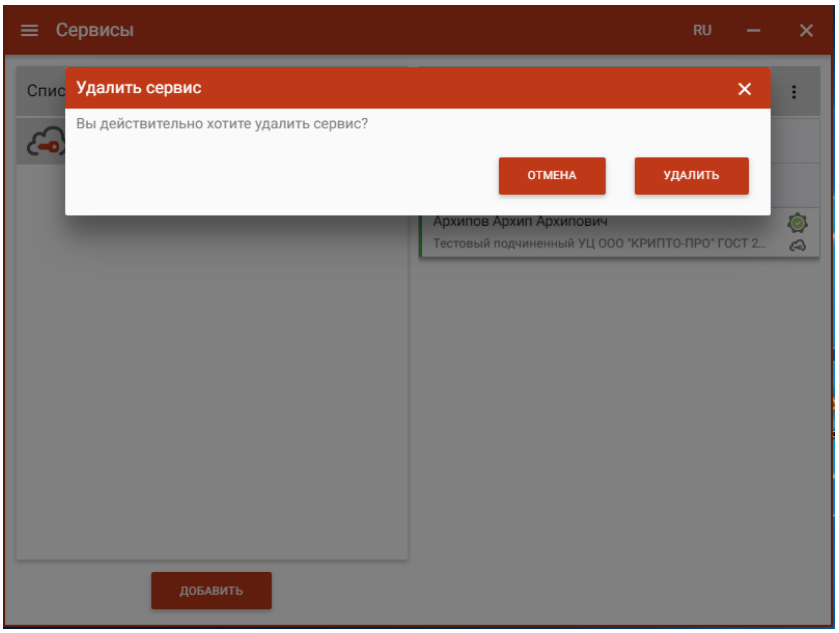


Рис. 8.14.7. Подтверждение удаления подключения

При удалении подключения удаляются сертификаты пользователя, связанные с этим подключением.

Обновление подключения. При выборе в контекстном меню приложения пункта **Обновить** обновляются настройки подключения и сертификаты.

8.15. О программе

Краткие сведения о программе, ссылка на полную документацию пользователя, а также адрес электронной почты для получения дополнительной технической поддержки можно узнать, выбрав в основном меню пункт **О программе** (рис. 8.15.1).

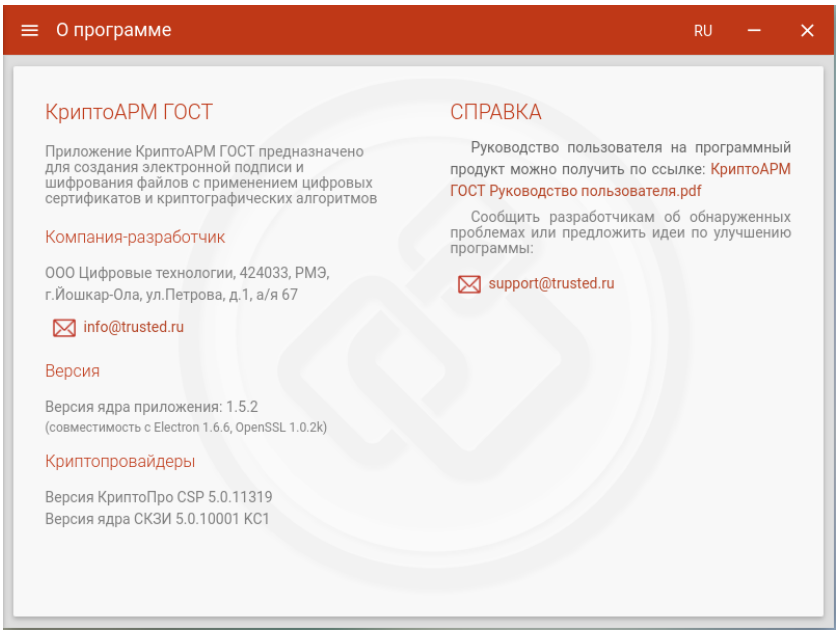


Рис. 8.15.1. Информация о программе

9. Включение режима логирования и консоль управления

Приложение КриптоАРМ ГОСТ построено на основе браузера, в котором исполняются скрипты, написанные на языке JavaScript и отображается интерфейс приложения. Ошибки, которые возникают при работе интерфейсной части приложения, связанные с проблемами подключения модулей и других компонент можно отследить в консоли управления, которую предоставляет браузер.

Открыть браузерную консоль приложения КриптоАРМ ГОСТ можно, запустив приложение из командной строки и указав параметр - devtools. Данная команда открывает окно с инструментарием для веб-разработки, где одной из вкладок будет представление консоли.

Для более глубокого анализа причин возникновения ошибок используется включение режима логирования, то есть сохранение служебной информации о выполненных операциях в текстовый файл. Данный режим включается указанием параметра - logcrypto при запуске приложения из командной строки.

Особенности включения этих режимов при работе с приложением на различных платформах представлены в следующих подраздела.

9.1. Отслеживание ошибок на платформе MS Windows

Для запуска командной строки нажать Win+R. Ввести команду cmd и ОК

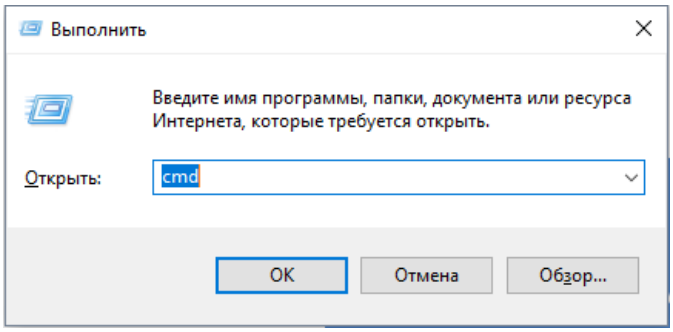


Рис. 9.1.1. Диалог для запуска приложений

В открывшемся окне ввести команду запуска приложения КриптоАРМ ГОСТ (рис. 9.1.2):

"C:\Program Files\CryptoARM GOST\CryptoARM_GOST.exe" devtools logcrypto

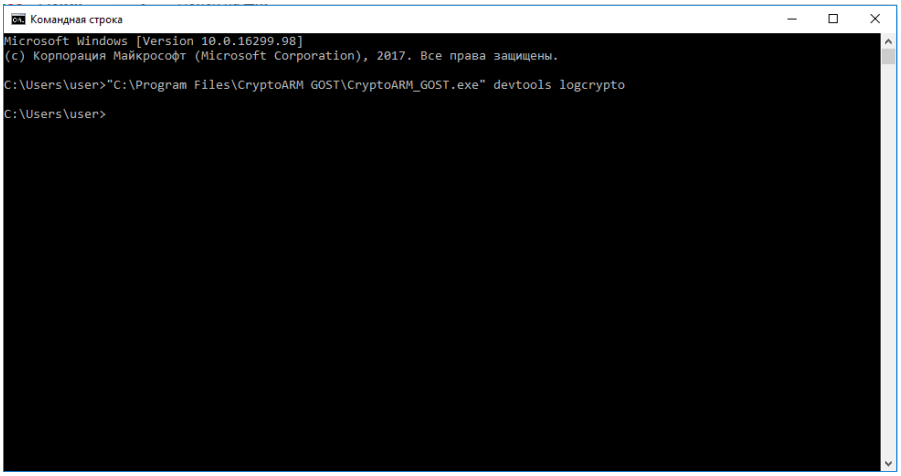


Рис. 9.1.2. Диалог командной строки

В результате выполнения этой команды откроется приложение КриптоАРМ ГОСТ с дополнительной панелью управления, которая представлена на рис. 9.1.3 и сохранением информации об операциях в журнал логирования.

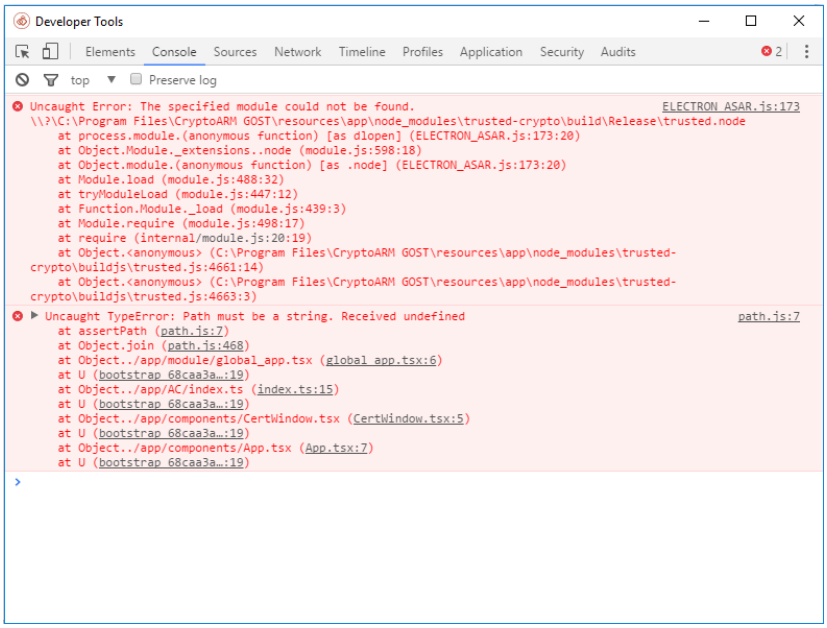


Рис. 9.1.3. Окно с вкладкой консоли управления

При выполнении операции, приводящей к ошибке, в открывшемся дополнительном окне управления на вкладке Console отобразится текст ошибки.

Журнал логирования представляет собой текстовый файл cryptoarm_gost.log, который располагается в каталоге пользователя .Trusted.

9.2. Отслеживание ошибок на платформе Linux

Для получения доступа к дополнительной панели управления приложением и включением режима логирования, в терминале ОС Linux нужно ввести команду (рис. 9.2.1):

/opt/cryptoarm_gost/CryptoARM_GOST devtools logcrypto

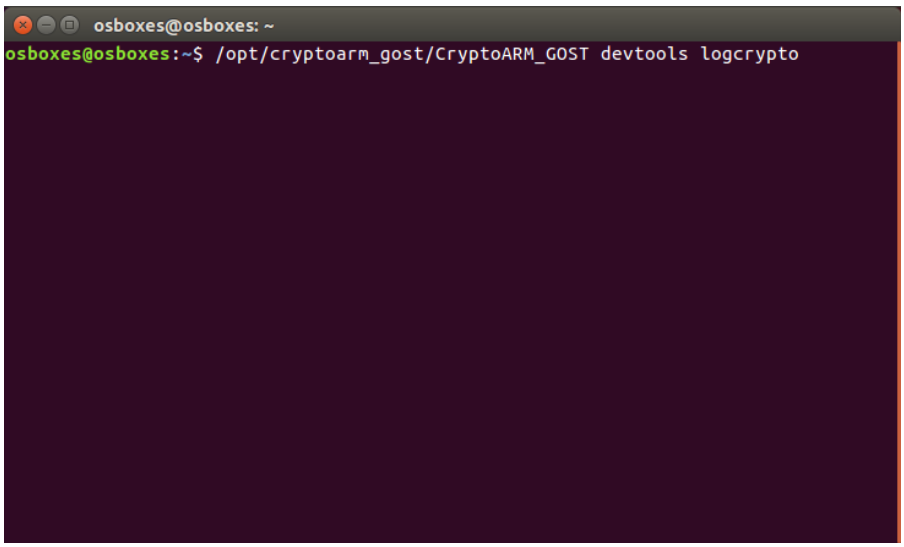


Рис. 9.2.1. Окно терминала

При выполнении операции, приводящей к ошибке, в открывшемся дополнительном окне на вкладке Console отобразится текст ошибки (рис. 9.2.2).

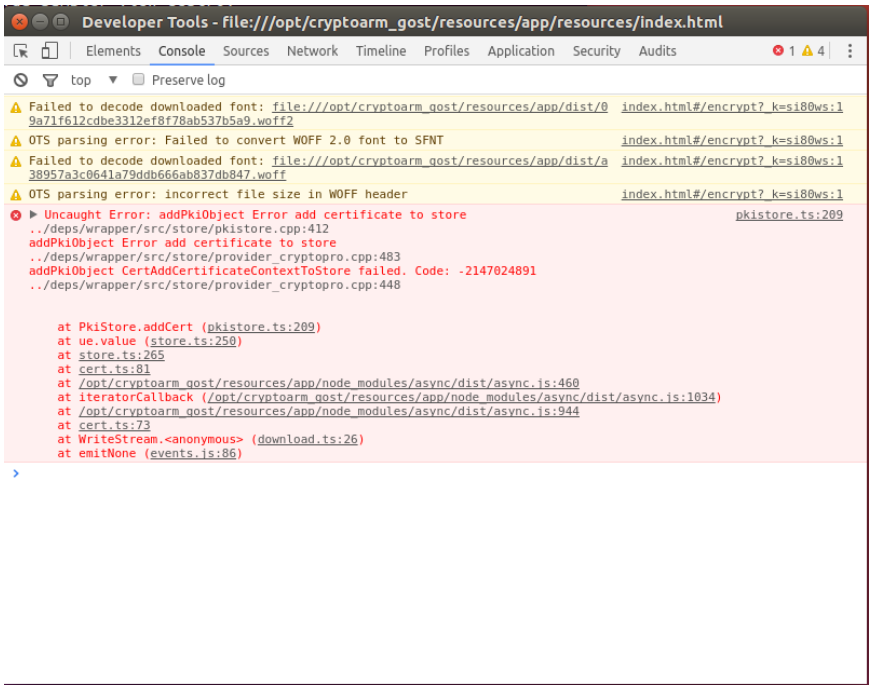


Рис. 9.2.2. Окно с вкладкой консоли управления

При выполнении операции, приводящей к ошибке, в открывшемся дополнительном окне управления на вкладке Console отобразится текст ошибки.

Журнал логирования представляет собой текстовый файл cryptoarm_gost.log, который располагается в каталоге пользователя .Trusted.

9.3. Отслеживание ошибок на платформе OS X

Для получения доступа к дополнительной панели управления приложением и включением режима логирования, в терминале ОС OS X ввести команду (рис. 9.3.1):

/Applications/CryptoARM-GOST.app/Contents/MacOS/CryptoARM_GOST devtools logcrypto

Рис. 9.3.1. Окно терминала

При выполнении операции, приводящей к ошибке, в открывшемся дополнительном окне на вкладке Console отобразится текст ошибки (рис. 9.3.2).

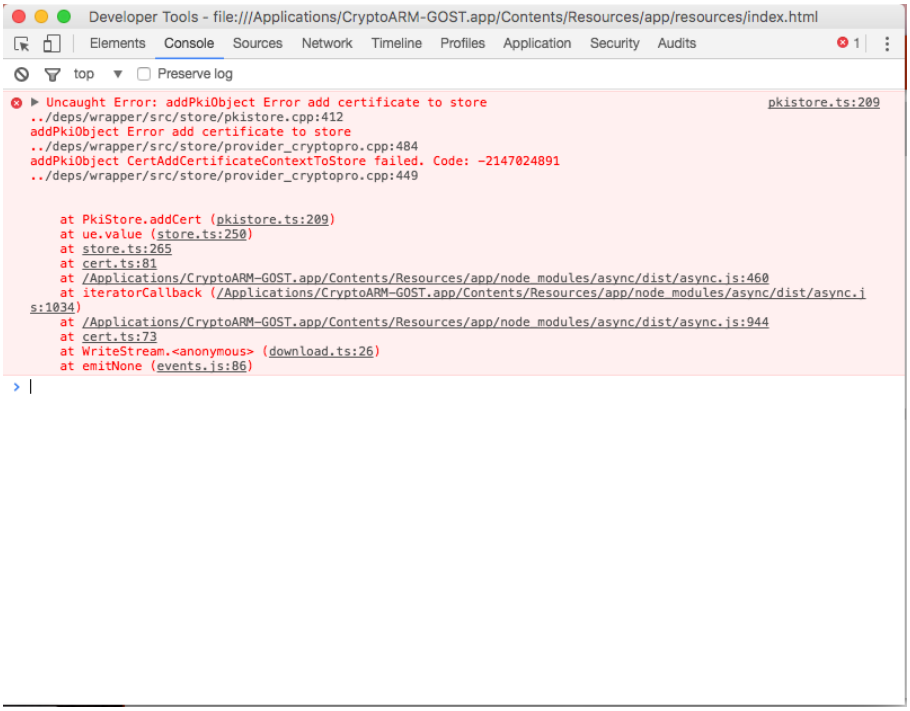


Рис. 9.3.2. Окно с вкладкой консоли управления

При выполнении операции, приводящей к ошибке, в открывшемся дополнительном окне управления на вкладке Console отобразится текст ошибки.

Журнал логирования представляет собой текстовый файл cryptoarm_gost.log, который располагается в каталоге пользователя .Trusted.

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 КриптоАРМ ГОСТ, 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