ESMART®

ESMART PKI Client
Руководство пользователя

Содержание

1. Общая информация

Программа ESMART PKI Client для персонального компьютера предназначена для работы с картами ESMART Token. Смарт-карты ESMART Token представляют собой пластиковые карты, в которые встроена интегральная схема (чип) для хранения и обработки информации. ESMART Token могут быть выпущены в формате USB-ключа, т.е. фактически карта и считыватель объединены в одном корпусе. Устройство и принцип работы подробно описаны в документе ***ESMART Token – Описание*** *и* ***ESMART Token ГОСТ - Описание****.*

Благодаря удобному интуитивно понятному графическому интерфейсу использовать ESMART PKI Client могут как опытные пользователи, так и начинающие. Перед использованием ESMART PKI Client необходимо ознакомиться с руководством.

1.1 Условия использования

ESMART PKI Client поставляется на безвозмездной основе для использования исключительно со смарт-картами ESMART Token и USB-ключами ESMART Token.

ESMART PKI Client не совместим с другими типами смарт-карт или USB-ключей.

Запрещается любым способом пытаться получить исходные коды программы ESMART PKI Client.

1.2 Функционал ESMART PKI Client

- *Просмотр общей информации*
  - *Номер/описание слота;*
  - *Серийный номер токена;*
  - *Производитель;*
  - *Модель токена;*
  - *Память;*
  - *Параметры ПИН-кодов;*
- *Работа с ключами*
  - *Создание ключевой пары RSA;*
  - *Создание ключевой пары ГОСТ (ГОСТ Р 34.10-2001, ГОСТ Р 34.10-2012)*
  - *Создание симметричных ключей (DES, 3DES и AES);*
- *Работа с сертификатами:*
  - *Создание запроса на сертификат;*
  - *Запись сертификата из файлов .cer или .crt;*
- *Работа с данными:*
  - *Запись до 9 блоков произвольных данных;*
- *Работа с контейнерами:*
  - *Импорт ключевой пары и сертификата из файлов;*
- *Электронная подпись файла в формате PKCS#7 и проверка электронной подписи.*

1.3 Преимущества

Программа ESMART PKI Client проста в установке и в работе, имеет интуитивный графический интерфейс. Обучение методам работы с программой не занимает много времени. Для работы с ESMART PKI Client не требуется навык работы с командной строкой.

1.4 Техническая поддержка

*Для получения технической поддержки обратитесь к администратору. Перед обращением в службу поддержки, ознакомьтесь с разделом **Возможные проблемы**.*

2. Установка и удаление

*Установка и удаление приложения ESMART PKI Client выполняется администратором. При необходимости обратитесь к соответствующему разделу документа **ESMART PKI Client – Руководство администратора**.*

3. ПИН-код

ПИН[1]-кодом называют сочетание символов, как правило цифр, но для карт и USB-ключей ESMART Token также могут использоваться алфавитные и служебные символы. Оптимально, надежный пароль должен быть не менее 8 символов и желательно содержать символы минимум 3 типов, например, большие и маленькие буквы и цифры, или буквы, цифры и служебные символы.

Благодаря аппаратной защите ПИН-код может быть проще, т.к. карта защищена от подбора пароля методом перебора. После того как несколько раз был введен неверный пароль, карта блокируется. Получить доступ к хранящимся на заблокированной карте ключам, данным и сертификатам невозможно. Разблокировать карту может администратор, который знает SO PIN.

Требования к ПИН-коду карты должны быть определены на корпоративном уровне и могут быть прописаны во внутренних документах. Ответственность за несоблюдение требований по хранению ПИН-кодов лежит на пользователе. За несоблюдение требований может налагаться штраф.

Не следует записывать ПИН-коды на листках бумаги, в ежедневнике или на стикерах, которые могут находиться на виду на рабочем месте. Если рекомендуемый требованиями ПИН-код карты длинный и сложный и его невозможно запомнить с первого раза, уберите записанный ПИН-код в запирающийся ящик стола. Запомнив ПИН-код, уничтожьте листок бумаги.

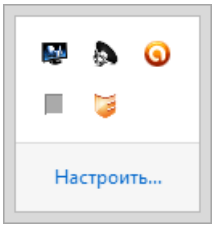
*Чтобы посмотреть требования к ПИН-коду, откройте окно настроек, см. раздел **Настройки**.*

В соответствии с Правилами пользования[2] СКЗИ ESMART Token ГОСТ, необходимо менять ПИН-код пользователя не реже, чем 1 раз в 6 месяцев.

4. Запуск программы

4.1 Запуск в Windows

Запустите программу двойным щелчком на иконке программы. Для удобства запуска можно создать ярлык и поместить его на Рабочий стол.



Если свернуть окно приложения, приложение не выключается, а сворачивается в трей (область в правом углу панели задач). Чтобы развернуть окно программы, щелкните один раз по иконке программы левой кнопкой мыши.

4.2 Запуск в Linux

Метод запуска программы в Linux зависит от используемой графической оболочки.

---

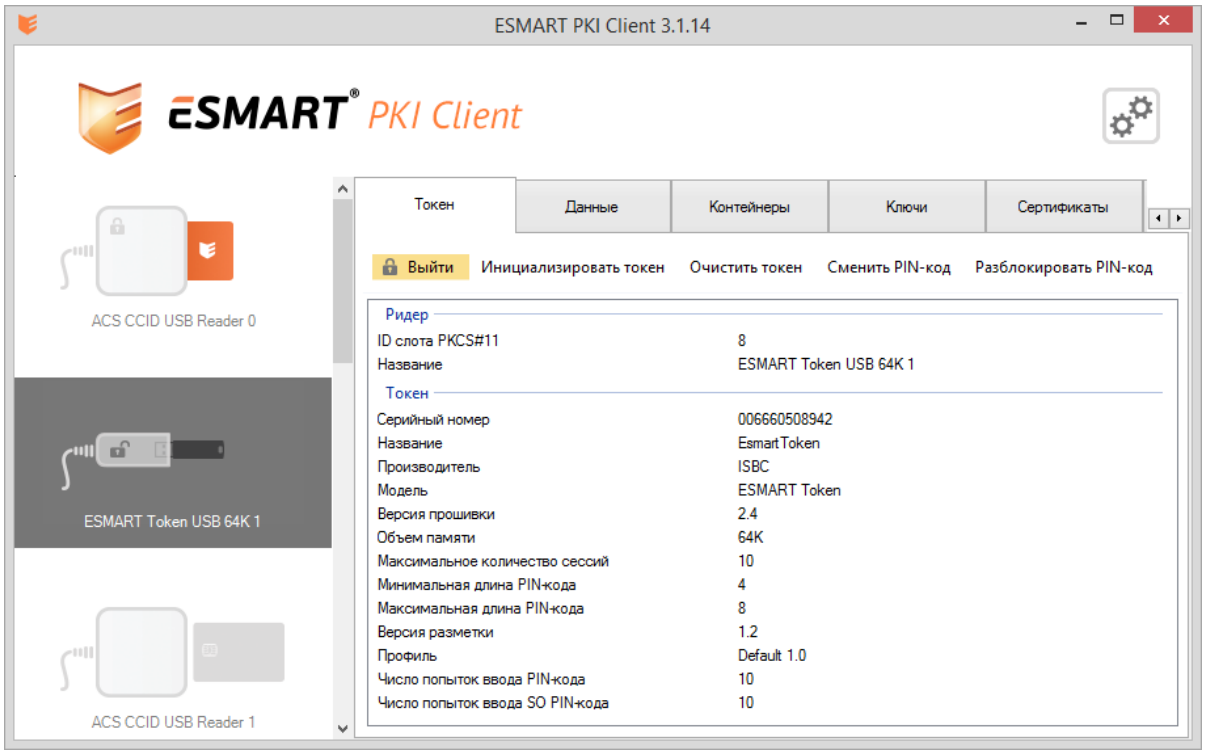
[1] *От англ. PIN code – Personal Identification Number – Персональный идентификационный номер*

[2] *Правила пользования конкретного СКЗИ можно получить, отправив запрос на esmart@isbc.ru с указанием ID СКЗИ чипа, даты приобретения и юр. лица покупателя.*

Запустите программу, щелкнув мышкой по иконке.

Для запуска программы также можно щелкнуть по иконке программы правой кнопкой мыши и в контекстном меню выбрать Open with Mono… Если программа не открывается или опция не доступна, обратитесь к администратору.

5. Интерфейс



Интерфейс программы поделен на 3 отдельных области:

1. *Шапка с логотипом, названием программы и кнопкой вызова настроек;*
2. *На левой панели отображается список подключенных считывателей и USB-ключей;*
3. *Основная панель состоит из нескольких вкладок, каждая подробно описана в следующем разделе.*

6. Вкладки основной панели

6.1 Вкладка Токен

*На вкладке **Токен** отображаются основные данные о выбранном в левой панели USB-ключе или смарт-карте ESMART Token. Также на вкладке есть кнопки **Авторизоваться** и **Выйти**. Авторизация подразумевает ввод ПИН-кода пользователя. После авторизации пользователь может видеть объекты типа private и удалять объекты. См. раздел **Порядок работы**.*

6.2 Вкладка Данные

*На вкладке **Данные** можно создать новые данные и просмотреть ранее созданные блоки данных. На ESMART Token может храниться до 9 блоков данных.*
*См. раздел **Данные**.*

6.3 Вкладка Контейнеры

*На вкладке **Контейнеры** можно загрузить ключевую пару и соответствующий сертификат из файлов .p12 или .pfx. См. раздел **Контейнеры**.*

6.4 Вкладка Ключи

*Вкладка **Ключи** предназначена для генерации ключевой пары для ассиметричного шифрования и симметричного. См. раздел **Ключи**.*

Поддерживаемые типы:

- *Ключевая пара RSA – асимметричное шифрование;*
- *Ключевая пара ГОСТ – асимметричное шифрование[3];*
- *Симметричный ключ (AES, DES, 3DES, 3KDES).*

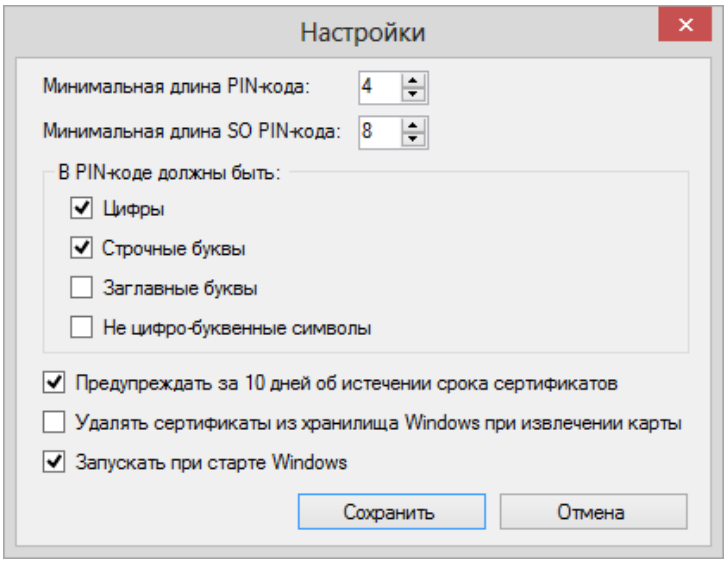
6.5 Вкладка Сертификаты

*Во вкладке **Сертификаты** показаны сертификаты, которые не принадлежат ни одной ключевой паре, например корневые сертификаты УЦ или сертификаты коллег и партнеров. См. раздел **Сертификаты**.*

[3] *Только для ESMART Token GOST*

7. Настройки

Раздел настроек предназначен для изменения параметров программы.



Первоначальная настройка программы выполняется администратором в соответствии с корпоративными требованиями. Пользователям в большинстве случаев не рекомендуется изменять настройки самостоятельно.

При необходимости обратитесь к соответствующему разделу руководства администратора.

8. Задачи пользователя

- *Ознакомиться с руководством пользователя;*
- *Получив карту, сменить ПИН-код пользователя;*
- *Использовать карту для входа в домен и/или электронной подписи и шифрования.*

Использование ESMART Token в офисных программах и почтовых клиентах описано в руководстве ***ESMART Token – ЭЦП и шифрование в Windows****.*

В соответствии с корпоративными требованиями, пользователь может выполнять некоторые задачи администратора самостоятельно, например, генерацию ключевой пары и создание запроса на сертификат. В этом случае рекомендуется также ознакомиться с руководством администратора.

9. Порядок работы

9.1 Подготовка к работе

Для использования программы требуется, чтобы администратором (или самим пользователем) были проведены следующие предварительные этапы:

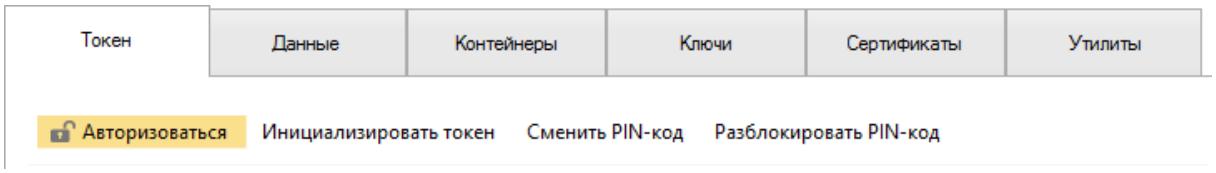
4. *Считыватель для смарт-карт или USB-ключ подключен к ПК.*
5. *Драйвер для считывателя смарт-карт или драйвер USB-ключа ESMART Token установлен в операционной системе и функционирует нормально.*
6. *На ПК пользователя установлен пакет ESMART PKCS11 и CSP в соответствии с выбранной операционной системой.*
7. *Установлено приложение ESMART PKI Client.*
8. *Произведена настройка программы.*

На предварительном этапе администратором на карту уже может быть записан действующий сертификат, выданный корпоративным УЦ.

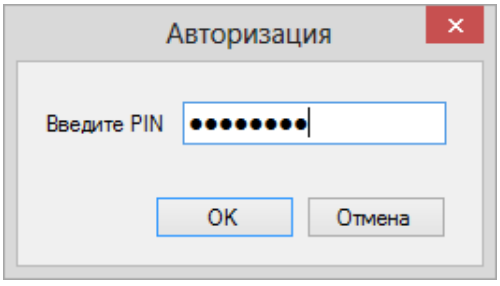
9.2 Регистрация на карте

Регистрацией на карте называется ввод действующего ПИН-кода. Без ввода ПИН-кода карты пользователь может видеть только служебную информацию о карте, основные объекты, объем доступной и занятой памяти, характеристики ПИН-кода и другую информацию.

*Чтобы зарегистрироваться на карте, нажмите **Авторизоваться** на верхней панели:*

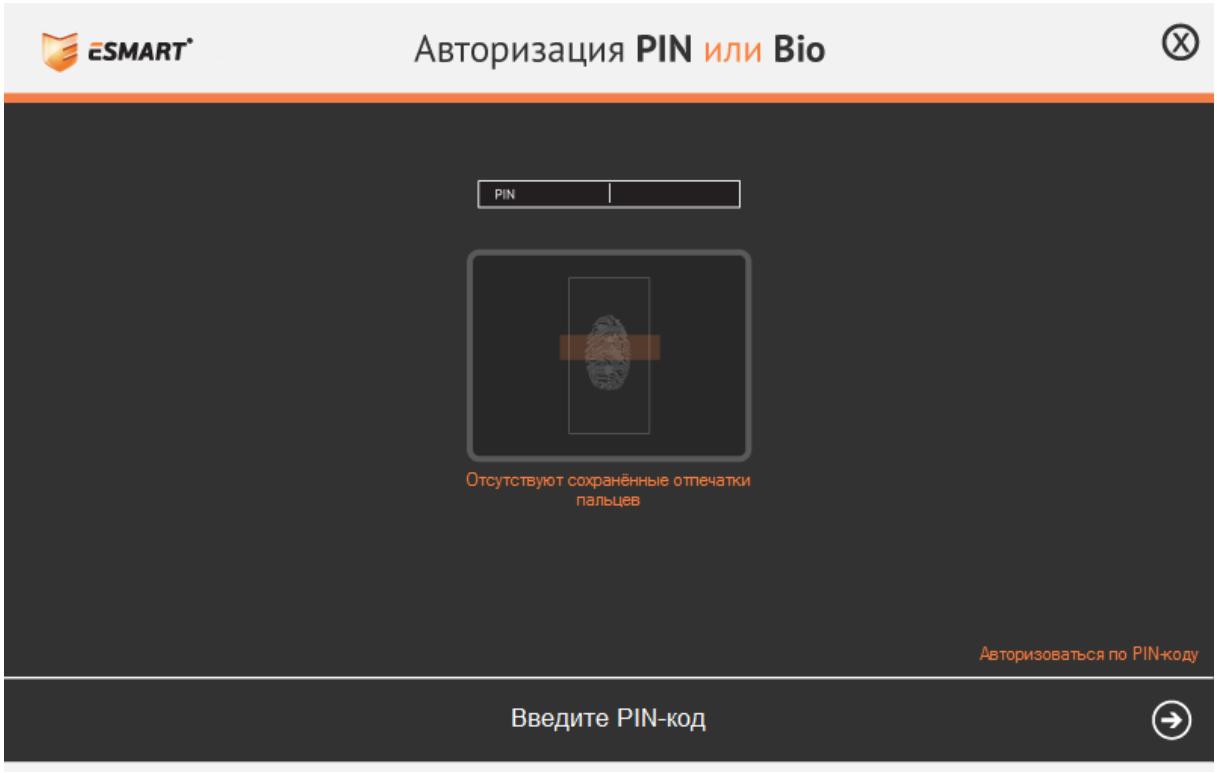


В появившееся окошко введите ПИН-код пользователя.



Авторизовавшись на карте, пользователь получает доступ к защищенным объектам, получает возможность создавать, импортировать и удалять объекты.

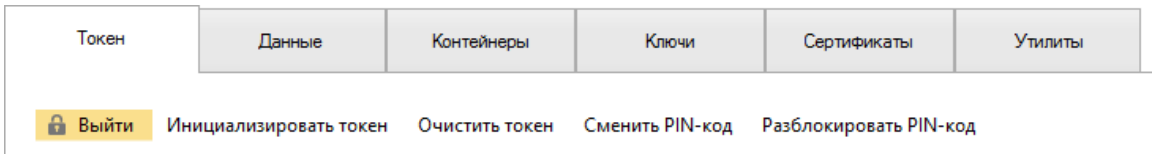
Для ESMART Token ГОСТ будет показано другое окно авторизации:



Подробно возможность входа по отпечатку пальца на ESMART Token ГОСТ описана в руководстве ***ESMART PKI Client – Биометрическая аутентификация.***

9.3 Завершение сеанса

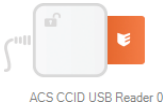
Для завершения сеанса, нажмите кнопку ***Выйти*** *на верхней панели.*



9.4 Обозначение режима

В левой панели показаны все считыватели и статус карт, вставленных в считыватели.

Смарт-карта вставлена в считыватель, но пользователь не зарегистрировался, т.е. не ввел ПИН-код. Большинство возможностей в данном режиме не доступно.



Смарт-карта вставлена в считыватель, пользователь ввел ПИН-код и ему доступны все пользовательские функции.

USB-ключ вставлен в считыватель, но пользователь не зарегистрировался, т.е. не ввел ПИН-код. Большинство возможностей в данном режиме не доступно.

USB-ключ вставлен в считыватель, пользователь ввел ПИН-код и ему доступны все пользовательские функции.

Считыватель подключен, но в считывателе нет карты.

Вставлена несовместимая смарт-карта или карта вставлена неверно.

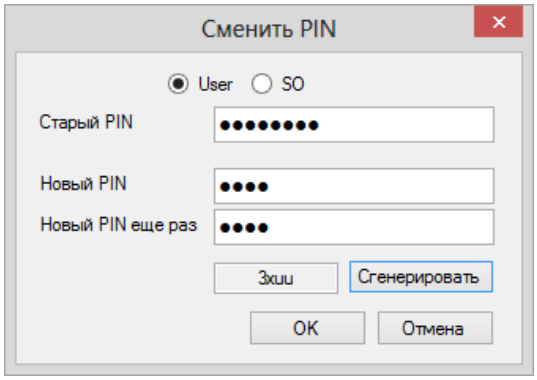
9.5 Инициализация

Инициализация USB-ключа или карты ESMART Token входит в обязанности администратора. Для инициализации требуется SO PIN карты.

***Внимание!** Если неверно ввести SO PIN несколько раз подряд, карта будет **заблокирована без возможности восстановления**. Количество неверных попыток задает администратор.*

9.6 Смена ПИН-кода пользователя (User PIN)

*Нажмите **Сменить ПИН** в верхней панели. В появившемся окне отметьте **User**, введите текущий ПИН-код и два раза новый ПИН-код. Нажмите **ОК**.*

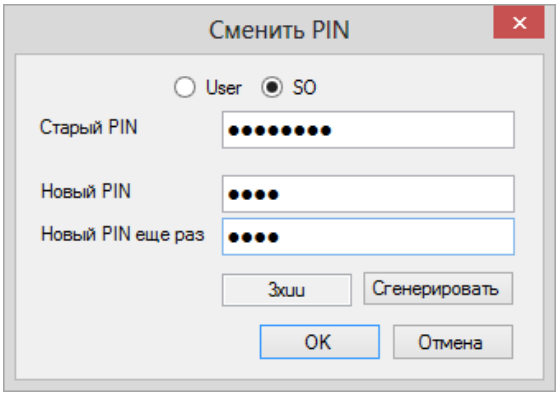


*ПИН-код, соответствующий требованиям, заданным в настройках, можно сгенерировать автоматически. Нажмите **Сгенерировать**. Новый автоматически сгенерированный ПИН-код будет автоматически подставлен в поля ввода и в открытом виде появится в поле. Чтобы сгенерировать новый ПИН-код, нажмите на кнопку еще раз.*

Если новый ПИН-код не соответствует условиям, заданным в настройках программы, появится предупреждение в виде красной иконки с восклицательным знаком.

Подобрав или сгенерировав подходящий ПИН-код, нажмите ОК, чтобы сменить ПИН-код пользователя.

9.7 Смена ПИН-кода администратора



Вкладка SO позволяет сменить ПИН-код администратора карты. Требуется ввод текущего действительного ПИН-кода администратора.

Внимание! *Если неверно ввести SO PIN несколько раз подряд, карта будет* ***заблокирована без возможности восстановления****. Количество неверных попыток задает администратор.*

9.8 Разблокировка ПИН-кода пользователя

Если пользователь ввел неверный ПИН-код несколько раз подряд, карта блокируется. Данные на карте при блокировке карты не удаляются. Чтобы разблокировать карту, требуется ввести SO PIN. Количество неверных попыток ввода ПИН-кода задает администратор.

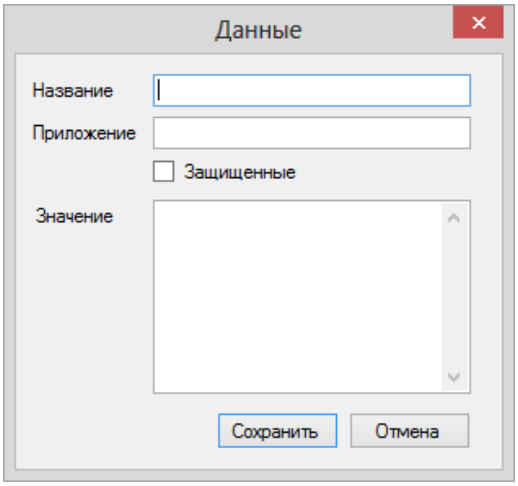
Внимание! *Если неверно ввести SO PIN несколько раз подряд, карта будет* ***заблокирована без возможности восстановления****. Количество неверных попыток задает администратор.*

10. Данные

На карте ESMART Token может храниться небольшой объем текстовой информации. На карте ESMART Token можно хранить логины и пароли, важную контактную информацию, важные заметки и другие конфиденциальные данные. Данные хранятся в так называемых блоках, каждый из которых имеет определенную структуру, описанную ниже.

ESMART Token позволяет хранить максимум 9 блоков данных.

10.1 Блоки данных



Поле	Описание	Наличие	Редактирование
Название	*Название отображается в списке и служит для поиска блока*	*Обязательно*	*Можно отредактировать, если пользователь авторизован на карте*
Приложение	*Любая информация, которую не требуется менять, например, адрес электронной почты или логин*	*Не обязательно*	*Задается только при создании блока данных, при редактировании не изменяется*
Значение	*Информация, которую требуется защитить. Не отображается в списке. Просмотр возможен только после ввода ПИН-кода*	*Не обязательно*	*Можно отредактировать, если пользователь авторизован на карте*

10.2 Типы блоков данных

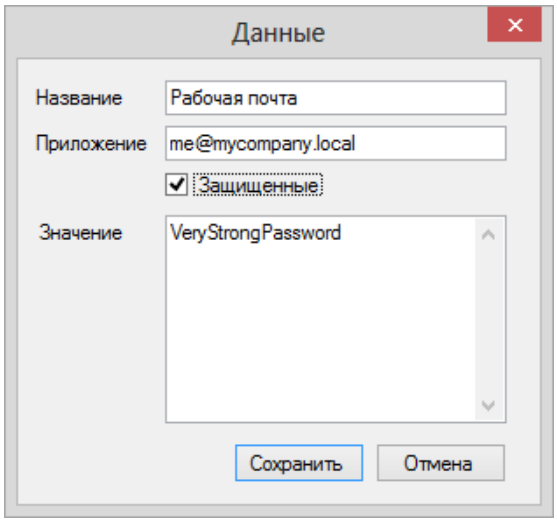
Для хранения текстовой информации на карте ESMART Token можно выбрать один из двух вариантов блоков данных:

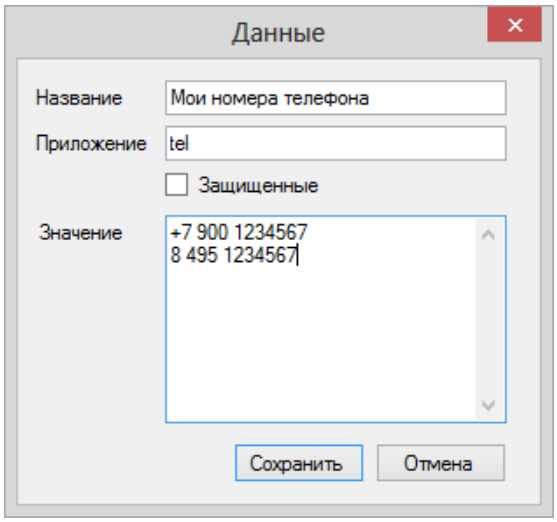
Защищенные данные

*Поля блока **Название** и **Приложение** не отображаются в списке, если пользователь не авторизован на карте.*

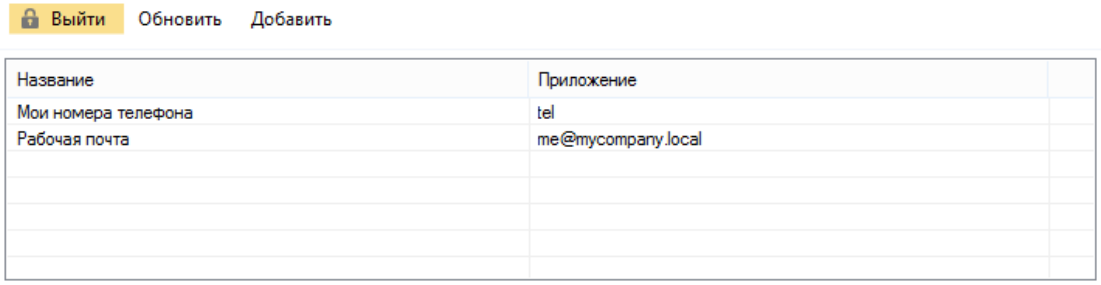
Обычные данные

*Поля блока **Название** и **Приложение** отображаются в списке, если пользователь не авторизован на карте. Для просмотра данных из поля Значение требуется авторизация на карте.*

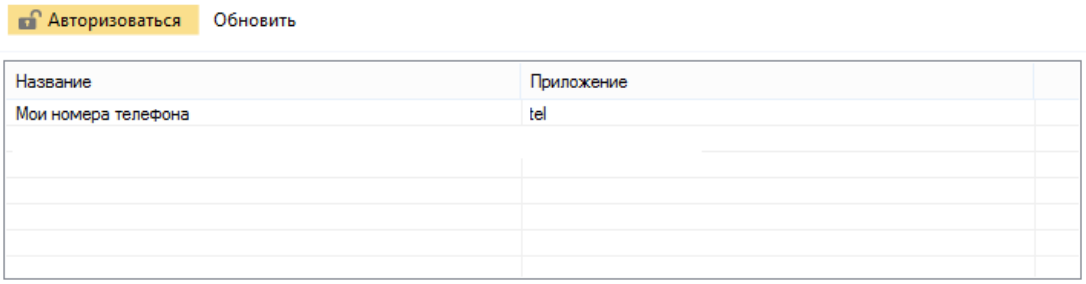




Если пользователь авторизован на карте, в списке присутствуют блоки данных обоих типов:

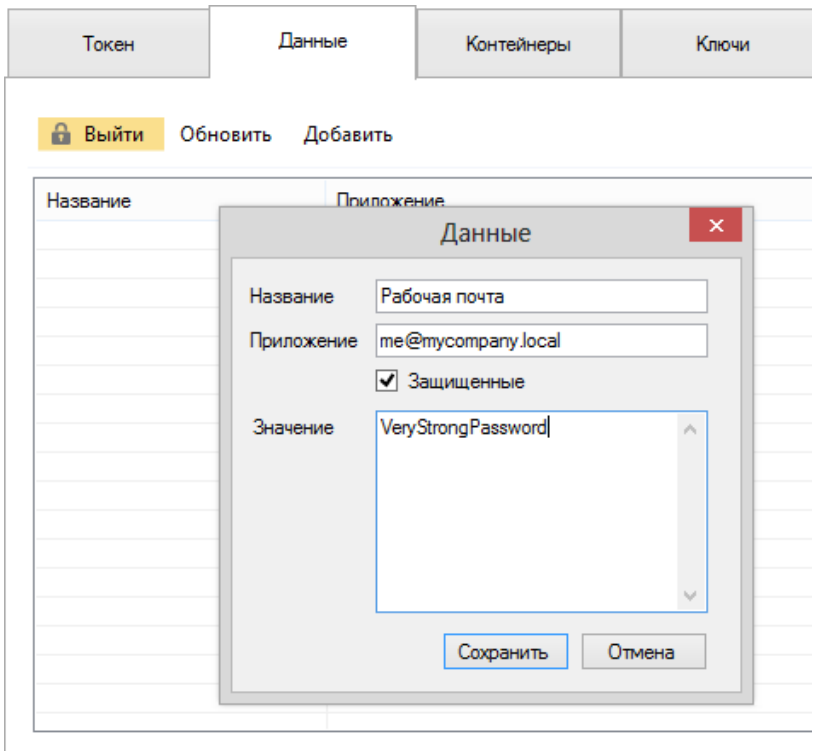


Если пользователь не авторизован на карте, в списке присутствуют только обычные блоки данных:

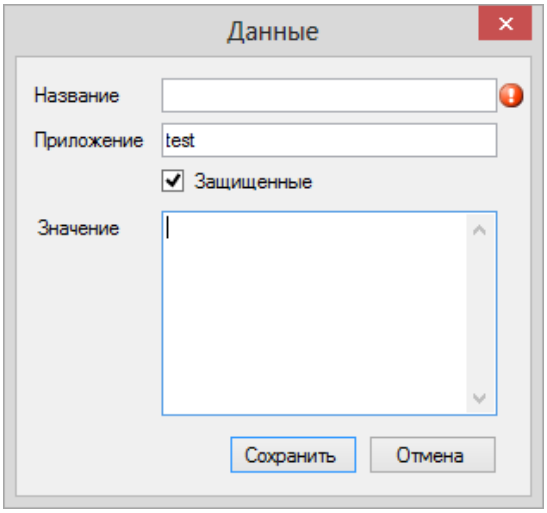


10.3 Добавление данных

*Чтобы добавить на карту текстовую информацию, откройте на верхней панели вкладку **Данные**. Нажмите **Добавить**. Заполните форму. См. раздел Типы блоков данных.*

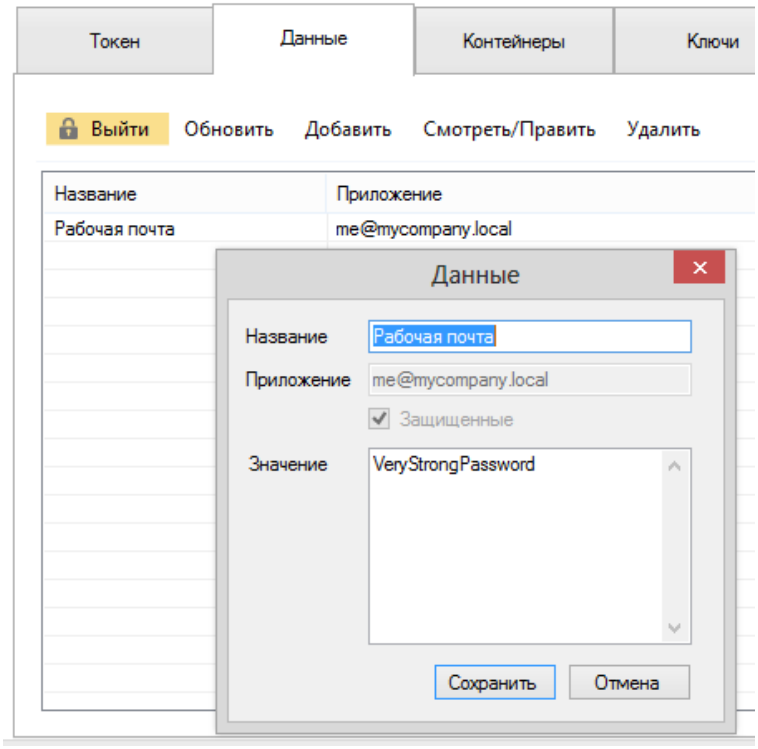


*Поле **Название** является обязательным для заполнения.*



10.4 Редактирование данных

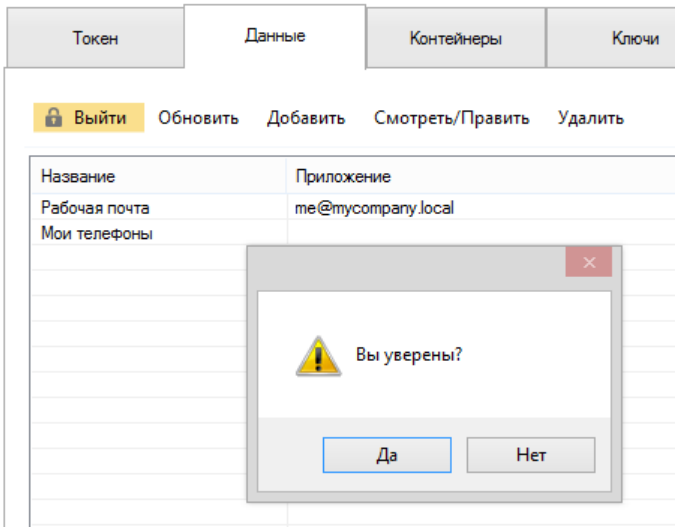
*Чтобы отредактировать данные, выберите в списке нужный блок и нажмите **Смотреть/Править**. В появившемся окне сделайте нужные изменения и нажмите **Сохранить**.*



*Значение поля **Приложение**, а также тип данных (Защищенные/Обычные) изменить невозможно. Создайте блок заново с требуемыми параметрами.*

10.5 Удаление данных

*Чтобы удалить блок данных, выберите его в списке и нажмите **Удалить**. Подтвердите выполнение операции.*



***Внимание!** Восстановить удаленные данные невозможно.*

11. Контейнеры

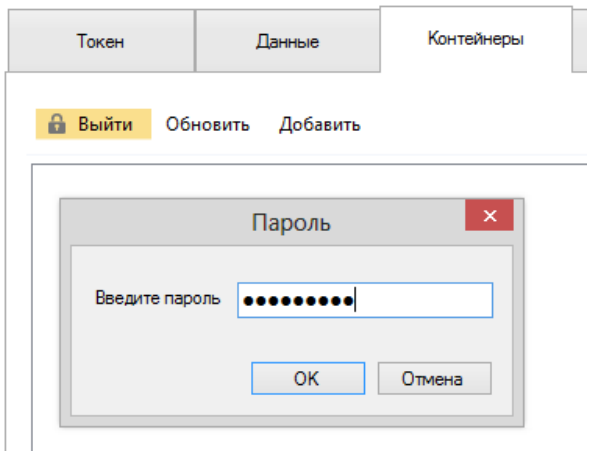
Под Контейнером понимают хранение на карте связанных объектов:

- *Сертификата X.509;*
- *Ключевой пары (RSA или ГОСТ), состоящей из*
  - *открытого ключа;*
  - *закрытого ключа.*

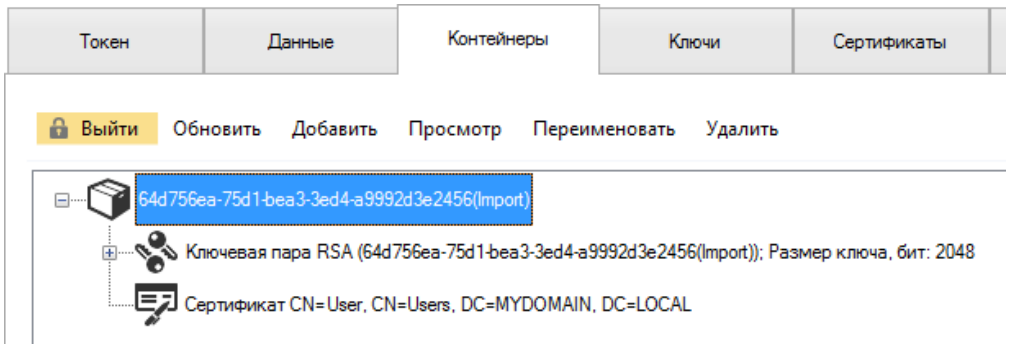
11.1 Добавление контейнера

На карту ESMART Token можно добавить все объекты контейнера из файла PKCS#12 (форматы файлов .p12 или .pfx).

Чтобы загрузить на карту контейнер из файла .p12 или .pfx, нажмите ***Добавить*** *и укажите путь к файлу. В появившемся окне введите пароль к файлу с ключевой парой и сертификатом. Если пароль к файлу не известен, его содержимое нельзя загрузить на карту.*



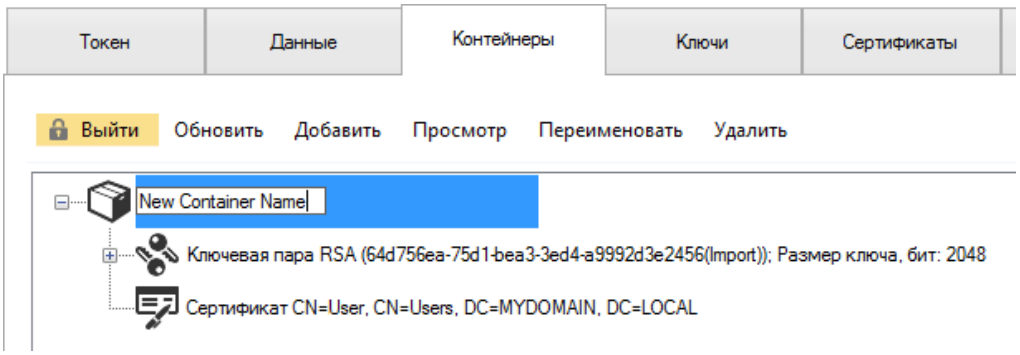
Содержимое файла (ключевая пара и сертификат) будут записаны на карту.



После того как содержимое контейнера перенесено на карту, рекомендуется удалить файл .p12 или .pfx. Если файл требуется сохранить в качестве резервной копии, примите меры для обеспечения безопасности файла.

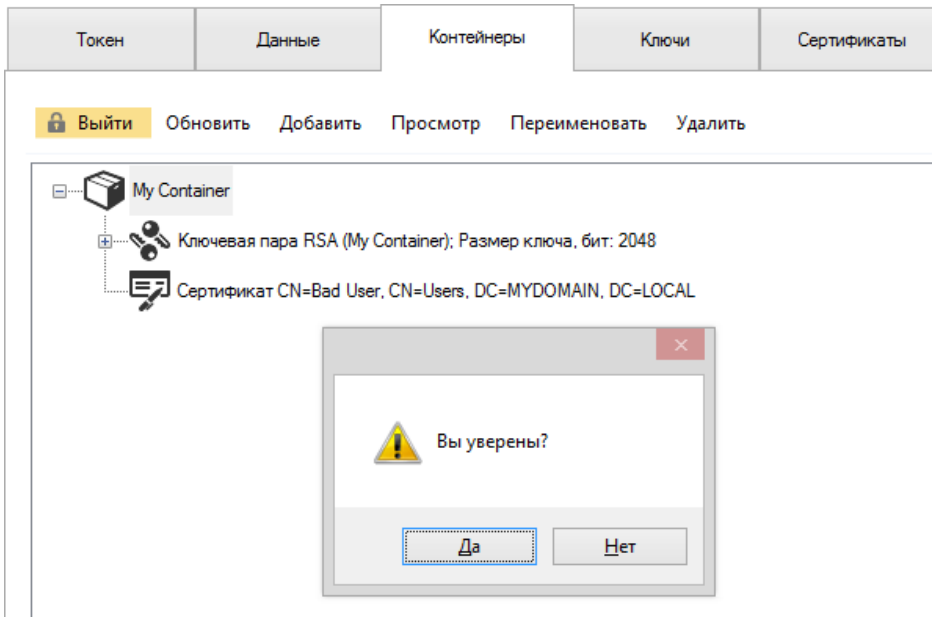
11.2 Переименование контейнера

*Чтобы было удобнее использовать список, контейнеры можно переименовать. Чтобы переименовать контейнер, выделите его и нажмите **Переименовать**. В поле для редактирования введите новое название. Нажмите на клавиатуре **Ввод (Enter)**.*



11.3 Удаление контейнера

*Чтобы удалить контейнер, выделите его и нажмите **Удалить**. Подтвердите операцию.*



***Внимание!** Восстановить удаленный контейнер невозможно. Ключевая пара и соответствующий сертификат будут стерты с карты без возможности восстановления.*

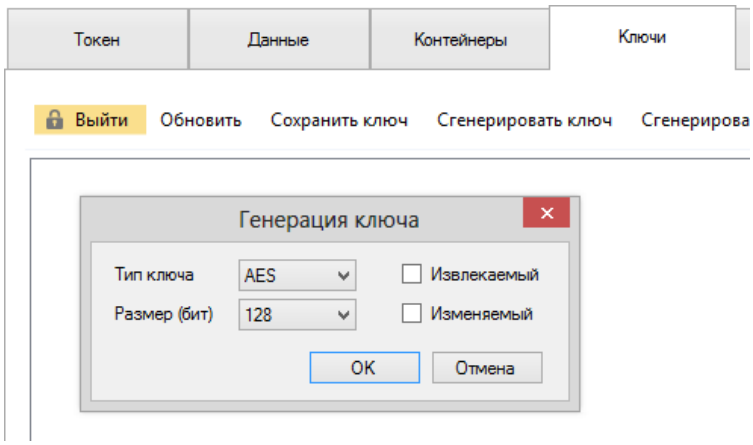
Контейнер на карту можно импортировать повторно, если имеется файл PKCS#12 (формат .pfx или .p12).

12. Ключи

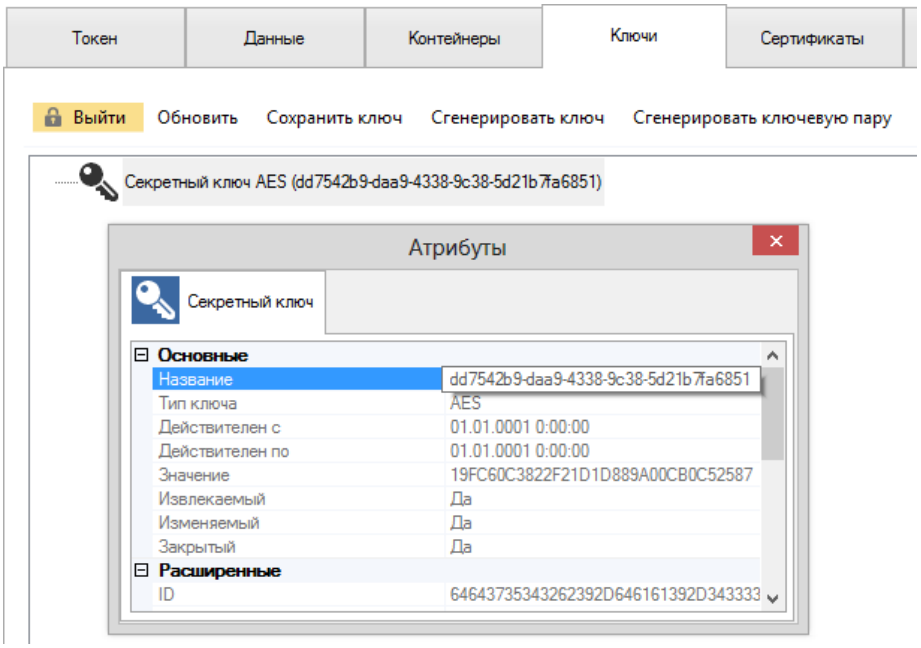
Вкладка предназначена для работы с ключами для симметричного шифрования (DES, 3DES, 3KDES и AES) и ключевыми парами RSA и ГОСТ для асимметричного шифрования.

12.1 Генерация ключа симметричного шифрования (DES, 3DES, AES)

*Для генерации ключей симметричного шифрования, нажмите **Сгенерировать ключ**. В появившемся окне выберите тип ключа и нажмите **ОК**.*

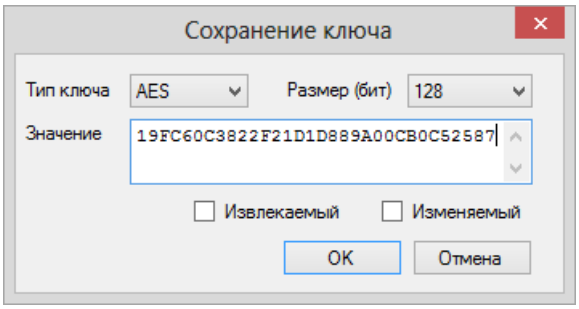


*Чтобы просмотреть данные ключа, выберите ключ из списка и нажмите **Просмотр**.*



12.2 Сохранение ключа

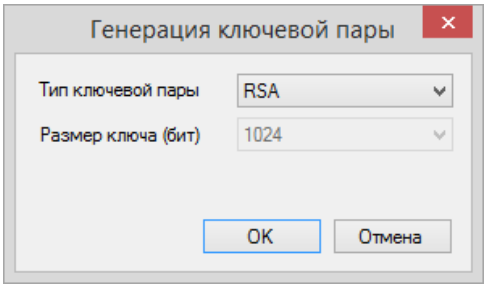
*Чтобы записать на карту существующий ключ симметричного шифрования DES, 3DES, 3KDES или AES, нажмите **Сохранить ключ**. Вставьте в поле значение ключа и нажмите **ОК**.*

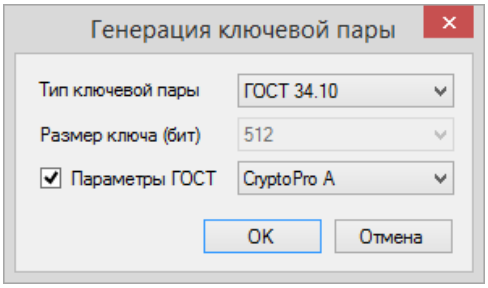


12.3 Генерация ключевой пары

Ключевая пара RSA, состоящая из открытого и закрытого ключей, которые связаны математически, применяется в асимметричном шифровании. Доступ к закрытому ключу должен иметь только его владелец, а открытый ключ пары можно свободно распространять.

*Нажмите **Сгенерировать ключевую пару**, выберите алгоритм ключевой пары (ГОСТ 34.10 или RSA) и размер ключа. Для ключевой пары по алгоритму ГОСТ также можно указать параметры эллиптической кривой (для обеспечения совместимости ключей).*





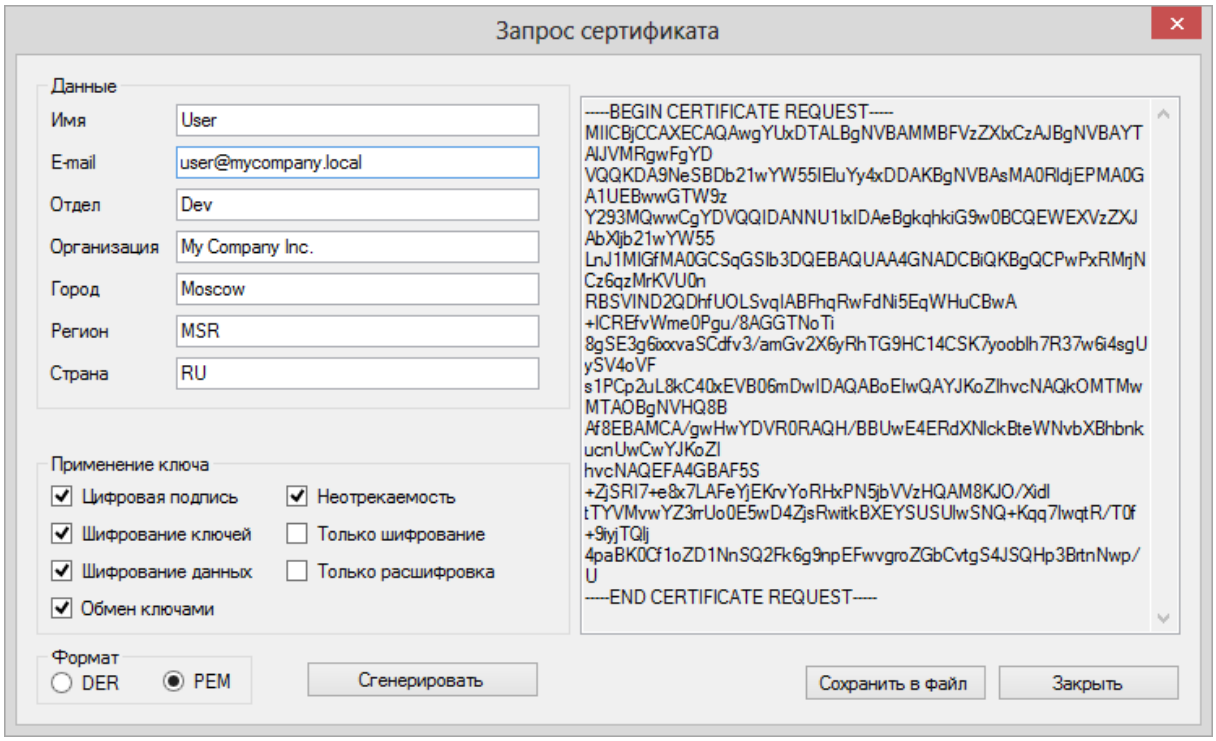
***Внимание!** Не вынимайте карту из считывателя до завершения операции генерации ключевой пары.*

12.4 Создание запроса на сертификат

*После того как на карте сгенерирована ключевая пара, необходимо создать запрос на сертификат (PKCS#10 или CSR). Выберите ключевую пару и нажмите **Запрос сертификата**.*

Заполните анкету в новом окне. Отметьте необходимые способы применения ключа. Укажите формат, в котором должен быть составлен запрос на сертификат. Как правило, используется PEM-формат (base64).

*Нажмите **Сгенерировать**. В окне справа появится запрос на сертификат, который представляет собой набор символов. Скопируйте содержимое окна полностью, включая первую и последнюю строки (BEGIN CERTIFICATE REQUEST и END CERTIFICATE REQUEST) или сохраните запрос в виде текста, нажав **Сохранить в файл**.*

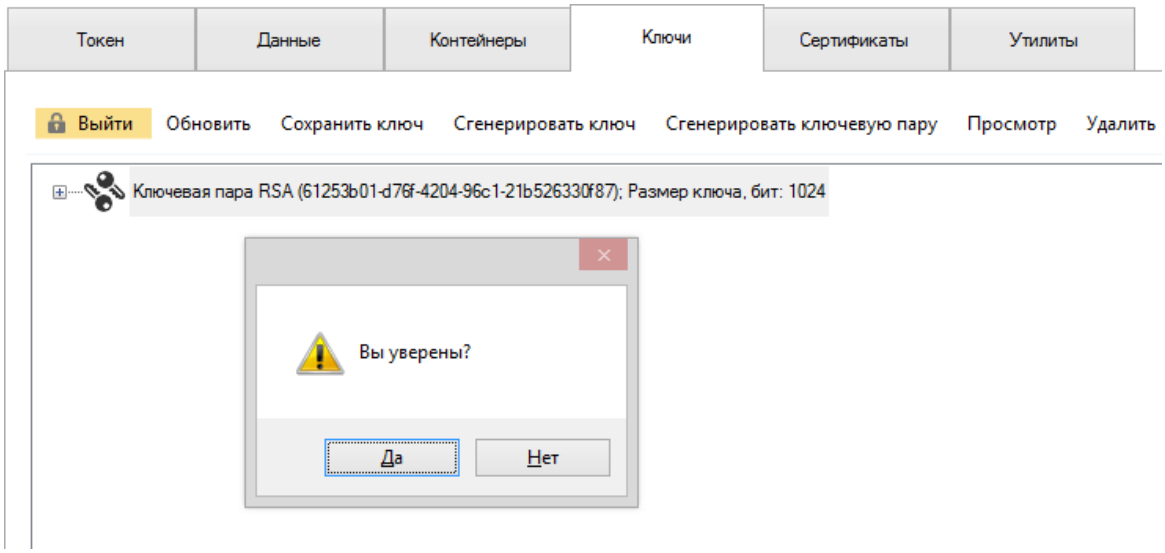


В соответствии с корпоративными правилами передайте запрос администратору, например, скопировав его в сообщение электронной почты или добавив файл в виде вложения.

Сохраните файл с полученным сертификатом на ПК. Запишите сертификат на ESMART Token. См. раздел ***Добавление сертификата****.*

12.5 Удаление ключей

Чтобы удалить ключи симметричного шифрования (DES, 3DES, KDES или AES) или ключевую пару RSA или ГОСТ, выберите объект и нажмите ***Удалить****. Подтвердите операцию.*



Внимание! *Если для ключевой пары был создан запрос на сертификат, а затем полученный сертификат был записан на карту, ключевая пара пропадет из списка в разделе* ***Ключи****, но появится вместе с сертификатом в разделе* ***Контейнеры****.*

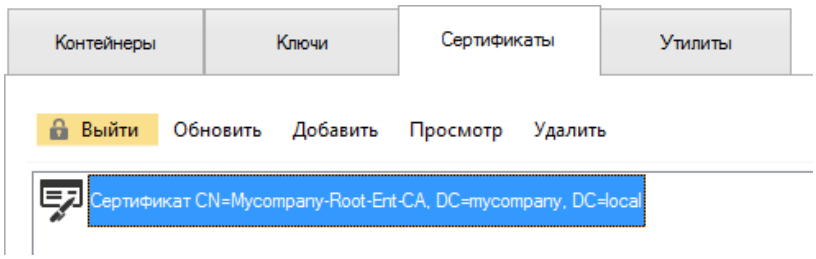
13. Сертификаты

На ESMART Token могут храниться следующие типы сертификатов X.509:

- ***Собственные сертификаты**, к которым на карте имеется закрытый ключ. Собственные сертификаты отображаются только во вкладке **Контейнеры**. Сертификаты используются для электронной подписи и дешифрования полученной информации.*
- ***Корневые сертификаты**, которые отображаются во вкладке **Сертификаты**. Корневые сертификаты следует хранить на карте, если часто используются разные ПК.*
- ***Другие сертификаты**, которые были получены от коллег, партнеров и т.д. При необходимости, работая за чужим ПК можно использовать сертификаты с карты, чтобы зашифровать сообщения, например, электронную почту открытым ключом получателя.*

13.1 Добавление сертификата

*Чтобы импортировать сертификат на карту, нажмите **Добавить** и укажите путь к файлу сертификата. Как правило, файлы пользовательских сертификатов имеют разрешение .cer, а файлы корневых сертификатов .crt.*

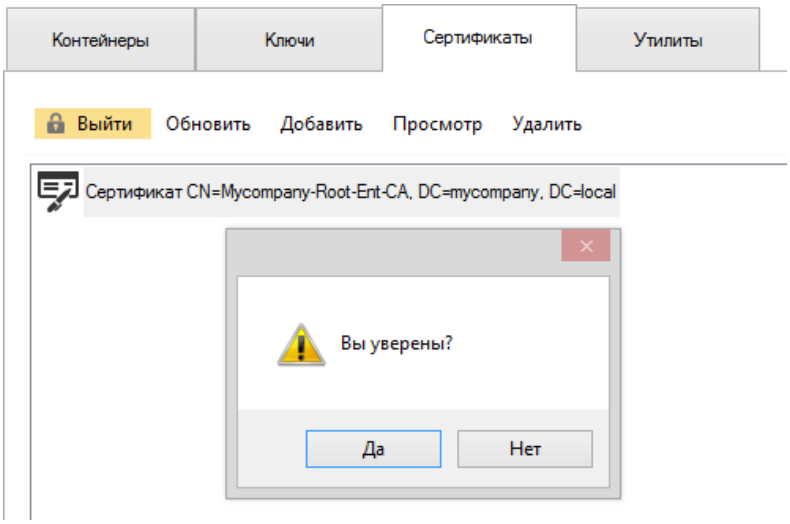


*В разделе **Сертификаты** постоянно отображаются только корневые сертификаты и другие сертификаты, например, сертификаты, полученные от коллег и партнеров.*

***Внимание!** Если на карту записывается сертификат для ключевой пары, которая была сгенерирована на карте (см. раздел Генерация ключевой пары), сертификат не будет показан во вкладке **Сертификаты**. Записанный сертификат будет прикреплен к соответствующей ключевой паре, которая автоматически переместиться во вкладку **Сертификаты**.*

13.2 Удаление сертификата

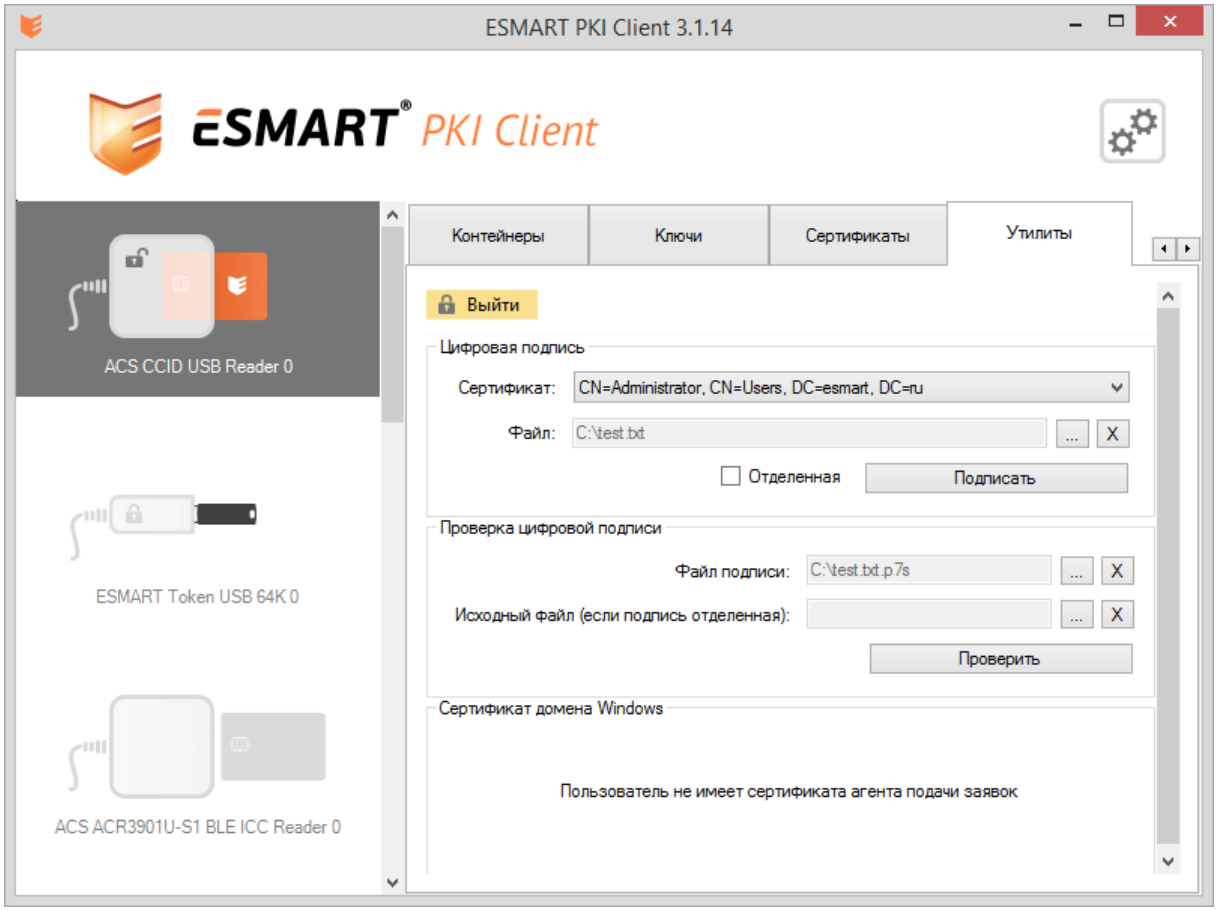
*Чтобы удалить сертификат, выберите его в списке и нажмите **Удалить**. Подтвердите выполнение операции.*



14. Утилиты

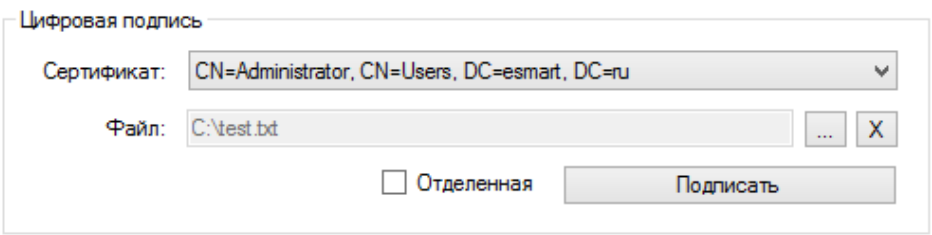
*На вкладке **Утилиты** собраны различные вспомогательные функции для работы с сертификатами и смарт-картами:*

- *Цифровая подпись файла (обычная или отделяемая);*
- *Проверка цифровой подписи (обычной или отделяемой);*
- *Выдача доменного сертификата на смарт-карту.*



14.1 Цифровая подпись

Смарт-карта может быть использована для подписи файла любого формата. Цифровая подпись представляет собой хэш-сумму подписываемого файла, зашифрованную закрытым ключом пользователя. При проверке подписи, зашифрованные данные расшифровываются открытым ключом получателя. Если расшифровка прошла успешно, подпись считается верной.

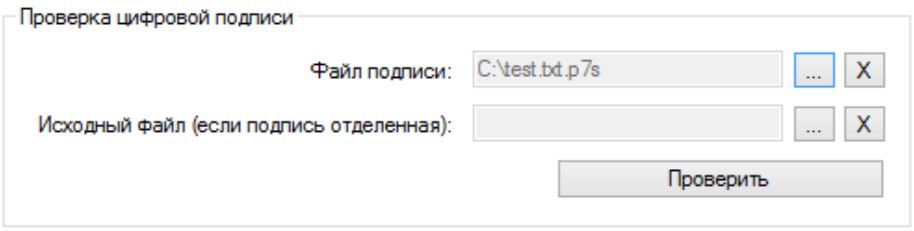


Чтобы воспользоваться функцией цифровой подписи файла выберите сертификат на карте, который будет использоваться для подписи и укажите файл, который будет подписан. Выберите тип подписи: отделяемая или неотделяемая. Оба типа подписи позволяют установить, был ли документ изменен с момента подписания. Задав все параметры, нажмите ***Подписать.*** *Отделяемая цифровая подпись будет сохранена в той же папке, что и исходный файл в формате: название_файла. detached.*

14.2 Проверка подписи

Для проверки подписи выберите подписанный файл или отдельный файл подписи в формате PKCS7. Файлы подписи могут иметь разное расширение, например .detached.

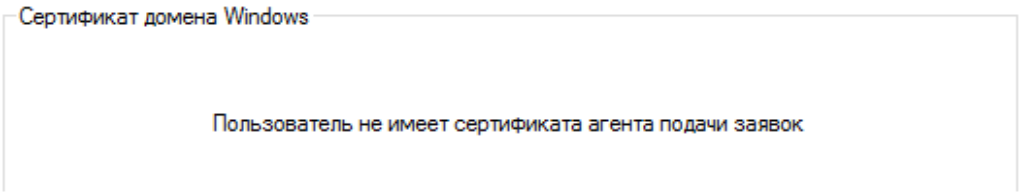
Введите все параметры и нажмите ***Проверить****.*



14.3 Выдача доменного сертификата

Как правило, сертификат для смарт-карты выписывает администратор.

Обычным пользователям будет показано сообщение: «Пользователь не имеет сертификата агента подачи заявок».



15. Возможные проблемы

Проблема	Способы устранения
Невозможно установить ESMART PKI Client	Установку приложения должен производить сотрудник, имеющий права администратора.
ESMART PKI Client не запускается в Linux	Для запуска программы в Linux требуется среда Mono. Обратитесь к администратору.
ESMART PKI Client не видит считыватель	Обратитесь к администратору.
Карта вставлена в считыватель, но не отображается	Обратитесь к администратору.
В Windows XP приложение не работает	Для Windows XP требуется установка пакета Microsoft Base CSP. Обратитесь к администратору.
Карта заблокирована после ввода неверного ПИН-кода	Для разблокировки карты требуется SO PIN. Обратитесь к администратору.
Невозможно сменить ПИН-код. Справа от поля появляется красная иконка с восклицательным знаком	Новый ПИН-код не соответствует требованиям, заданным в настройках программы. Откройте окно настроек, чтобы увидеть текущие требования к ПИН-коду. Пользователям не рекомендуется изменять настройки самостоятельно, а обратиться к администратору.
При запуске ESMART PKI Client появляется сообщение «Программа уже запущена»	Программа уже запущена в фоновом режиме. См. раздел Запуск в Windows