ESMART®

ESMART PKI Client
Руководство администратора

Содержание

1. Общая информация

Программное обеспечение ESMART PKI Client предназначено для работы со смарт-картами или USB-ключами ESMART Token и ESMART Token ГОСТ. Программа позволяет выполнить все необходимые операции со смарт-картами или USB-ключами без использования командной строки.

ESMART PKI Client является кроссплатформенным приложением, см. раздел 1.2 Системные требования.

Перед использованием ESMART PKI Client необходимо ознакомиться с руководством.

Интеллектуальные карты ESMART Token представляют собой пластиковые карты, в которые встроена интегральная схема (чип) для хранения и обработки информации. ESMART Token также 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****.*

1.1 Условия использования

ESMART PKI Client поставляется на безвозмездной основе для использования исключительно со смарт-картами и USB-ключами ESMART Token и ESMART Token ГОСТ. ESMART PKI Client устанавливается вместе с модулями, обеспечивающими работу с ESMART Token посредством криптопровайдера (только в Windows) или по стандарту PKCS#11 (в Windows, Linux, Mac OS).

ESMART PKI Client не может использоваться с другими типами смарт-карт и USB-ключей.

Запрещается любым способом пытаться получить исходные коды приложений или динамических библиотек, входящие в состав ESMART PKI Client.

1.2 Системные требования

Приложение является кроссплатформенным, т.е. работа с приложением возможна как в ОС Windows, так и в Linux и MacOS X. Для работы приложения в Linux, требуется установка Mono[1] — свободной кроссплатформенной реализации .NET Framework.

Рекомендуемые операционные системы:

- *MS Windows*
  - *Windows XP SP3;*
  - *Windows Vista;*
  - *Windows 7;*
  - *Windows 8;*
  - *Windows Server 2003;*
  - *Windows Server 2008, Windows Server 2012;*
- *Linux*
  - *OpenSuse;*
  - *Debian;*
  - *Ubuntu.*
- *MacOS X 10.7 и выше*

[1] *Страница проекта http://www.mono-project.com. Требуется дистрибутив версии не ниже 2.10*

1.3 Функционал ESMART PKI Client

- Просмотр общей информации:
  - Номер/описание слота;
  - Серийный номер;
  - Производитель;
  - Модель;
  - 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 (PKCS#10);
  - 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 (PKCS#12).
- Электронная подпись файла в формате PKCS#7 и проверка электронной подписи;
- Выдача сертификата на ESMART Token в Active Directory.

1.4 Преимущества

Графическое приложение ESMART PKI Client

- полностью заменяет бесплатные утилиты, например, pkcs11-tool и OpenSSL;
- просто в установке и в работе;
- имеет интуитивный графический интерфейс;
- не требуется использовать командную строку;
- позволяет ставить цифровую подпись на файлы любого типа и проверять уже подписанные файлы;
- может использоваться для выдачи сертификатов пользователя на смарт-карту в домене на базе Windows Server 2003, Windows Server 2008 или Windows Server 2012.

1.5 Техническая поддержка

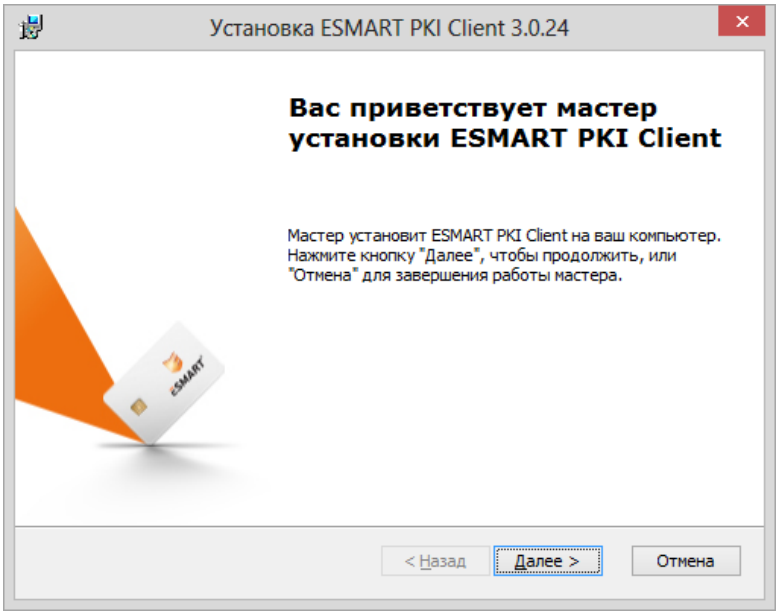
Для получения технической поддержки обратитесь по адресу helpdesk@isbc.ru. Перед обращением в службу поддержки, ознакомьтесь с разделом **Возможные проблемы**.

2. Установка и удаление

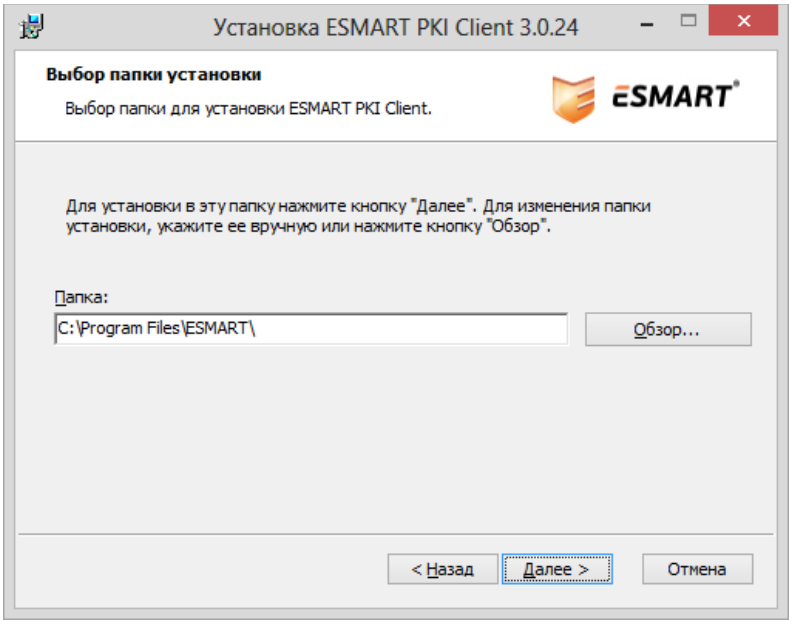
2.1 Windows

Установка приложения ESMART PKI Client в ОС Windows проста и интуитивно понятна. Установка может производиться вручную или с помощью программы-мастера (Windows\installer\setup.exe). Требуются права администратора.

*Рекомендуется установить пользователям бесплатное приложение ESMART PKI Client. При установке ESMART PKI Client через групповые политики необходимо заранее установить для всех пользователей сертификат ISBC в хранилище **Доверенные издатели**. Сертификат можно скопировать из инсталлятора приложения.*



Выберите путь установки или оставьте предложенный вариант.



Следуйте подсказкам программы-инсталлятора. Перезагрузите ПК, если появится соответствующее сообщение.

При установке ESMART PKI Client на ПК устанавливаются следующие программные компоненты:

- *Пользовательское приложение ESMART PKI Client;*
- *Модуль криптопровайдера (см. ESMART Token - CSP);*
- *Модуль PKCS#11 (см. ESMART Token PKCS#11).*

Также при установке в реестр будут добавлены записи, необходимые для работы ESMART Token с криптопровайдером SignalCOM CSP.

Удалять ESMART PKI Client рекомендуется через Панель управления › Удаление программ.

2.2 Linux

Для работы ESMART PKI Client требуется установка пакета для работы с картой по стандарту PKCS#11. Установка в ОС Linux производится при помощи rpm-пакета Linux\pkcs11\isbc-pkcs11-x.x.x-x.i586, где x – номер версии.

```
rpm -ivh isbc-pkcs11-x.x.x-x.i586.rpm
```

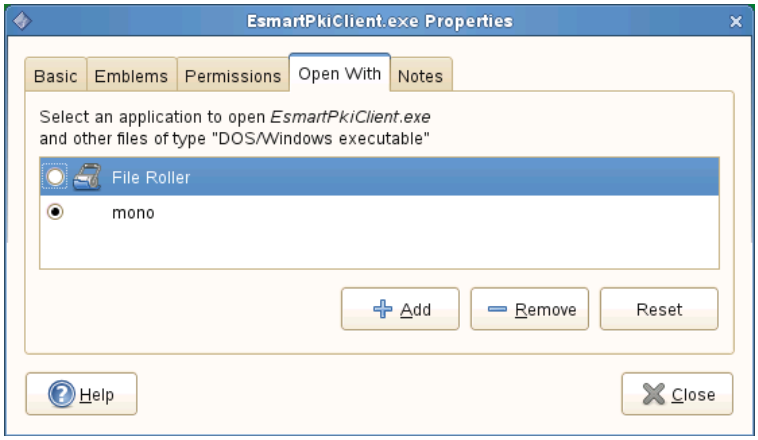
Требуются права root. Дистрибутив помещает библиотеки libisbc_esmart_token_mod.so, libisbc_pkcs11_main.so и libEsmartToken_Javalib.so (см. руководство ESMART Token – PKCS11 Java) в папку usr/lib.

Скопируйте папку ESMART PKI Client из дистрибутива из папки Windows/installer.

Для запуска программы из командной строки наберите команду, указав действительный путь к исполняемому файлу:

```
mono EsmartPkiClient.exe
```

Для удобства пользователей в среде Gnome рекомендуется в свойствах файла установить открытие по умолчанию через Mono, а также вынести ярлык программы ESMART PKI Client на рабочий стол.



Для удаления ESMART PKI Client удалите папку с исполняемым файлом. Удалите из usr/lib библиотеки libisbc_esmart_token_mod.so, libisbc_pkcs11_main.so и libEsmartToken_Javalib.so.

3. ПИН-код

ПИН[2]-кодом называют сочетание символов, как правило цифр, но для 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 можно при помощи SO PIN[3].

SO PIN используется администратором для инициализации карты, разблокировки карты после ввода пользователем неверного ПИН-кода.

В соответствии с Правилами пользования[4] СКЗИ ESMART Token ГОСТ, необходимо менять ПИН-код пользователя не реже, чем 1 раз в 6 месяцев.

3.1 Автоматическая генерация ПИН-кода

ESMART PKI Client позволяет сгенерировать ПИН-код, соответствующий требованиям безопасности, которые задаются в настройках программы. Требования к ПИН-коду задаются администратором в соответствии с корпоративными требованиями. См. раздел ***Требования к ПИН-коду****.*

4. Параметры объектов

4.1 Открытые объекты (тип Public)

Объекты доступны для чтения и просмотра без предъявления ПИН-кода. К таким объектам относятся:

- *Сертификаты;*
- *Открытые ключи RSA;*
- *Открытые ключи ГОСТ;*
- *Данные, для которых не выбрана опция – Защищенные (см. раздел 11.2 Типы блоков данных).*

4.2 Закрытые объекты (тип Private)

Объекты и их параметры отображаются в программе только после предъявления ПИН-кода. К таким объектам относятся:

- *Закрытые ключи RSA;*
- *Закрытые ключи ГОСТ;*
- *Ключи DES, 3DES и AES;*
- *Данные, для которых выбрана опция – Защищенные (см. раздел 11.2 Типы блоков данных).*

---

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

[3] *SO PIN (Security Officer PIN) – ПИН-код администратора*

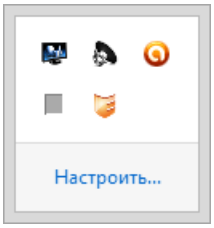
[4] *Правила пользования конкретного СКЗИ можно получить, отправив запрос на esmart@isbc.ru с указанием ID СКЗИ чипа, даты приобретения и юр. лица покупателя.*

5. Запуск программы

5.1 Запуск в Windows

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

Программу можно запустить меню Пуск › ESMART › ESMART PKI Client.



Если свернуть окно программы, программа 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 или выберите в контекстном меню ***Развернуть****.*

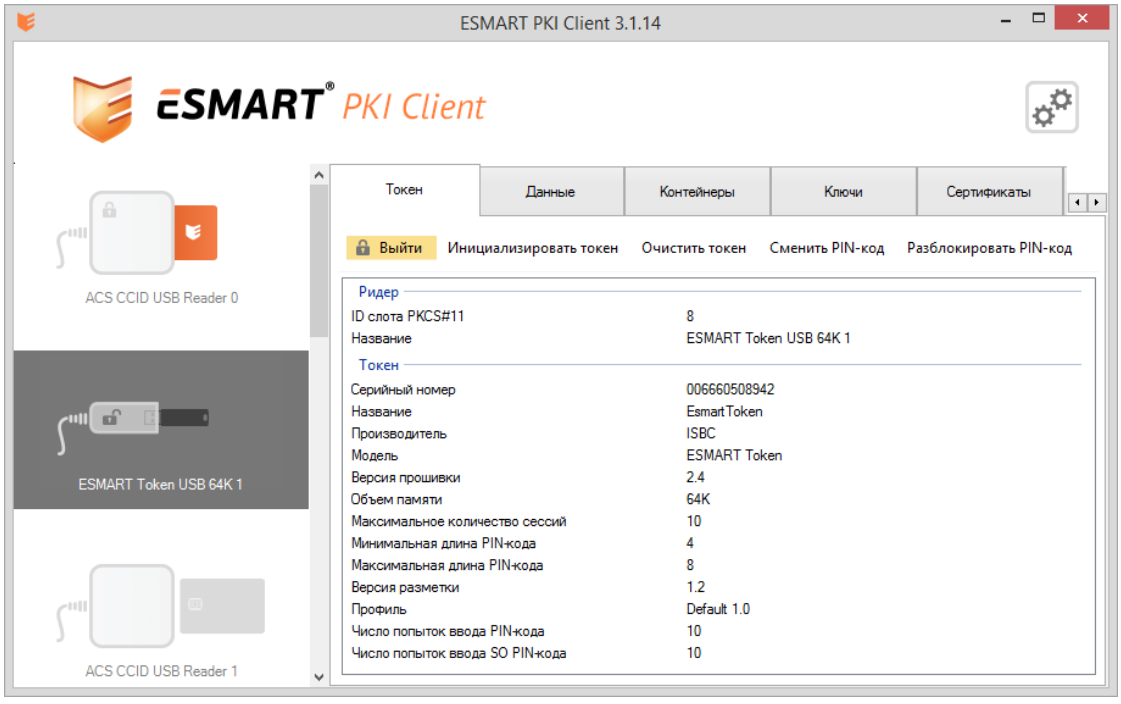
Для удобства в настройках программы можно задать автоматический запуск ESMART PKI Client. *См. стр. 11.*

5.2 Запуск в Linux

Для запуска программы в Linux требуется щелкнуть по иконке EsmartPkiClient.exe правой кнопкой мыши и в контекстном меню выбрать Open with Mono... (Открыть с помощью Mono...).

Для удобства пользователя можно настроить автоматическую ассоциацию. *См. стр 4 и далее.*

6. Интерфейс



Интерфейс программы поделен на 3 панели:

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.*

7. Вкладки основной панели

7.1 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, добавлять и удалять объекты. См. раздел **Порядок работы.***

7.2 Вкладка Данные

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

7.3 Вкладка Контейнеры

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

7.4 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[5];*
- *Симметричный ключ (AES, DES, 3DES, 3KDES).*

7.5 Вкладка Сертификаты

*Во вкладке **Сертификаты** показаны сертификаты, которые не принадлежат ни одной ключевой паре, например, корневые сертификаты УЦ или сертификаты коллег и партнеров. В число показанных сертификатов также могут попасть сертификаты с неверно загруженным идентификатором. См. раздел **Сертификаты**.*

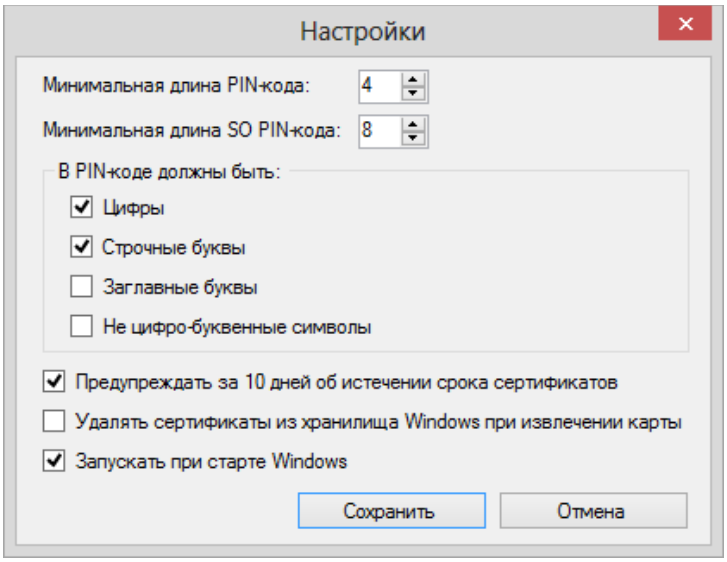
7.6 Вкладка Утилиты

*На вкладке **Утилиты** размещены средства добавления и проверки цифровой подписи. Также на вкладке **Утилиты** есть раздел для выдачи доменного сертификата.*

[5] *Только для ESMART Token GOST*

8. Настройки

В окне настроек можно изменить некоторые параметры работы ESMART PKI Client.



8.1 Автозагрузка

Включение опции Автозагрузка позволяет не вызывать программу каждый раз из меню Пуск или с помощью ярлыка на рабочем столе. Программа будет запускаться автоматически при загрузке операционной системы. Используется по умолчанию.

8.2 Удаление сертификатов из хранилища Windows

*Только для ОС Windows. Опция позволяет автоматически удалять сертификаты, загруженные с карты, из папки **Личное** хранилища сертификатов Windows, когда пользователь вынимает карту ESMART Token из считывателя. Удаление сертификатов обеспечивает наиболее высокий уровень безопасности. Настройка используется в соответствии с корпоративными требованиями к безопасности.*

***Внимание!** Чтобы сертификат был удален из хранилища, когда пользователь вынимает карту из считывателя, необходимо, чтобы приложение ESMART PKI Client было запущено на ПК. Для удобства приложение можно свернуть, а при необходимости вызвать из трея. См. стр. 9.*

По умолчанию опция не активирована.

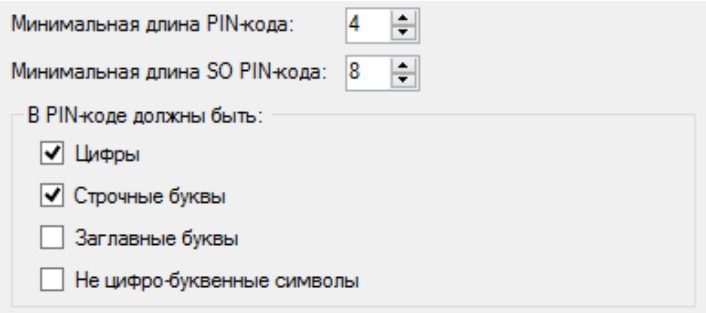
8.3 Предупреждение об истечении срока сертификатов

Сертификаты X.509 имеют ограниченный срок действия. Как правило, период действия пользовательских сертификатов составляет несколько лет.
Использовать истекший сертификат невозможно, его необходимо заменить новым сертификатом. При этом в соответствии с требованиями корпоративной безопасности либо выписывается новый сертификат к используемой паре ключей, либо новый сертификат будет выписан к новой ключевой паре.

Опция автоматического напоминания об истечении сертификатов позволяет за 10 дней напомнить пользователю и администратору о необходимости обновить сертификат. По умолчанию опция активирована.

8.4 Требования к ПИН-коду

Корпоративной политикой безопасности могут быть определены требования к ПИН-коду карты. Общие требования к ПИН-коду карты описаны в разделе ПИН-код. В настройках программы ESMART PKI Client можно задать требования к количеству и типу знаков ПИН-кода.



Задайте параметры ПИН-кода в соответствии с корпоративными требованиями. Смена настроек не влияет на уже заданные ПИН-коды карты. Требования учитываются только при смене ПИН-кода пользователя или администратора через программу ESMART PKI Client. Требования к ПИН-коду, заданные в настройках программы ESMART PKI Client, можно обойти, сменив ПИН-код через утилиты, работающие по стандарту PKCS#11, например pkcs11-tool. См. руководство ***ESMART Token – PKCS11****.*

При выборе параметров ПИН-кода необходимо обратить внимание, что ПИН-код должен достаточно легко запоминаться пользователем, чтобы не нужно было его записывать. Слишком строгие требования могут привести к тому, что пользователь захочет записать ПИН-код на листке бумаги или в ежедневнике в открытом виде, что с большой вероятностью может привести к компрометации ПИН-кода. Поскольку ПИН-код карты защищен от прямого подбора (не более 10 попыток), комбинация должна быть такой, чтобы пользователь мог ее легко запомнить.

9. Задачи администратора

После получения карт ESMART Token и считывателей или USB-ключей ESMART Token в задачи администратора входят следующие действия[6]:

4. *Ознакомиться с документацией и руководством администратора;*
5. *Установить драйвер USB-ключа или считывателя;*
6. *Установить ESMART PKI Client с помощью инсталлятора или установить вручную отдельные компоненты;*
7. *Проверить и при необходимости изменить настройки программы ESMART PKI Client;*
8. *Настроить удобный для пользователя запуск программы с помощью ярлыка, через меню Пуск или автозапуск;*
9. *Выдать сертификат и записать его на карту;*
10. *Добавить в хранилище сертификатов сертификат УЦ;*
11. *Проверить работу системы, например, выполнив вход в домен по карте;*
12. *Проверять действительность сертификатов и обновлять сертификаты при необходимости;*
13. *Удалять недействительные сертификаты с карт и токенов.*

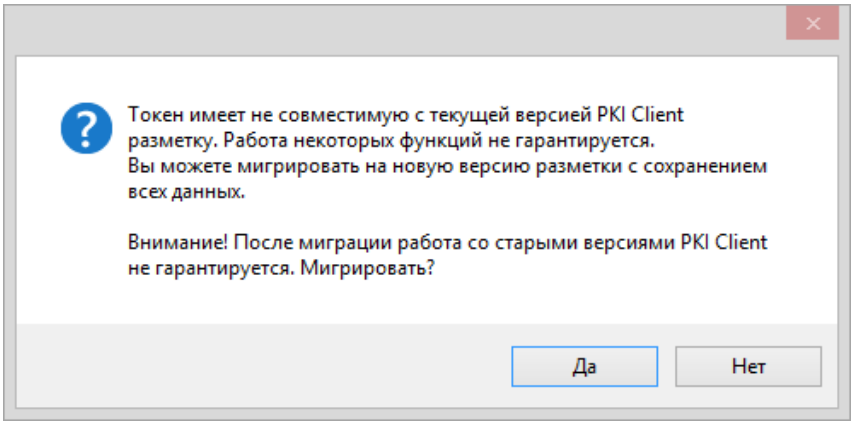
[6] *Список задач администратора также может включать первоначальную настройку корпоративного центра сертификации и его обслуживание или подбор и заключение договора с внешним удостоверяющим центром.*

10. Порядок работы

10.1 Миграция токена

При использовании смарт-карт или USB-токенов со старой разметкой в ряде случаев необходимо мигрировать на новую разметку. Миграция осуществляется с помощью приложения ESMART PKI Client. При миграции на ESMART Token сохранятся все данные.

Если требуется мигрировать токен на новую разметку, в интерфейсе приложения ESMART PKI Client появится следующий запрос на миграцию:



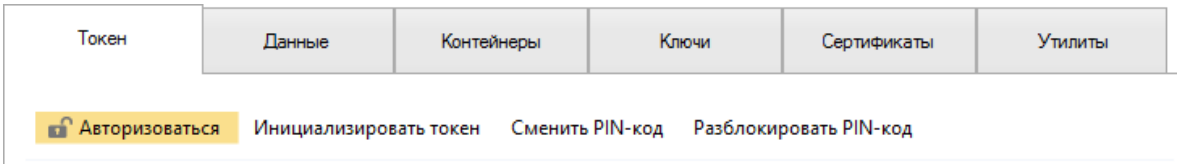
Подтвердите миграцию и введите ПИН-код пользователя.

***Важно**: в операционной системе Windows XP на токене невозможно авторизоваться пока не будет произведена миграция.*

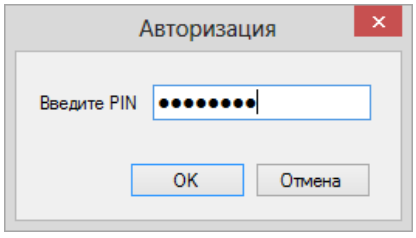
10.2 Регистрация на карте

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

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

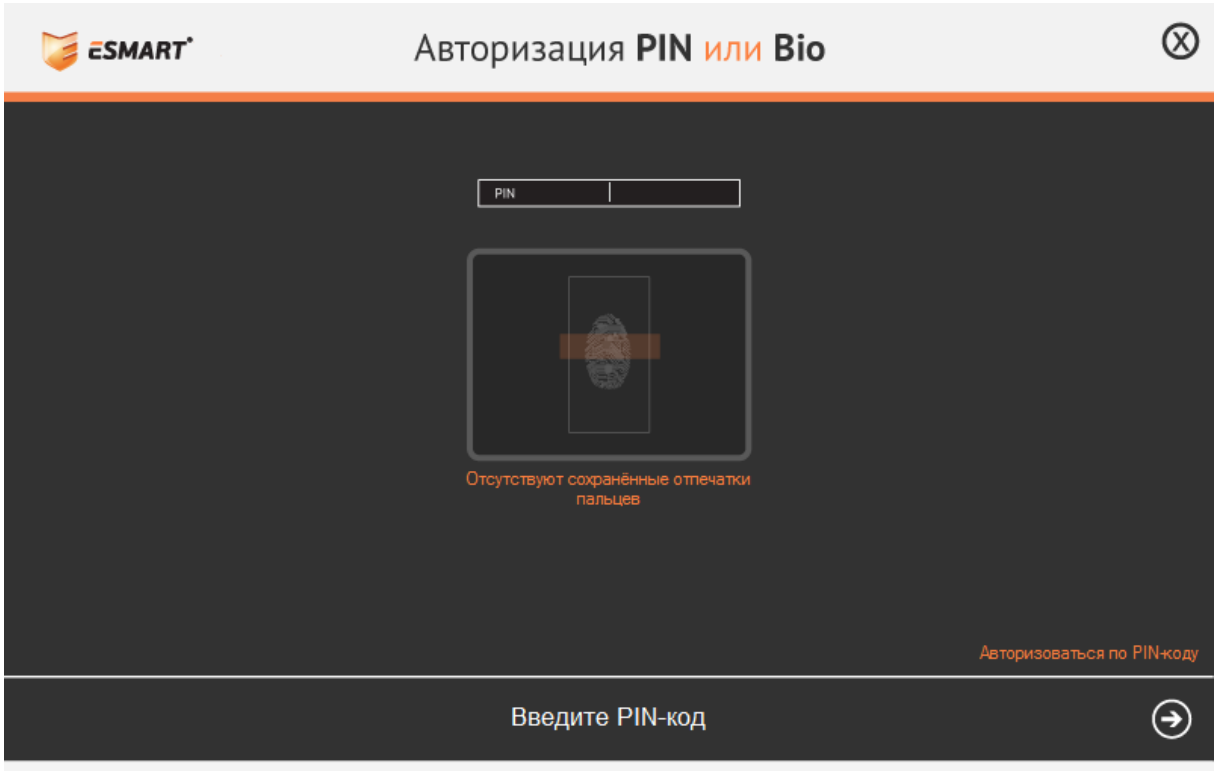


В появившееся окошко введите ПИН-код пользователя.



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

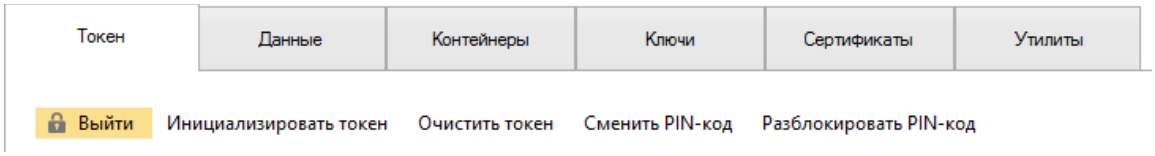
Для ESMART Token ГОСТ будет показано другое окно авторизации:



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

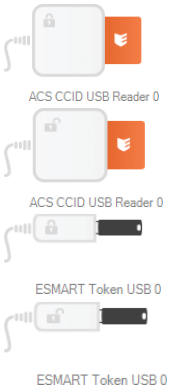
10.3 Завершение сеанса

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



10.4 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.

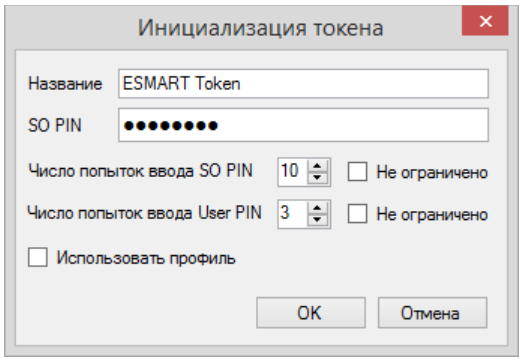
Вставлена несовместимая смарт-карта или карта вставлена неверно.

10.5 Инициализация

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

***Внимание!** При инициализации вся информация (ключи, сертификаты и контейнеры, а также данные) будет стерта.*

*Для инициализации карты или USB-ключа ESMART Token нажмите **Инициализировать токен** в верхней панели. В появившемся окне введите название карты и SO PIN.*



Задайте число попыток ввода PIN-кода пользователя и PIN-кода администратора.

***Внимание!** Если неверно ввести SO PIN заданное количество раз, карта будет заблокирована **без возможности восстановления**.*

10.6 Инициализация с указанием профиля

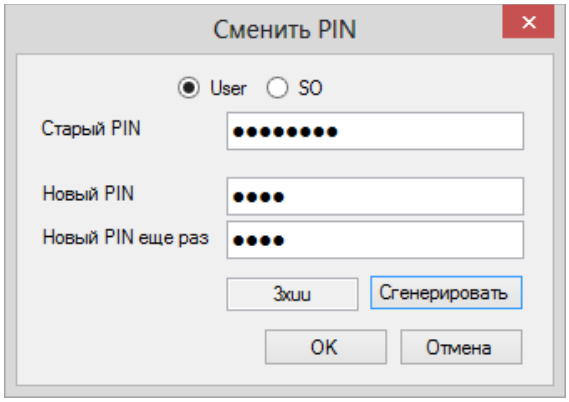
Профили определяют, какие типы данных будут храниться на ESMART Token для оптимального использования памяти и некоторые другие параметры. Профили применяются только при форматировании токена. Например, можно увеличить размер памяти под пользовательские данные за счет уменьшения максимального количества симметричных ключей.

Профиль по умолчанию	*Если при инициализации токена профиль не указан, используется профиль по умолчанию, в рамках которого оптимально для большинства способов применения сбалансированно распределение памяти под ключевые пары и сертификаты, данные и симметричные ключи.*
CryptoPro NoPIN	*Использование данного профиля позволяет пользователю не вводить ПИН-код по умолчанию в приложениях ESMART PKI Client и КриптоПро CSP не ниже версии 3.6 R4.*
Max RSA	*Профиль рассчитан на хранение максимально-возможного количества ключевых пар RSA (10 ключевых пар) за счет объектов других типов (данных не более 8 и симметричных ключей не более 8)*
Max RSA SM	*Профиль аналогичен Max RSA, дополнительно включена опция Secure Messaging*
PGP Desktop 10	*Профиль для работы с приложением PGP Desktop версии 10*

ViPNet	*Профиль для работы с криптопровайдером ViPNet CSP. Дополнительно на карте может хранится 1 ключевая пара RSA и 8 симметричных ключей.*
ViPNet2	*Профиль для работы с криптопровайдером ViPNet CSP рассчитан на хранение контейнеров ViPNet максимального размера. Дополнительно на карте может хранится до 8 симметричных ключей. Место под ключевую пару RSA не предусмотрено.*
ViPNet3	*Профиль для работы с криптопровайдером ViPNet CSP рассчитан на хранение максимального количества контейнеров ViPNet меньшего развера. Дополнительно на карте может хранится до 8 симметричных ключей. Место под ключевую пару RSA не предусмотрено.*
ViPNet SM	*Профиль аналогичен ViPNet, дополнительно включена опция Secure Messaging*

10.7 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**.*



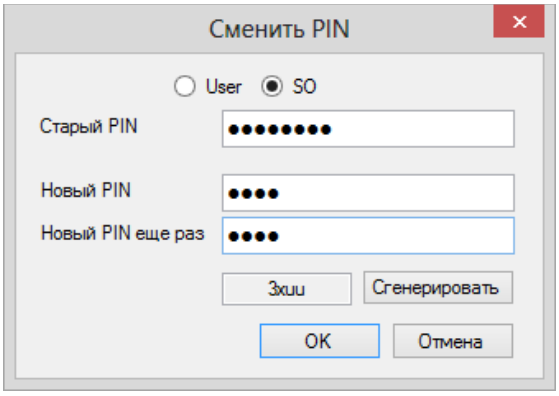
*ПИН-код, соответствующий требованиям, заданным в настройках, можно сгенерировать автоматически. Нажмите **Сгенерировать**. Новый автоматически сгенерированный ПИН-код будет автоматически подставлен в поля ввода и в открытом виде появится в поле. Чтобы сгенерировать новый ПИН-код, нажмите на кнопку ещё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

Если ПИН-код, введенный пользователем, 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.

10.8 Смена ПИН-кода администратора (SO PIN)

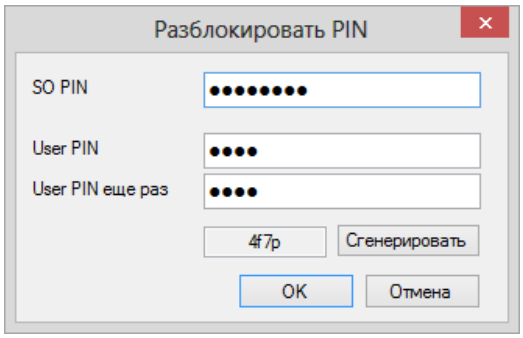
*Нажмите **Сменить ПИН** в верхней панели. В появившемся окне отметьте SO, введите текущий SO PIN и два раза новый SO PIN.*



Автоматическая генерация ПИН-кода администратора выполняется так же, как для ПИН-кода пользователя.

10.9 Разблокировка ПИН-кода пользователя

Если пользователь ввел неверный ПИН-код 10 раз подряд, карта блокируется. Данные на карте при блокировке карты не удаляются. Чтобы разблокировать карту, требуется ввести SO PIN.



***Внимание!** Если ввести неверный SO PIN несколько раз подряд, карта **блокируется без возможности восстановления**. Количество неудачных попыток задается при инициализации.*

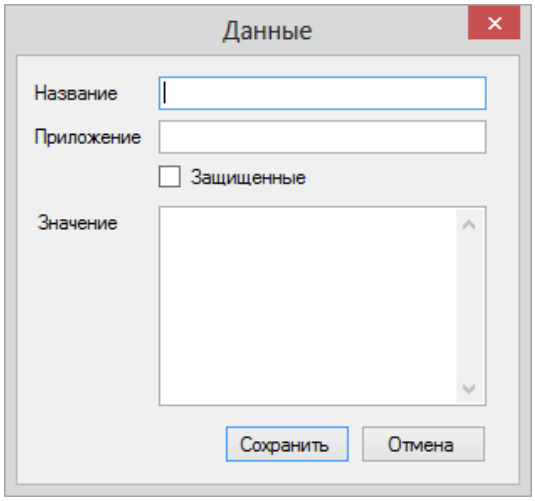
11. Данные

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.

11.1 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

11.2 Типы блоков данных

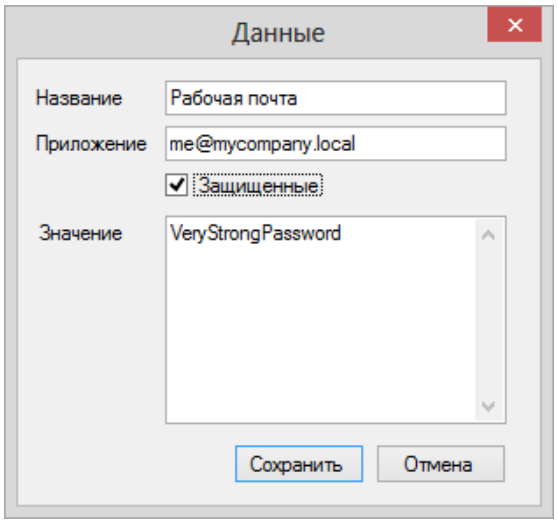
Для хранения текстовой информации на карте ESMART Token можно выбрать один из двух вариантов блоков данных:

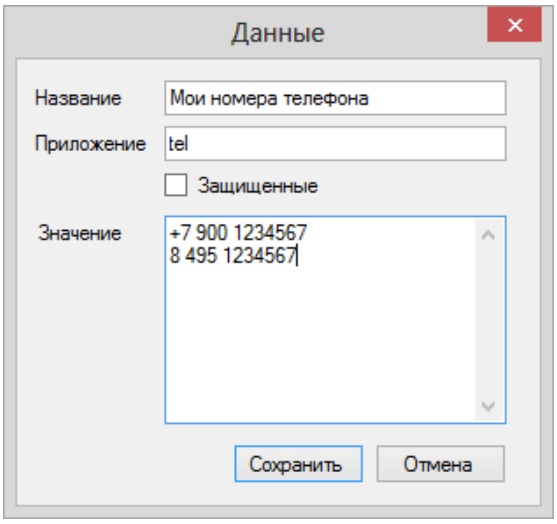
Защищенные данные

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

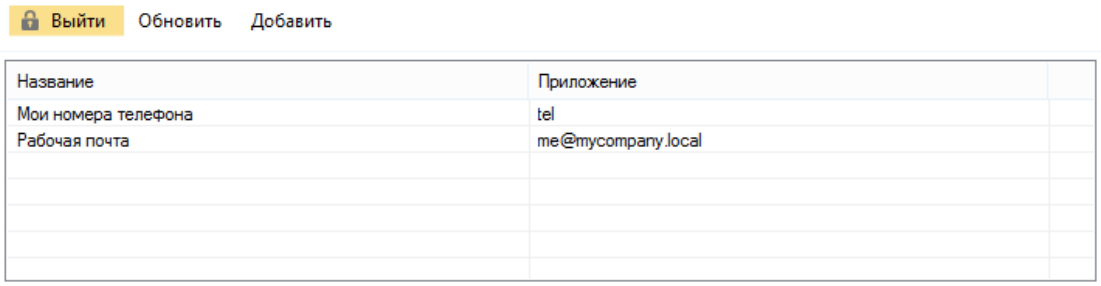
Обычные данные

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

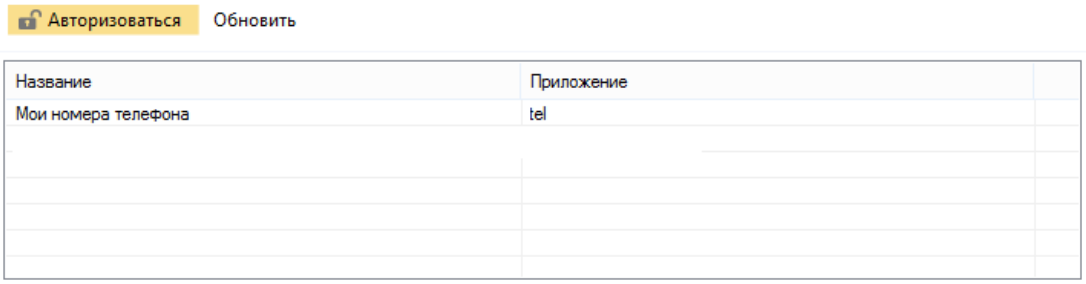




Если пользователь авторизован, в списке присутствуют блоки данных обоих типов:

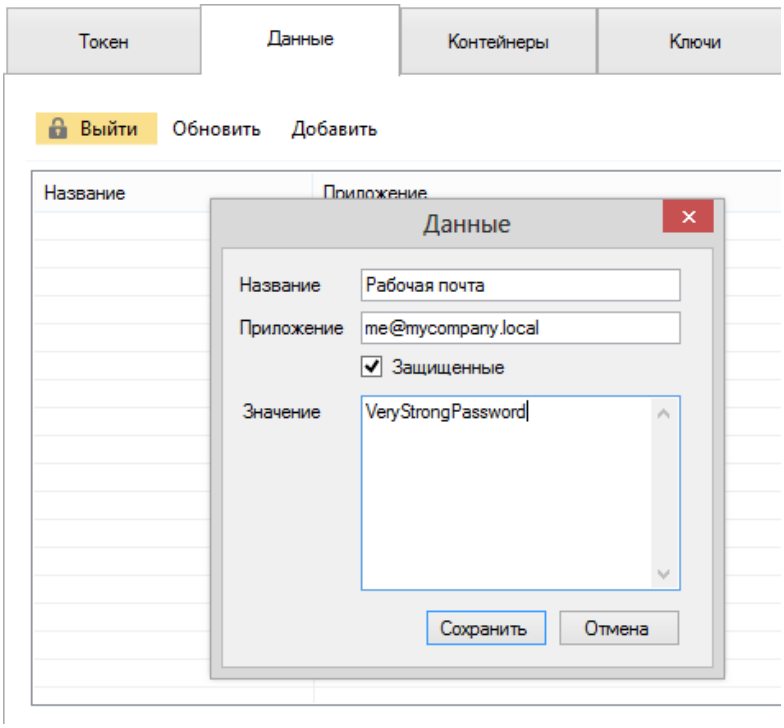


Если пользователь не авторизован, в списке присутствуют только обычные блоки данных:

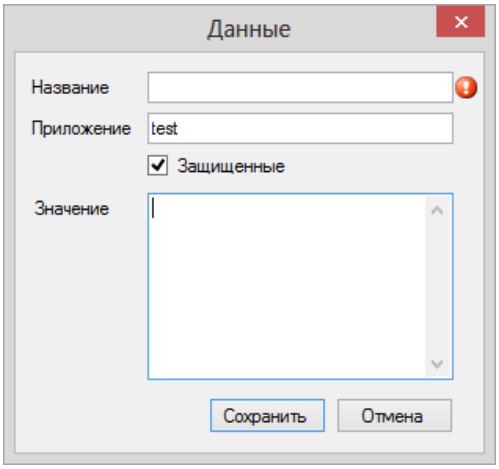


11.3 Добавление данных

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

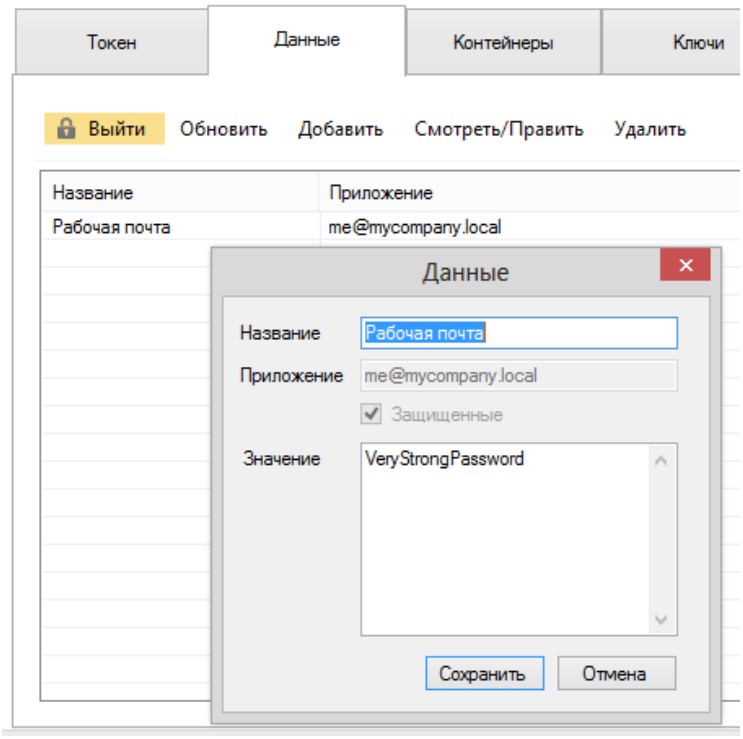


Поле ***Название*** *является обязательным для заполнения. Поле* ***Приложение*** *может быть пустым, но если не заполнить его при создании блока данных, отредактировать его будет невозможно.*



11.4 Редактирование данных

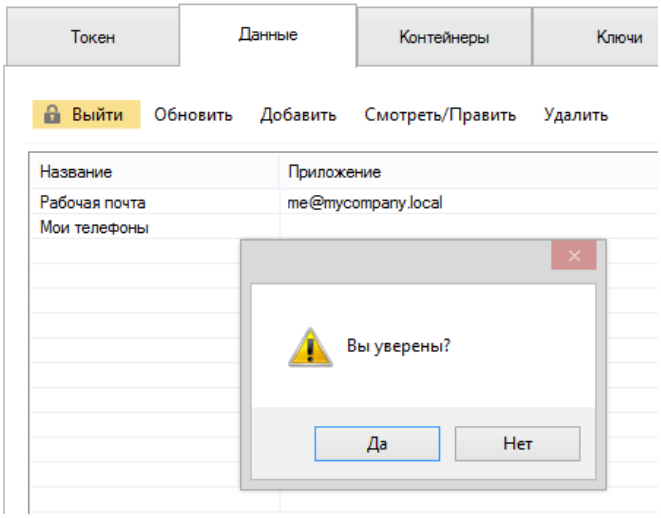
Чтобы отредактировать данные, выберите в списке нужный блок и нажмите ***Смотреть/Править****. В появившемся окне сделайте нужные изменения и нажмите* ***Сохранить****.*



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

11.5 Удаление данных

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



Внимание! *Восстановить удаленные данные невозможно.*

12. Контейнеры

Под Контейнером понимают хранение на карте связанных объектов:

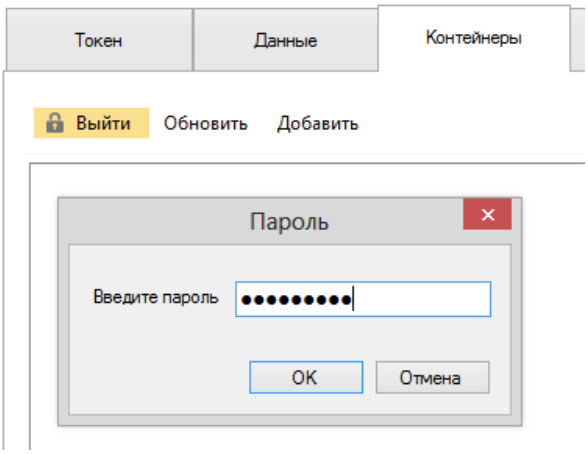
- *Сертификата X.509;*
- *Ключевой пары (RSA или ГОСТ), состоящей из*
  - *открытого ключа;*
  - *закрытого ключа.*

Перечисленные объекты имеют одинаковые параметры «Название» (Label) и «Идентификатор» (ID).

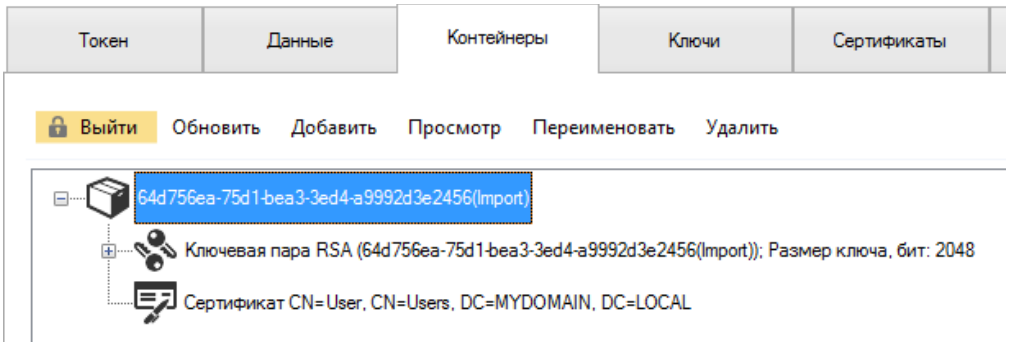
12.1 Добавление контейнера

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

Чтобы загрузить 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.



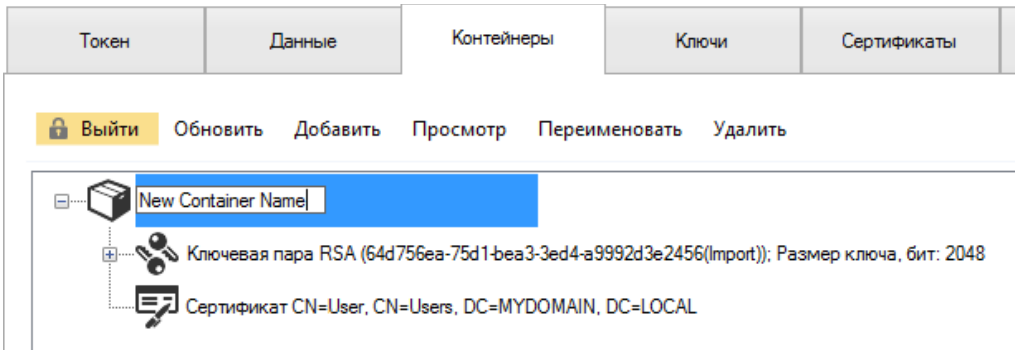
После того как содержимое контейнера перенесено на карту, рекомендуется удалить файл .p12 или .pfx. Если файл требуется сохранить в качестве резервной копии, примите меры для обеспечения безопасности файла.

12.2 Просмотр параметров объектов

Для просмотра параметров объектов, выберите сам контейнер, сертификат или ключи и нажмите ***Просмотр****.*

12.3 Переименование контейнера

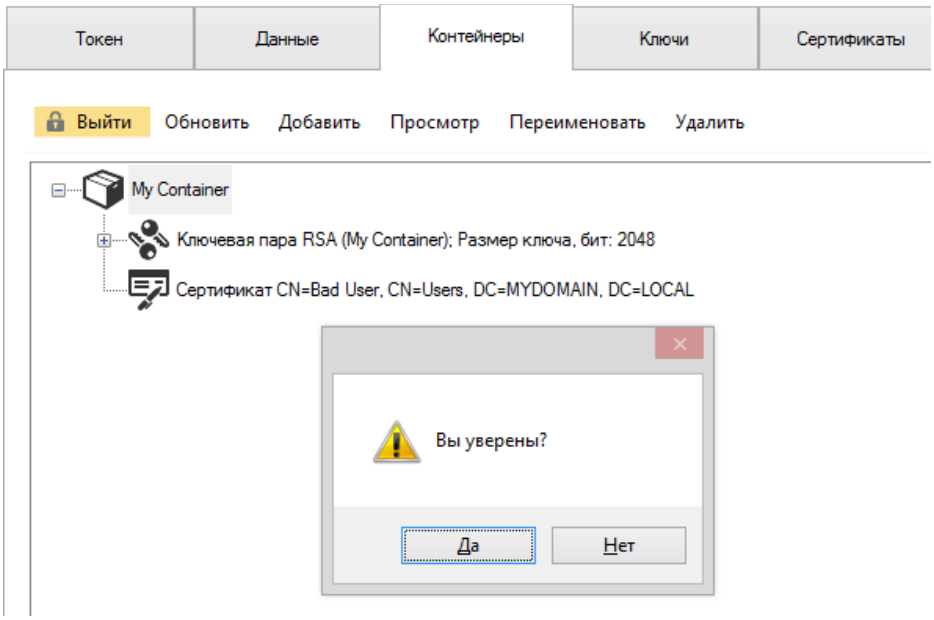
Чтобы было удобнее использовать список, контейнеры можно переименовать, т.е. изменить его параметр ***Label****. Чтобы переименовать контейнер, выделите его и нажмите* ***Переименовать****. В поле для редактирования введите новое название. Нажмите на клавиатуре* ***Ввод (Enter)****.*



При переименовании контейнера фактически параметр «Название» (Label) меняется для открытого ключа, для закрытого ключа и для соответствующего сертификата.

12.4 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.*

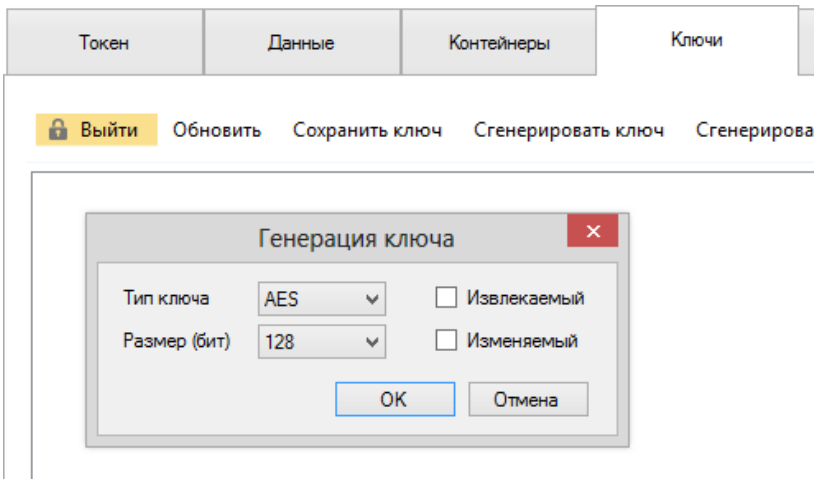
Контейнер на карту можно импортировать повторно, если имеется файл PKCS#12 (формат .pfx или .p12). См. раздел Добавление контейнера.

13. Ключи

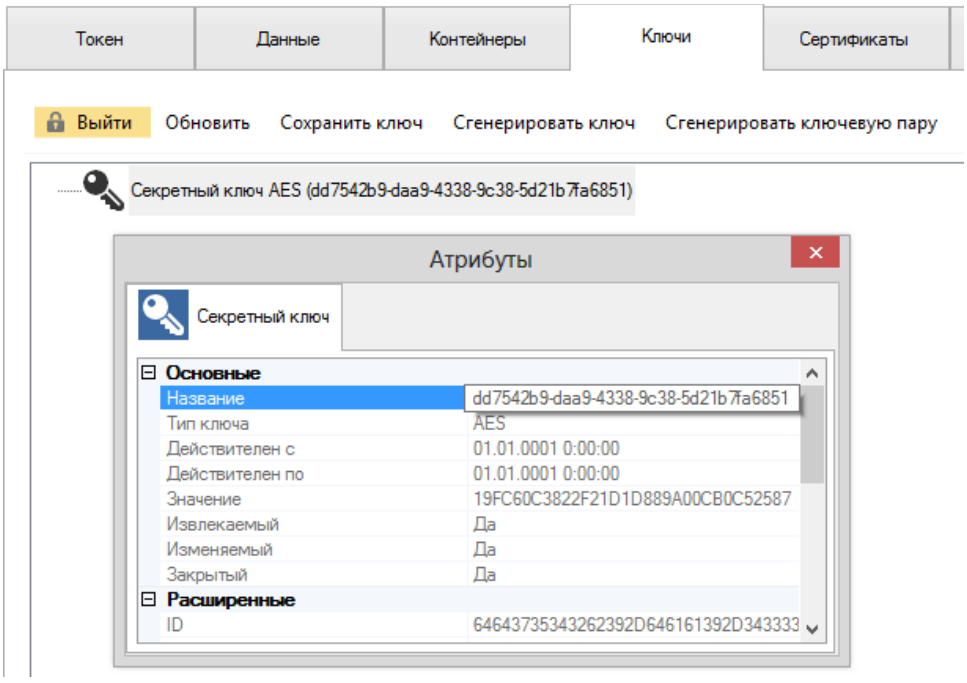
Вкладка предназначена для работы с ключами для симметричного шифрования (DES, 3DES, 3KDES и AES) и ключевыми парами RSA и ГОСТ для асимметричного шифрования.

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

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

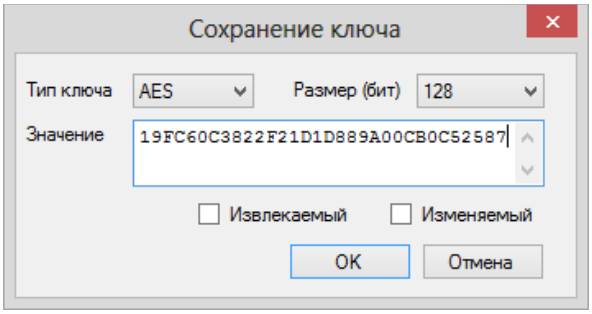


Чтобы просмотреть данные ключа, выберите ключ из списка и нажмите ***Просмотр****.*



13.2 Сохранение ключа

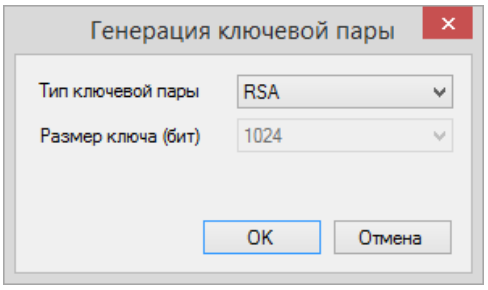
Чтобы записать на карту существующий ключ симметричного шифрования DES, 3DES, 3KDES или AES, нажмите ***Сохранить ключ****. Вставьте в поле значение ключа и нажмите* ***ОК****.*

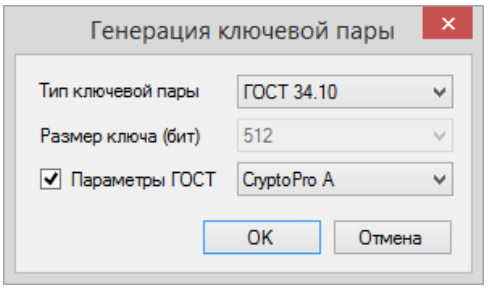


13.3 Генерация ключевой пары

Ключевая пара, 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).*

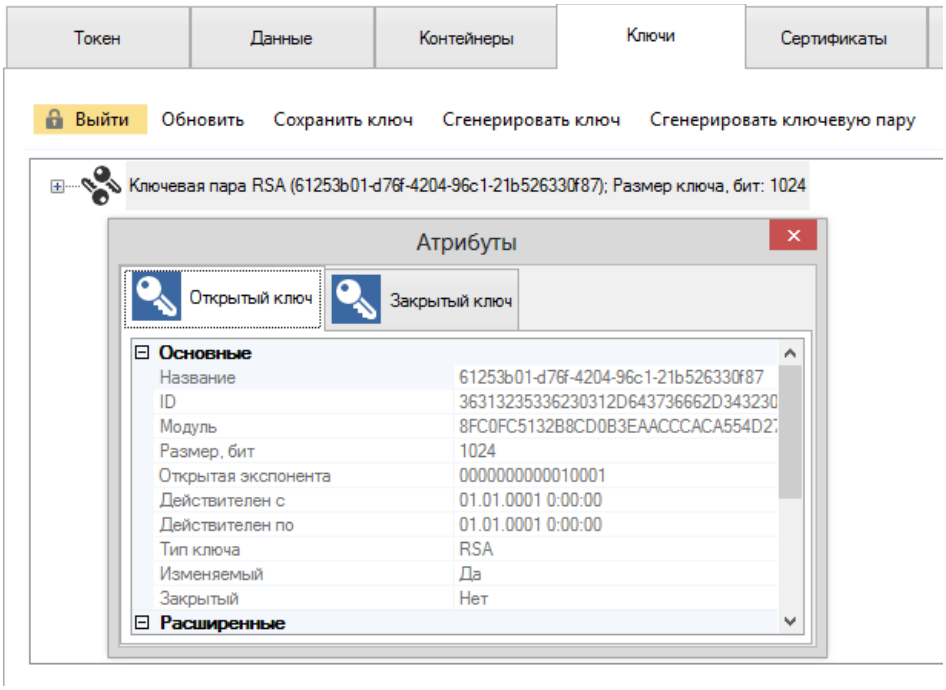




***Внимание!** Не вынимайте карту из считывателя до завершения операции генерации ключевой пары.*

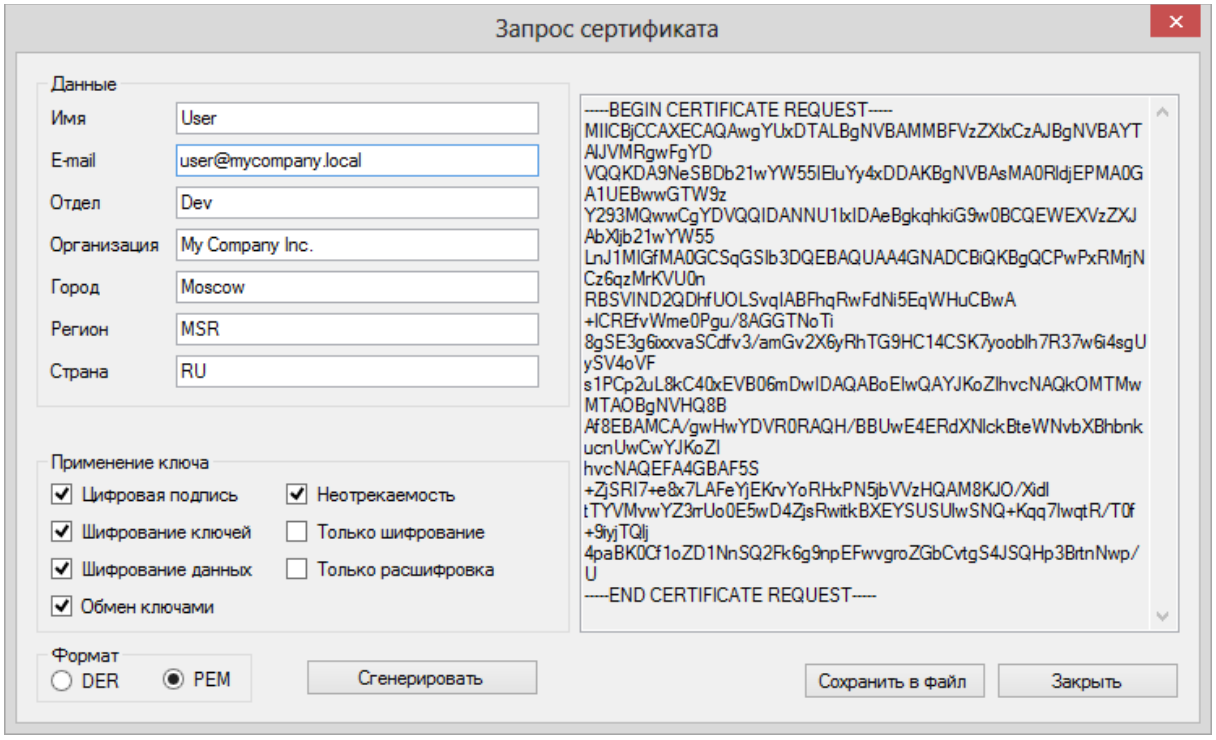
13.4 Создание запроса на сертификат

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



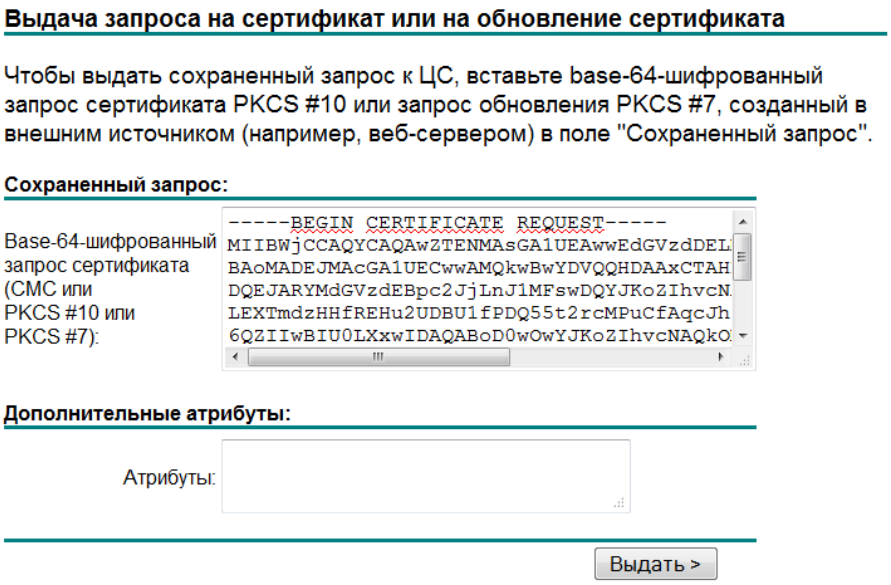
Заполните анкету в новом окне. Отметьте необходимые способы применения ключа. Укажите формат, в котором должен быть составлен запрос на сертификат. Как правило, используется PEM-формат (base64).

*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 текстовый файл, нажав **Сохранить в файл**.*



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

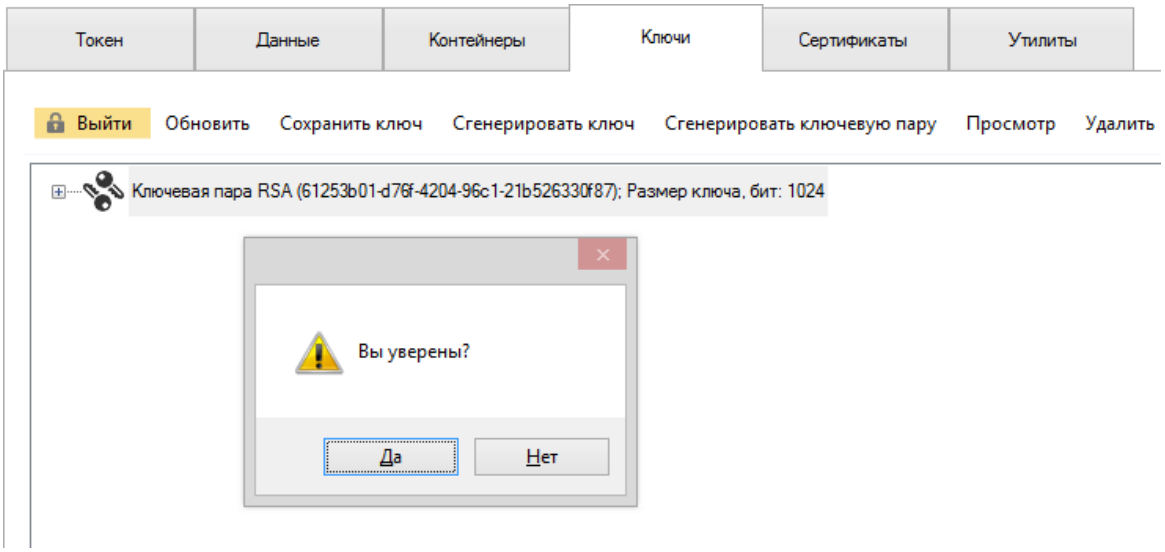
используется веб-интерфейс УЦ[7], просто вставьте скопированный запрос в форму и нажмите ***Выдать***.



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

13.5 Удаление ключей

Чтобы удалить ключи симметричного шифрования (DES, 3DES, 3KDES 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***.

[7] *Веб-интерфейсы центров сертификации могут значительно отличаться*

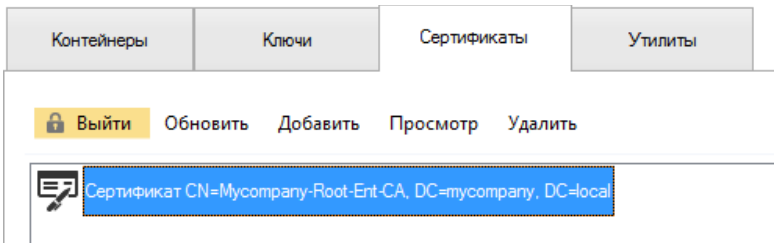
14. Сертификаты

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. При необходимости можно установить корневой сертификат с карты.*
- ***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.*

14.1 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.*

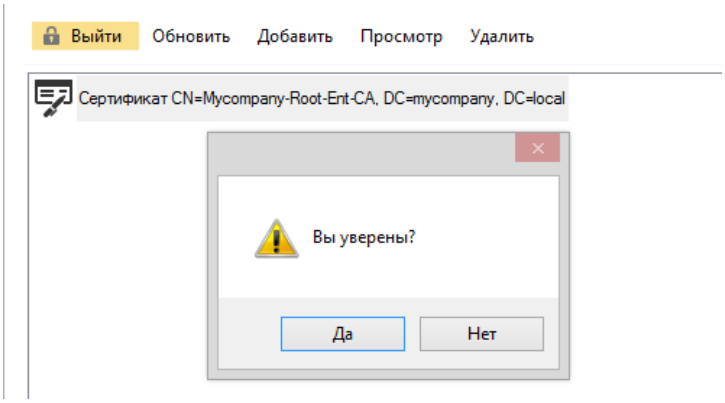


*В разделе **Сертификаты** постоянно отображаются только корневые сертификаты и другие сертификаты, например, сертификаты, полученные от коллег и партнеров.*

***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 переместится во вкладку **Контейнеры**.*

14.2 Удаление сертификата

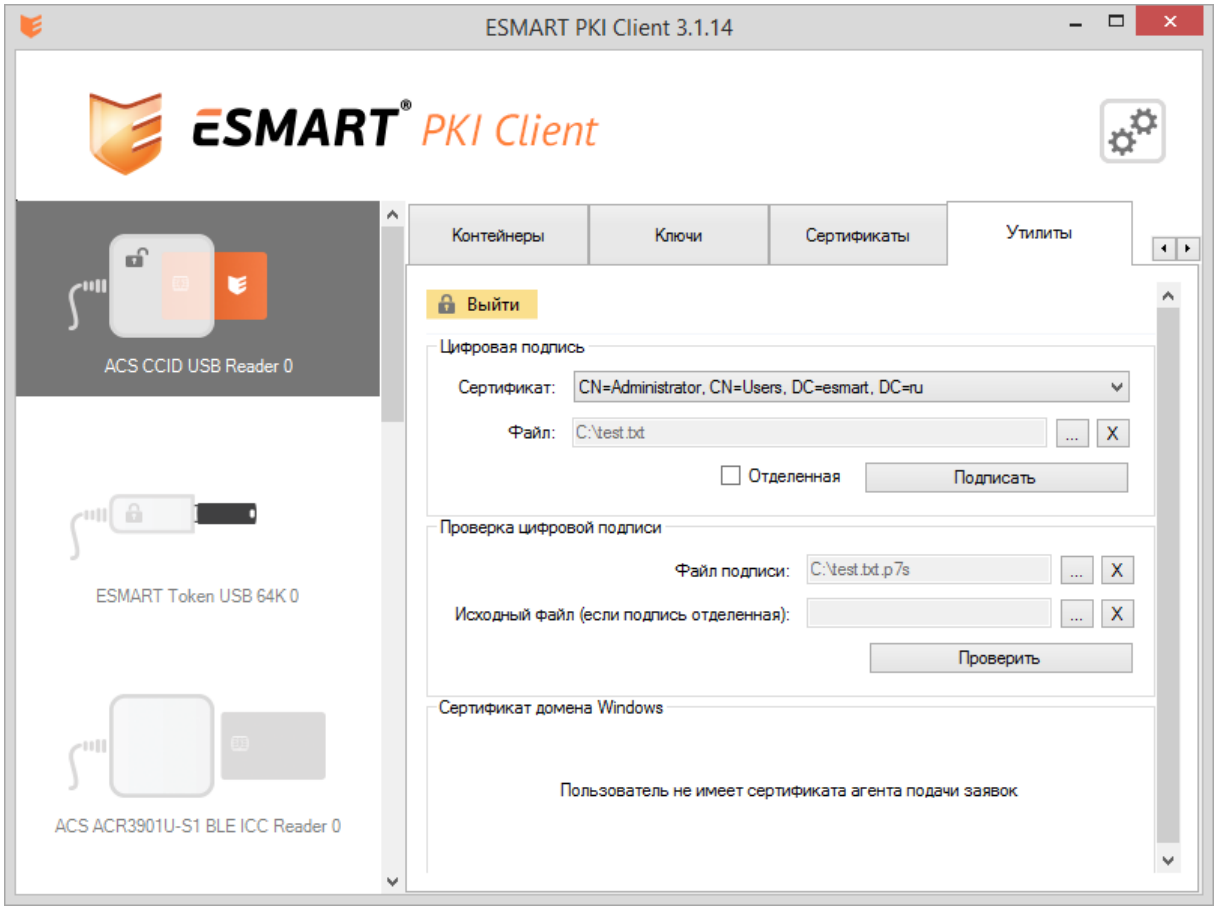
*Чтобы удалить сертификат, выберите его в списке и нажмите **Удалить**. Подтвердите выполнение операции.*



15. Утилиты

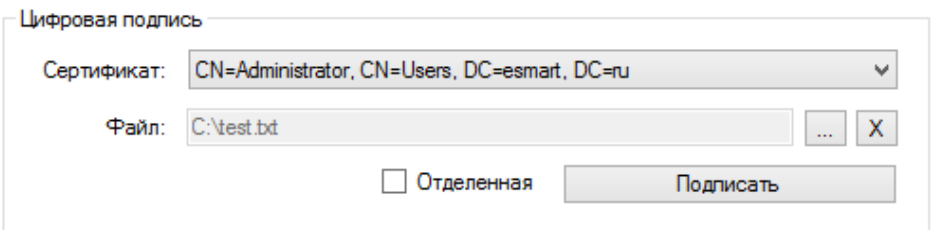
*На вкладке **Утилиты** собраны различные вспомогательные функции для работы с сертификатами и смарт-картами:*

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



15.1 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.

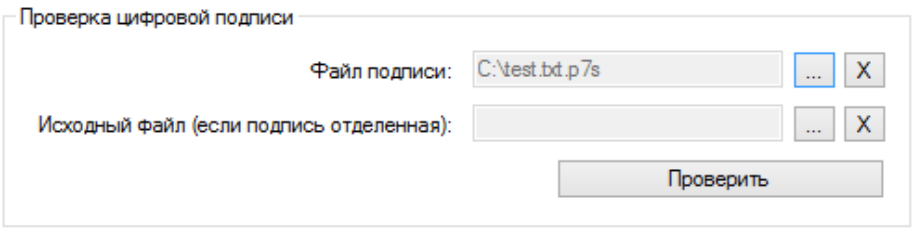


Чтобы воспользоваться функцией цифровой подписи файла выберите сертификат на карте, который будет использоваться для подписи и укажите файл, который будет подписан. Выберите тип подписи: отделяемая или неотделяемая. Оба типа подписи позволяют установить, был ли документ изменен с момента подписания.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

15.2 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****.*

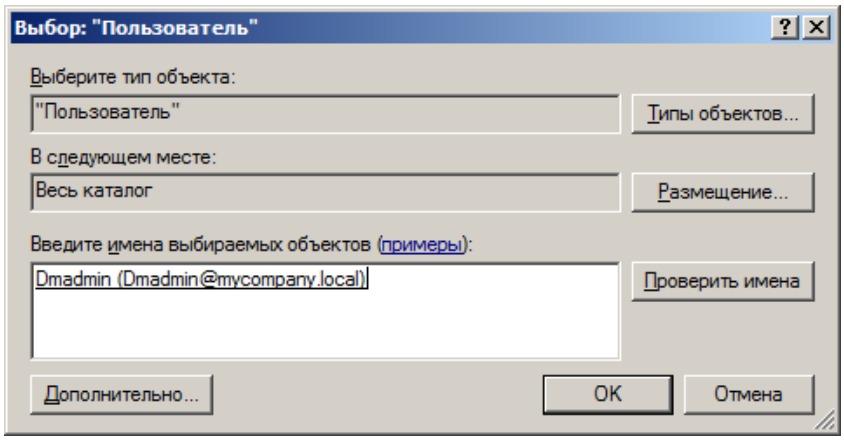


15.3 Выдача доменного сертификата

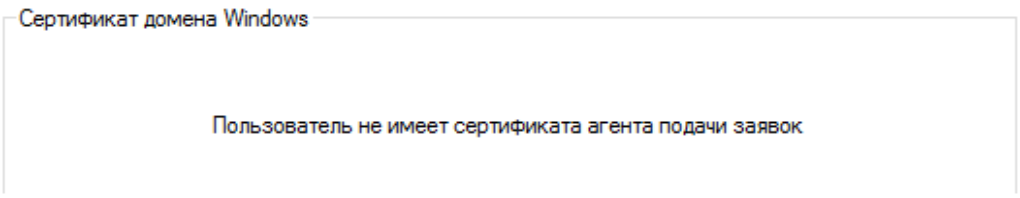
ESMART PKI Client позволяет упростить выдачу сертификата в домене на базе Windows Server 2003 или 2008 типа Enterprise. ESMART PKI Client позволяет выписать сертификат по шаблону ***Пользователь со смарт-картой*** *(Smartcard User).*

Как правило, сертификат для смарт-карты выписывает администратор. Для этого ему выдается специальный сертификат по шаблону Enrollment Agent (Агент подачи заявок).

Чтобы выписать сертификат при помощи ESMART PKI Client, укажите пользователя и нажмите ***Выпустить сертификат****.*



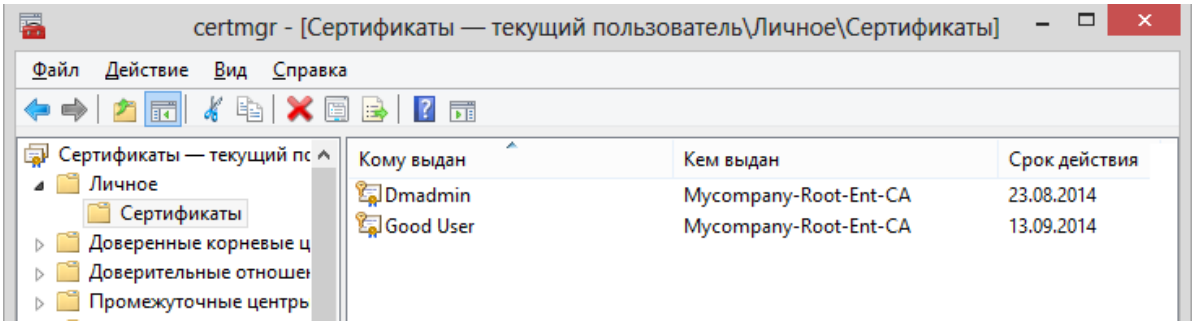
Обычным пользователям будет показано сообщение: Пользователь не имеет сертификата агента подачи заявок.



16. Работа с хранилищем сертификатов

Только для Windows. Требуются права администратора.

Для запуска хранилища сертификатов наберите в командной строке certmgr.msc или добавьте оснастку ***Сертификаты*** *(Текущий пользователь) в Консоли управления (MMC).*



Сертификаты пользователя находятся в папке ***Личное***.

Корневые сертификаты устанавливаются в папку ***Доверенные корневые центры сертификации***.

16.1 Установка доверенного корневого сертификата

Для корректной работы в Windows требуется, чтобы самоподписанные корневые сертификаты удостоверяющего центра, выдавшего сертификат пользователя, находились в папке ***Доверенные корневые сертификаты*** *в хранилище Windows.*

В хранилище сертификатов при установке ОС Windows автоматически добавляются корневые сертификаты важных организаций, например, Microsoft, Comodo, Thawte, VeriSign и др.

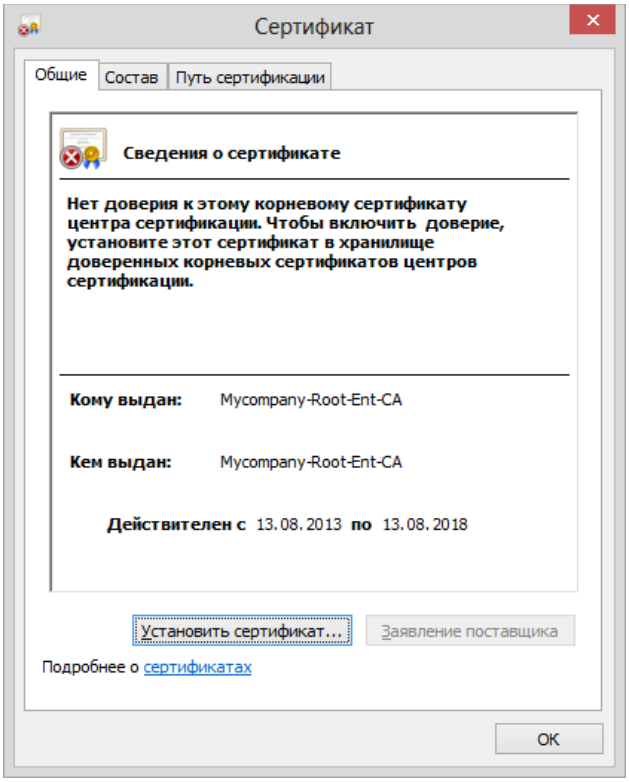
Внимание! *Без необходимости не следует удалять доверенные корневые сертификаты, т.к. это может приводить к сбоям в работе системы, невозможности авторизоваться на интернет-сайтах и другим проблемам.*

Если используются сертификаты, полученные от крупных УЦ, скорее всего дополнительных действий не потребуется.

Если используется корпоративный УЦ, соответствующий корневой сертификат необходимо импортировать в хранилище на каждом ПК. Для этого удобно хранить корневой сертификат на смарт-карте.

Получите корневой сертификат используемого УЦ. Как правило, корневой сертификат можно скачать через веб-интерфейс УЦ.

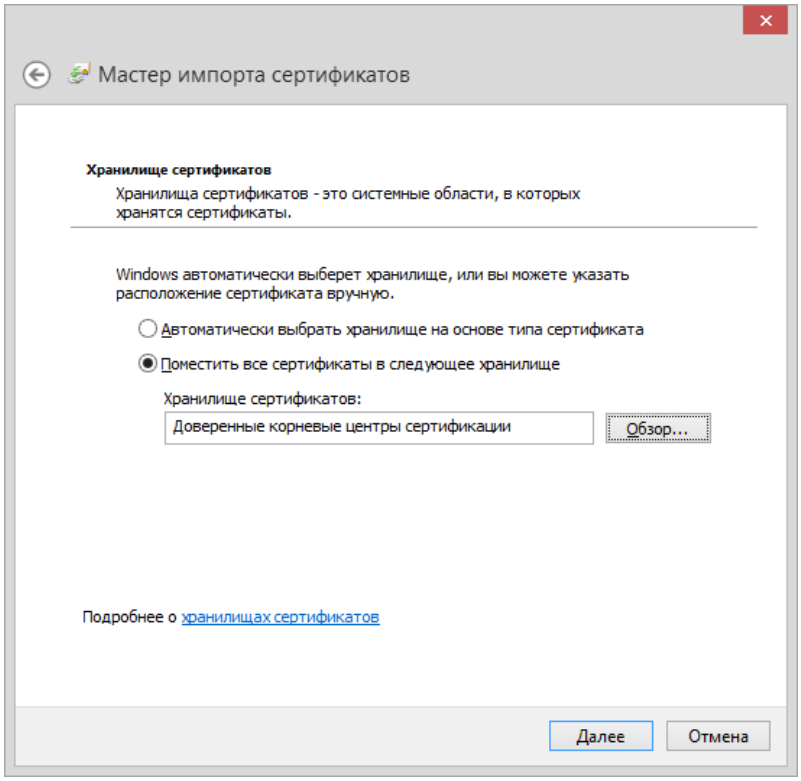
Как правило, корневые сертификаты имеют разрешение файла .crt. Откройте окно сертификата, щелкнув два раза левой кнопкой мыши по значку файла. Нажмите ***Установить сертификат***.



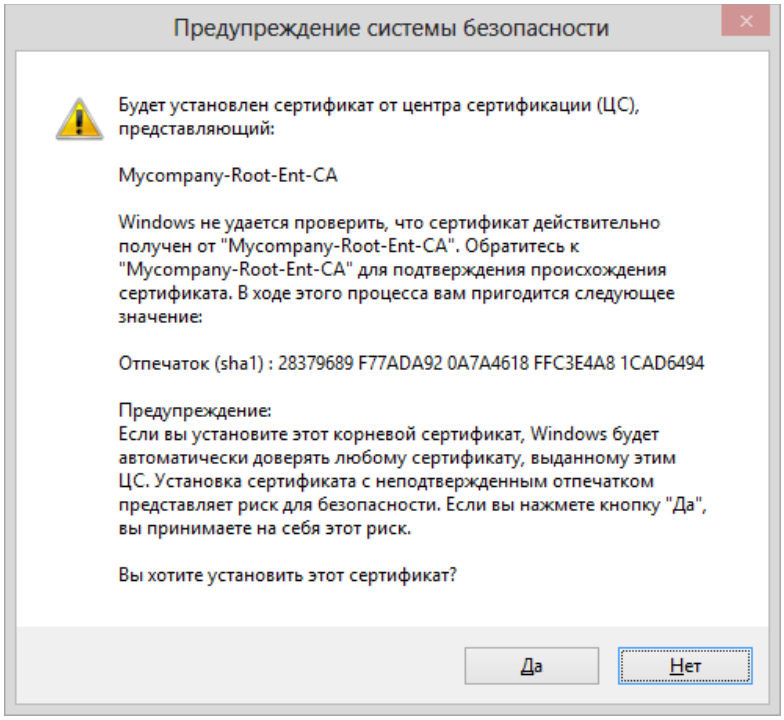
Запустится мастер установки сертификатов.

Выберите хранилище для установки:

- *Автоматически на основе типа сертификата – рекомендуется для пользователей;*
- *Поместить все сертификаты в следующее хранилище – рекомендуется для администраторов, если при автоматической установке тип сертификата определяется неверно.*



При установке корневых сертификатов требуется подтверждение операции.



Проверьте данные сертификата и подтвердите операцию. Проверьте, появился ли сертификат в папке хранилища ***Доверенные корневые сертификаты***.

17. Проверка параметров реестра

Только для Windows. Требуются права администратора.

Для корректной работы ESMART PKI Client требуется, чтобы соответствующие записи, ассоциированные с картами ESMART Token, присутствовали в реестре.

Чтобы проверить реестр, проделайте следующие операции:

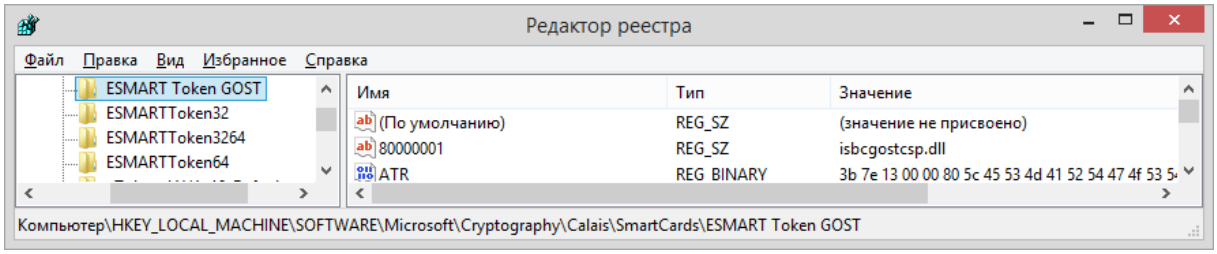
Запустите редактор реестра (Сочетанием WIN+R запустите командную строку. Введите ***regedit*** *для запуска редактора реестра).*

HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Cryptography\Calais\SmartCards

HKEY_LOCAL_MACHINE\SOFTWARE\ Wow6432Node\Microsoft\Cryptography\Calais\SmartCards (только для 64-битных систем)

В реестре должны быть следующие записи:

- *ESMART Token Gost*
- *ESMARTToken32*
- *ESMARTToken3264*
- *ESMARTToken64*



Если записи не найдены, воспользуйтесь файлами редактирования реестра из дистрибутива.
Структура папок:
ESMART CSP\registry files

- *x64 – для 64-битных систем*
  - *csp x64.reg – для добавления записей*
  - *remove csp x64.reg – для удаления записей*
- *x86 – для 32-битных систем*
  - *csp x64.reg – для добавления записей*
  - *remove csp x64.reg – для удаления записей*

ESMART GOST CSP\registry files

- *x64 – для 64-битных систем*
  - *csp x64.reg – для добавления записей*
  - *remove csp x64.reg – для удаления записей*
- *x86 – для 32-битных систем*
  - *csp x64.reg – для добавления записей*
  - *remove csp x64.reg – для удаления записей*

ESMART PKCS 11\registry files

- *x64 – для 64-битных систем*
  - *esmarttoken x64.reg – для добавления записей*
  - *remove esmarttoken x64.reg – для удаления записей*
- *x86 – для 32-битных систем*
  - *esmarttoken x64.reg – для добавления записей*
  - *remove esmarttoken x64.reg – для удаления записей*

Запустите файлы редактирования реестра двойным щелчком мыши. Подтвердите выполнение операции.

18. Возможные проблемы

Проблема	Способы устранения
Невозможно установить ESMART PKI Client	Требуются права администратора в Windows, права root в Linux
ESMART PKI Client не запускается в Linux	Для запуска программы в Linux требуется среда Mono. См. стр. 4
ESMART PKI Client не видит считыватель	Перезапустите приложение. Переустановите драйвер считывателя
Карта вставлена в считыватель, но не отображается	Проверьте: - тип карты ESMART Token - записи в реестре - наличие библиотек isbc_pkcs11_main.dll
В Windows XP приложение не работает	Для Windows XP требуется установка пакета Microsoft Base CSP
Карта заблокирована после ввода неверного ПИН-кода	Разблокируйте карту, используя ПИН-код администратора.
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
Ошибка при инициализации PKCS#11. Возможно в системе не установлены соответствующие библиотеки.	Переустановите ESMART PKI Client или установите библиотеки вручную. См. ESMART Token – PKCS11 и ESMART Token – CSP. Переустановите драйвер считывателя.
Криптопровайдер SignalCOM CSP не распознает или некорректно работает с ESMART Token	Переустановите или установите более новую версию ESMART PKI Client. При установке в реестр будут внесены все необходимые записи.