Руководство оператора СКЗИ «MS_KEY K» - «АНГАРА» Исп.8.x.x. с поддержкой технологии ISBC ESMART

Создание запросов и запись сертификатов ЭП для ЕГАИС с помощью ESMART PKI Client

V 1.3
ООО «НТЦ Альфа-Проект»
2019г.

Телефон: +7 (495) 215-51-61 Сайт: www.angara.cards E-mail: info@alfa-project.moscow

Список терминов и сокращений

Термин	Описание
MS_KEY ESMART АНГАРА	СКЗИ «MS_KEY K» - «АНГАРА» Исп.8.x.x с поддержкой технологии ISBC ESMART
ЕГАИС	Единая государственная автоматизированная информационная система
ЭП	Электронная подпись
КЭП	Квалифицированная электронная подпись
Электронный идентификатор, крипто-ключ, программно-аппаратный криптопровайдер	СКЗИ «MS_KEY K» - «АНГАРА»
ПО	Программное обеспечение, ESMART PKI Client
ОС	Операционная система

Введение

MS_KEY ESMART АНГАРА объединил в себе СКЗИ «MS_KEY K» - «АНГАРА» и технологию ISBC ESMART. Это устройство имеет широкую область применения, что позволяет использовать его в таких системах, как: ЕГАИС, КриптоПро и других системах защиты информации. Поддерживает интерфейсы APDU/PKCS#11. Более подробное описание смотрите в эксплуатационной документации.

В данной инструкции описывается процесс генерации с помощью приложения ESMART PKI Client ключевой пары ГОСТ 34.10-2012 (256 бит), создание запроса сертификата на основе этой ключевой пары и запись сертификата ЭП на ключевой носитель MS_KEY ESMART АНГАРА.

Этапы загрузки КЭП на программно-аппаратный криптопровайдер.

1. Установка ПО и авторизация на MS_KEY ESMART АНГАРА

- ***Установите приложение*** ESMART PKI Client ***актуальной версии***[1]. После скачивания архива извлеките содержимое в папку. Выберите установочный файл: setup.exe (для 32-х разрядной (ОС) или setup.x64.exe (для 64-х разрядной ОС). Далее следуйте подсказкам программы-инсталлятора. Перезагрузите компьютер, если появится соответствующее сообщение.

- ***Запустите приложение ESMART PKI Client.*** Для этого в трее (область в правом углу панели задач (Рис.1) разверните окно программы, нажав один раз по иконке программы левой кнопкой мыши. Для удобства запуска можно создать ярлык и поместить его на Рабочий стол. Если свернуть окно приложения, приложение не выключается, а сворачивается в трей.

Рис. 1

[1] На момент написания этой инструкции последней версией является ESMART PKI Client 4.5.1. от 28.Авг.2019

- ***Подключите электронный идентификатор.*** В главном окне программы появится информация об устройстве (Рис. 2).

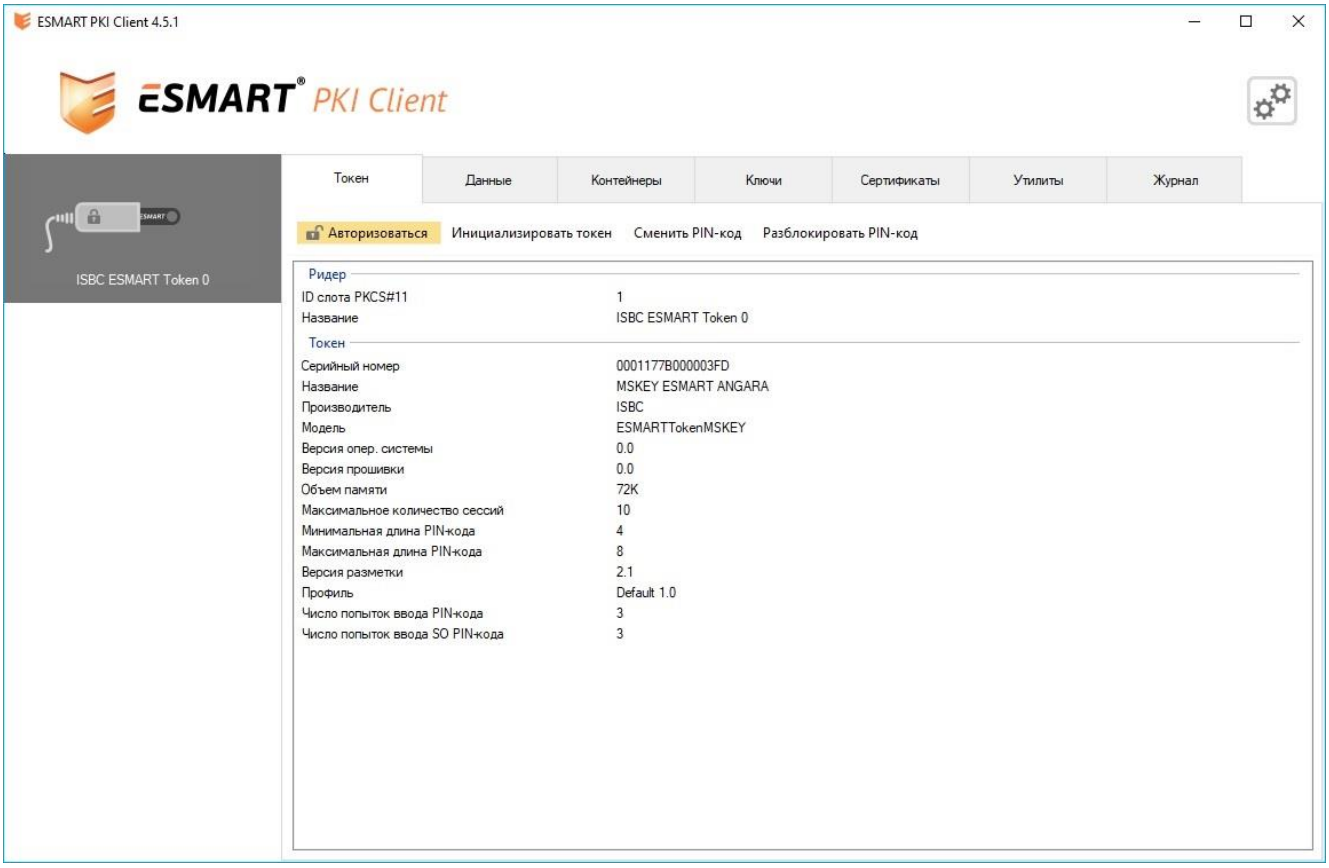

Рис. 2

- ***Пройдите авторизацию.*** Чтобы зарегистрироваться на электронном идентификаторе, нажмите «Авторизоваться**»** на верхней панели (Рис.3 а). В открывшемся окне введите восьмизначный PIN-код пользователя (Рис. 3 б).

По умолчанию ПИН-код пользователя: 12345678. Для интеллектуальных карт и USB-ключей MS_KEY ESMART АНГАРА также могут использоваться алфавитные и служебные символы. Оптимально, надежный пароль должен содержать символы минимум 3 типов, например, заглавные и строчные буквы и цифры, или буквы, цифры и служебные символы. Благодаря аппаратной защите PIN-код может быть проще, т.к. электронный идентификатор защищен от подбора пароля методом перебора. После того как несколько раз был введен неверный пароль, носитель блокируется. Получить доступ к хранящимся на заблокированном носителе ключам, данным и сертификатам невозможно. Разблокировать криптопровайдер может администратор, который предъявляет SO PIN.

После авторизации на карте откроется доступ к защищенным объектам, появится возможность создавать, импортировать и удалять объекты.

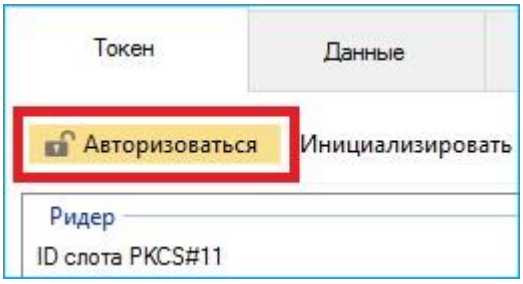

Рис. 3 а

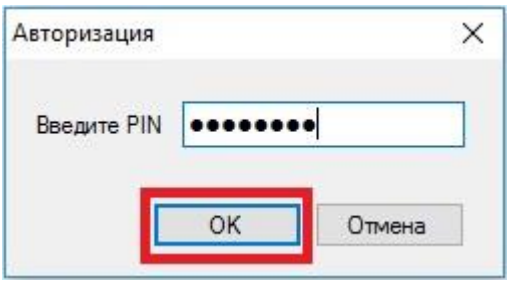

Рис. 3 б

2. Генерация ключевой пары

- ***Сгенерируйте ключевую пару***. Для этого перейдите во вкладку «Ключи», выберите пункт «Сгенерировать ключевую пару». В открывшемся окне выберите тип ключевой пары ГОСТ 34.10-2012, 256 бит. Нажмите кнопку «ОК» (Рис. 4).

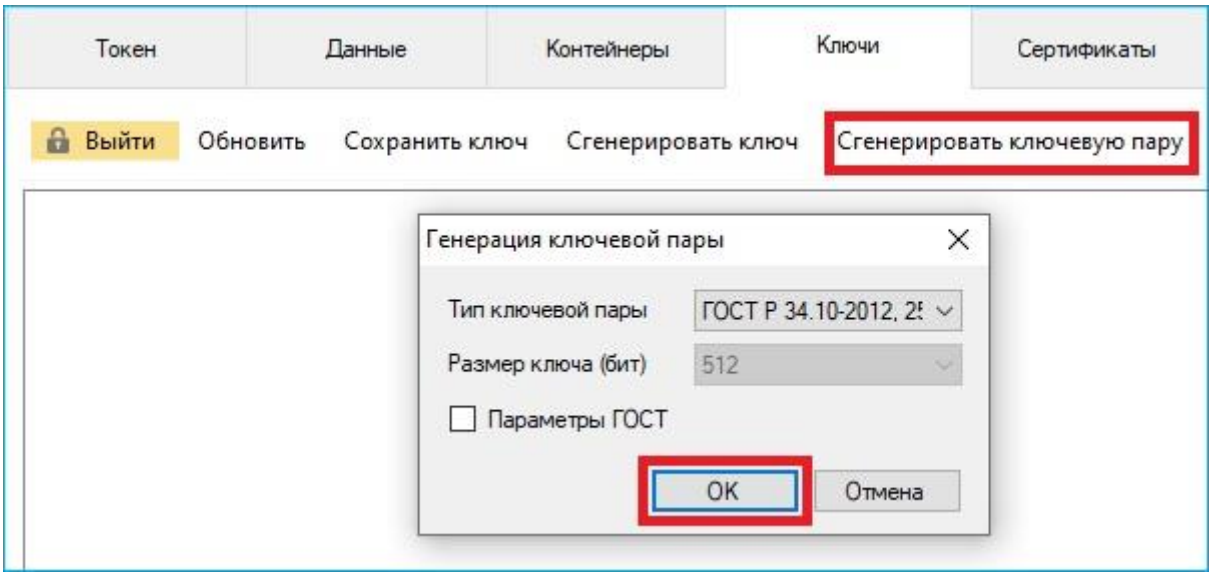

Рис. 4

- ***На основе созданной ключевой пары сформируйте запрос сертификата и сохранить его.*** Выберите нажатием левой клавиши мыши ключевую пару ГОСТ 34.10. В окне появятся дополнительные функции. Нажмите на пункт: «Запрос сертификата» (Рис. 5 а).

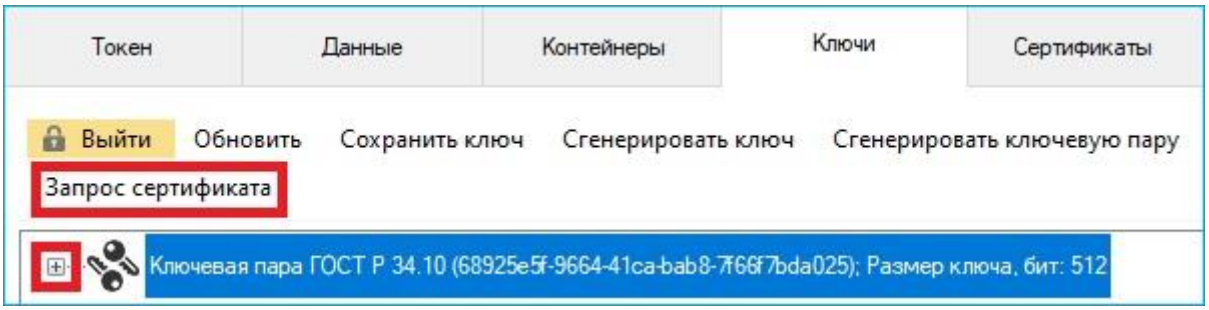

Рис. 5 а

При нажатии на символ «+» (Рис. 5 а), Вы можете просмотреть дополнительную информацию о ключевой паре (Рис. 5 б).

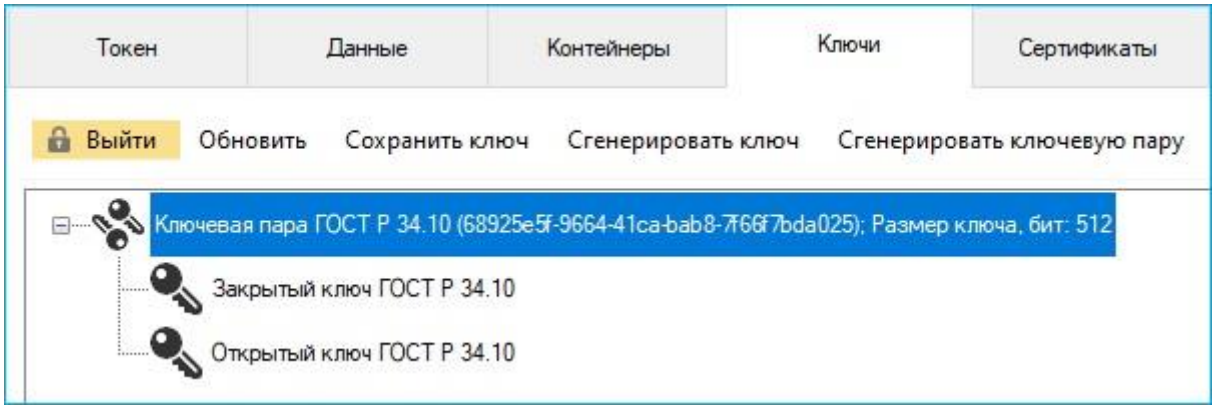

Рис. 5 б

3. Формирование запроса на сертификат ЭП

- ***Создайте запрос сертификата и сохраните его в файле.*** Заполните форму (Рис. 6 а):
  - укажите актуальные данные;
  - в пункте «Расширения» выберите опцию **«ЕГАИС»**;
  - укажите применение ключа: **«Электронная подпись», «Шифрование ключей», «Шифрование данных», «Неотрекаемость»**;
  - выберите параметр **«Юридическое лицо»** или **«Физическое лицо»**, на которое будет выдан сертификат[2];
  - Формат запроса рекомендуется выбрать **«PEM»**.

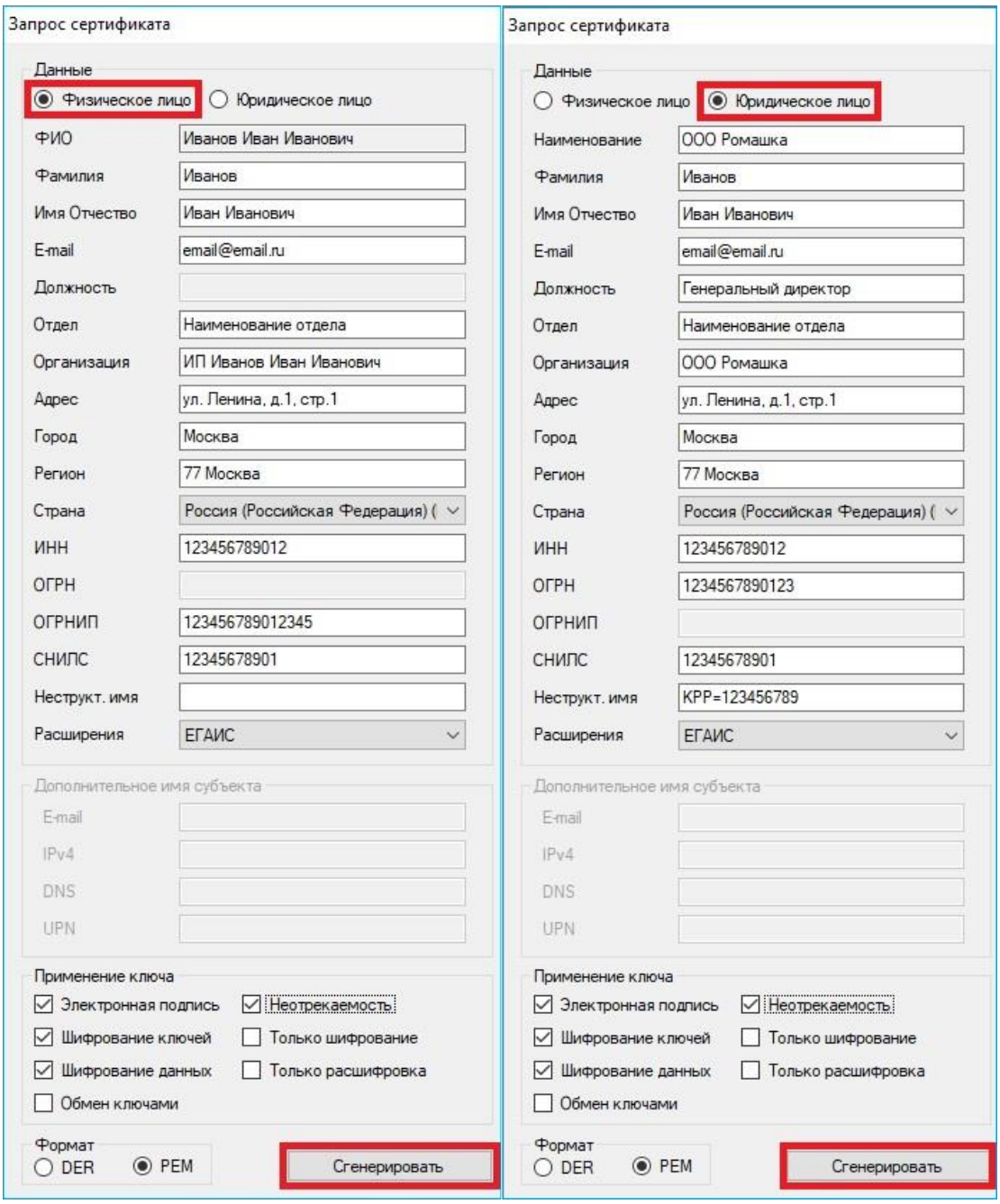

Рис. 6 а

[2] Неструктурированное имя: UN (1.2.840.113549.1.9.2) – обязательно к заполнению. Должен быть записан один из вариантов:
- для ЮЛ должны присутствовать 4 символа КПП= или KPP= и далее 9 цифр КПП организации, сотрудником которого является владелец СКПЭП.
- для ИП должны присутствовать только 4 символа КПП= или KPP=.

ОГРНИП: OGRNIP (1.2.643.100.5) (только для ИП). Текст длиной 15 цифр. Не разрешается использовать пробел в начале и в конце текста. Заполните это поле, если требуется.

Далее нажмите кнопку «Сгенерировать», и после формирования запроса сохраните его, нажав соответствующую клавишу. После успешного сохранения файла закройте окно запроса сертификата с помощью клавиши «Закрыть» (Рис. 6 б).

Рис. 6 б

- ***На основе сохранённого запроса сформируйте сертификат КЭП.*** Квалифицированный сертификат открытого ключа производится удостоверяющим центром (УЦ) с применением средств КЭП.

4. Записать сертификат на электронный идентификатор

- ***Запишите полученный сертификат на MS_KEY ESMART АНГАРА.*** Для этого перейдите во вкладку «Сертификаты» и нажмите кнопку «Добавить» (Рис. 7). Обратите внимание, что на момент записи сертификата вы должны быть авторизованы на устройстве.

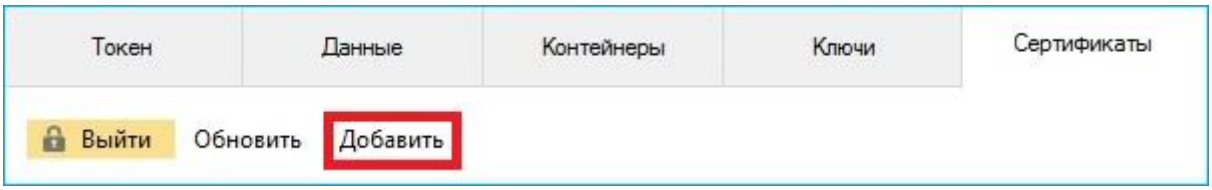

Рис. 7

В открывшемся окне выберите сертификат, который был сгенерирован по Вашему запросу и нажмите кнопку «Открыть» (Рис. 8).

Рис. 8

Нажмите на клавишу «ОК» в окне с уведомлением о завершении записи сертификата на электронный носитель (Рис. 9).

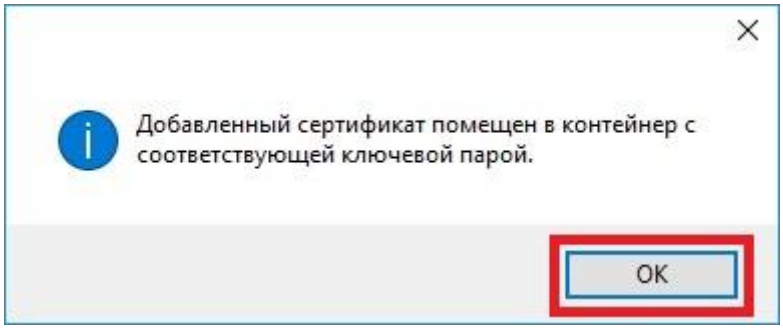

Рис. 9

- ***Контейнер сформирован.*** После завершения установки Вашего сертификата, информацию о нем можно посмотреть во вкладке «Контейнеры» (Рис. 10 а).

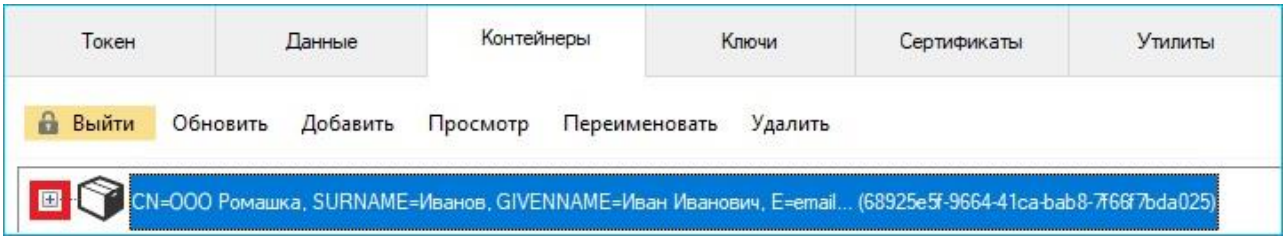

Рис. 10 а

При нажатии на значок «+» (Рис. 10 а) сформированного контейнера откроется его содержимое: ключевая пара и сертификат (Рис.10 б).

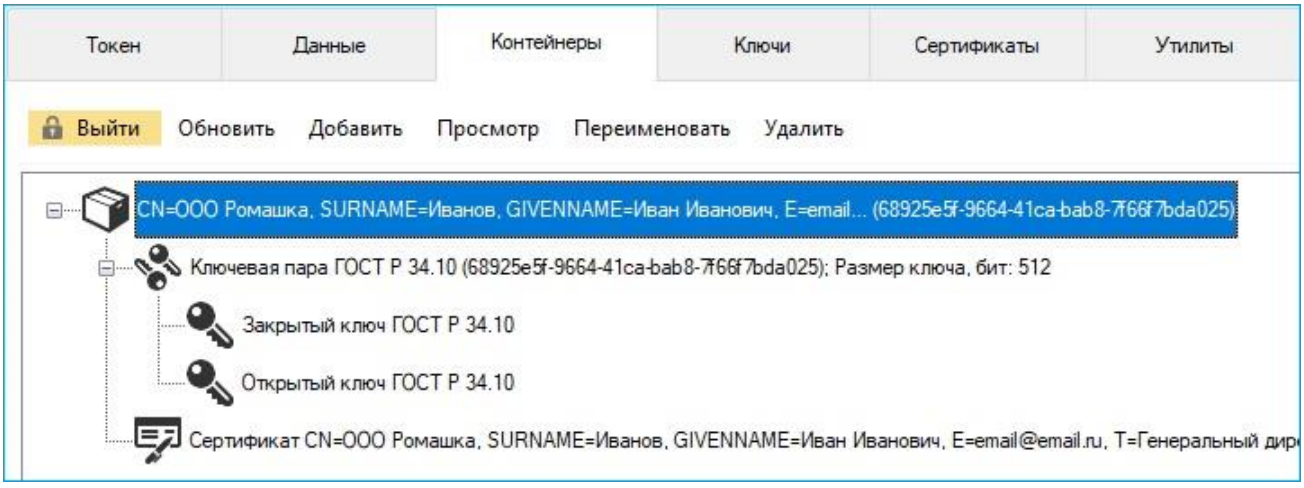

Рис. 10 б.