127018, Москва, Сущёвский Вал, 18
Телефон: (495) 995 4820
Факс: (495) 995 4820
https://CryptoPro.ru
E-mail: info@CryptoPro.ru

КРИПТОПРО

Средство Криптографической Защиты Информации

КриптоПро CSP Версия 5.0 KC1 1-Base Инструкция по использованию СКЗИ под управлением ОС iOS

ЖТЯИ.00101-01 92 02
Листов 31

2019 г

Содержание

1 Инсталляция СКЗИ КриптоПро CSP

Инсталляция, деинсталляция и обновление средства криптографической защиты информации (далее — СКЗИ) КриптоПро CSP версии 5.0 KC1 производится в составе прикладной программы, разработанной с применением КриптоПро CSP. При этих действиях следует руководствоваться документацией от производителя прикладной программы (как правило, это система документооборота или банк-клиент).

2 Интерфейс СКЗИ КриптоПро CSP

2.1 Доступ к контрольной панели СКЗИ

Данный раздел является инструкцией по использованию контрольной панели (панели настройки) СКЗИ КриптоПро CSP версии 5.0 КС1.

Панель настройки КриптоПро CSP доступна из прикладной программы, разработанной на базе СКЗИ. Метод вызова контрольной панели определяет разработчик прикладной программы.

Контрольная панель СКЗИ КриптоПро CSP (см. рис. 1) предоставляет доступ к следующим функциям:

- взаимодействие с УЦ;
- удаление ключей и сертификатов;
- установка сертификатов;
- удаление сохраненных паролей;
- управление лицензией;
- проверка целостности;
- скачивание и установка сертификатов и CRL.

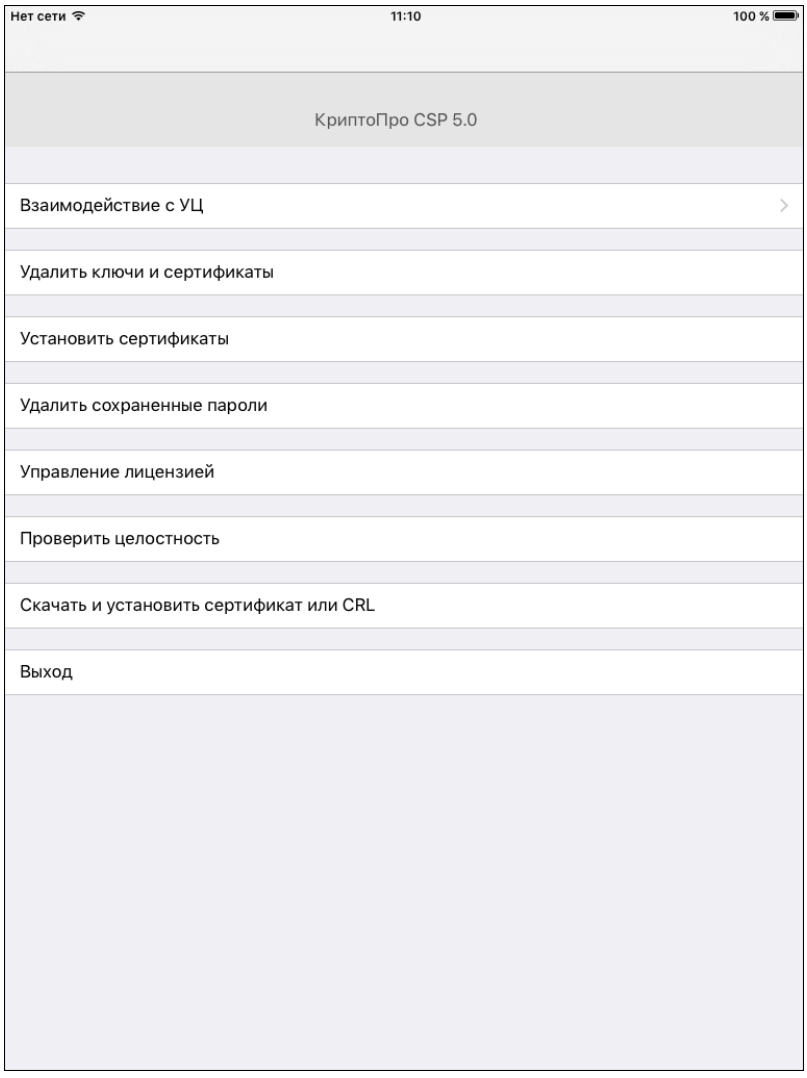

Рисунок 1. Контрольная панель СКЗИ КриптоПро CSP

2.2 Удаление ключей и сертификатов

Данная функция выполняет удаление с устройства всех закрытых ключей, ключей электронной подписи и сертификатов как личных, так и корневых. Для запуска процесса удаления нажмите кнопку «Удалить ключи и сертификаты» Контрольной панели и подтвердите действие в открывшемся окне (см. рис. 2). В случае успешного завершения процедуры появится окно с соответствующим сообщением (см. рис. 3).

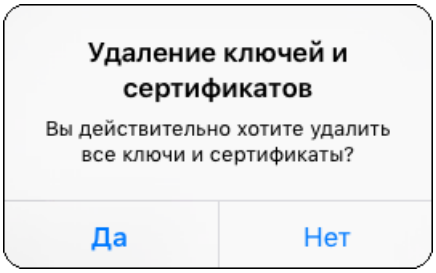

Рисунок 2. Диалоговое окно подтверждения удаления ключей и сертификатов

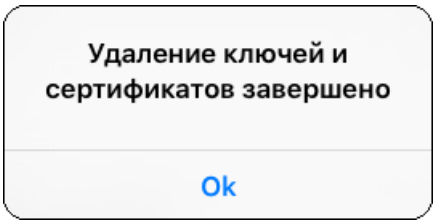

Рисунок 3. Успешное завершение процедуры удаления ключей и сертификатов

Примечание. Будьте внимательны при использовании данной функции, поскольку удаленные ключи невозможно восстановить.

2.3 Установка сертификатов

Функция осуществляет установку сертификатов из контейнеров на устройстве в соответствующие хранилища сертификатов. Для запуска процесса установки нажмите кнопку «Установить сертификаты» Контрольной панели и подтвердите действие в открывшемся окне (см. рис. 4). В случае успешного завершения процедуры появится окно с соответствующим сообщением (см. рис. 5).

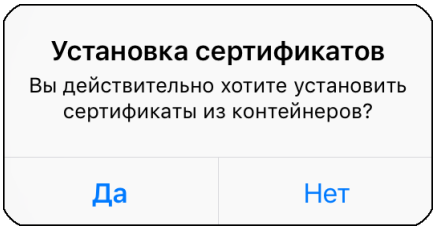

Рисунок 4. Диалоговое окно подтверждения установки сертификатов

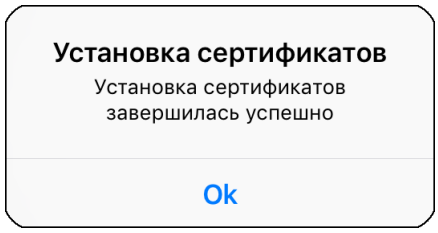

Рисунок 5. Успешное завершение процедуры установки сертификатов

2.4 Удаление сохраненных паролей

Для удаления запомненных паролей контейнеров закрытого ключа с устройства нажмите кнопку «Удалить сохраненные пароли» Контрольной панели и подтвердите действие в открывшемся окне (см. рис. 6). В случае успешного завершения процедуры появится окно с соответствующим сообщением (см. рис. 7).

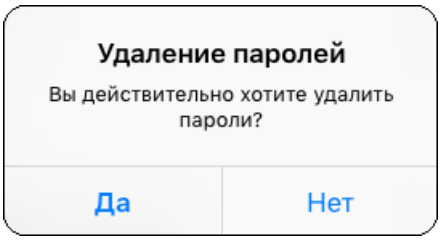

Рисунок 6. Диалоговое окно подтверждения удаления сохраненных паролей

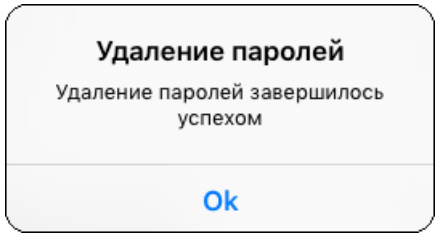

Рисунок 7. Успешное завершение процедуры удаления сохраненных паролей

2.5 Ввод серийного номера лицензии

При установке программного обеспечения КриптоПро CSP без ввода лицензии пользователю предоставляется лицензия с ограниченным сроком действия. Для использования КриптоПро CSP после окончания этого срока необходимо использовать лицензию, полученную у организации-разработчика или организации, имеющей права распространения продукта.

Существует три способа лицензирования КриптоПро CSP для ОС iOS:

1) Лицензия на приложение — производитель приложения поставляет его вместе с лицензией на CSP. Ввод лицензии пользователем не требуется.

2) Лицензия на сертификат — если удостоверяющий центр, который используется в информационной системе, поддерживает такую функцию, пользователь может запросить сертификат с расширением, в котором содержится лицензия на КриптоПро CSP. Эта лицензия распространяется только на действия с сертификатом, содержащим расширение.

3) Ввод лицензии пользователем через контрольную панель.

Для ввода/просмотра лицензии через контрольную панель необходимо нажать кнопку «Управление лицензией». Откроется диалоговое окно управления лицензиями (см. рис. 8), информирующее о сроке действия лицензии либо ее отсутствии.

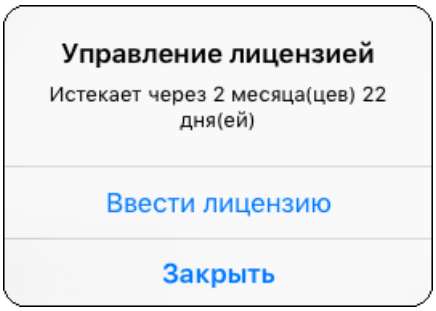

Рисунок 8. Диалоговое окно управления лицензиями

Для ввода нового серийного номера лицензии нажмите кнопку «Ввести лицензию». Откроется окно ввода лицензии (см. рис. 9). После ввода нового серийного номера текущая лицензия заменится на новую.

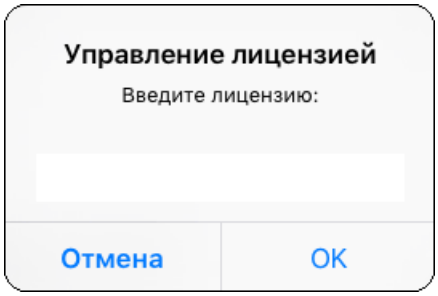

Рисунок 9. Окно ввода лицензии

2.6 Проверка целостности

Функция осуществляет проверку целостности КриптоПро CSP и прикладной программы, разработанной на базе СКЗИ. Для проверки целостности нажмите кнопку Проверить целостность из Контрольной панели СКЗИ. В открывшемся окне (см. рис. 10) отображается информация о результатах проверки, параметрах версии КриптоПро CSP, а также ожидаемое и полученное в ходе проверки значения хэш-функции приложения.

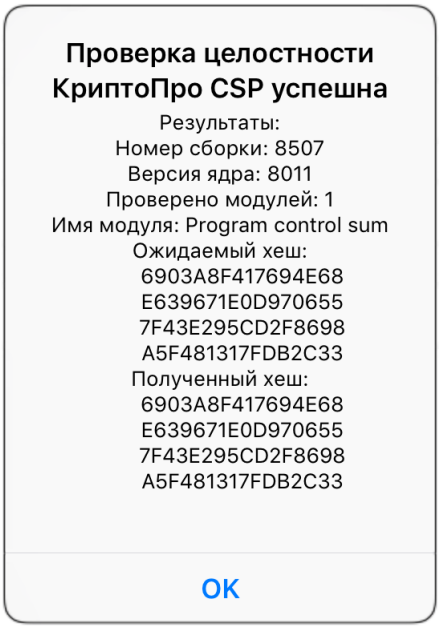

Рисунок 10. Окно с результатами проверки целостности приложения

2.7 Установка внешних сертификатов и CRL

Для обеспечения доверия к сертификатам, выданным определенным УЦ, и получения сведений об отозванных сертификатах необходимо загрузить сертификаты УЦ и актуальные списки отозванных сертификатов (COC, CRL). Загружаемые сертификаты будут установлены в хранилище сертификатов Root, а CRL — в хранилище CA.

Для скачивания сертификата или CRL нажмите кнопку «Скачать и установить сертификат или CRL» Контрольной панели СКЗИ. В открывшемся окне (см. рис. 11) введите адрес для скачивания и подтвердите действие. В случае успешного завершения процедуры появится окно (см. рис. 12) с результатами установки сертификатов/CRL и количеством установленных объектов.

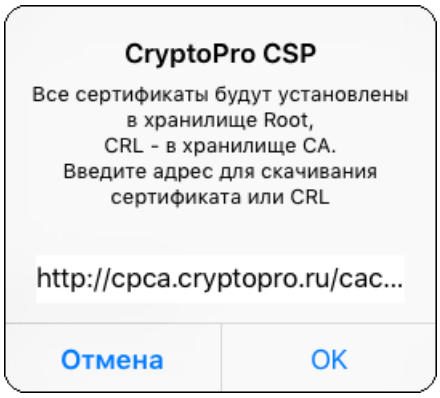

Рисунок 11. Диалоговое окно загрузки сертификатов/CRL

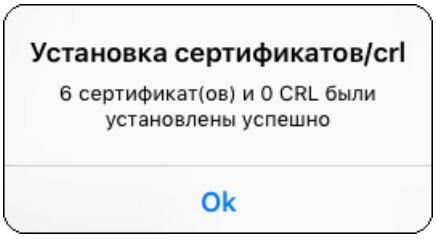

Рисунок 12. Успешное завершение процедуры установки сертификатов/CRL

2.8 Взаимодействие с УЦ

Настройка параметров взаимодействия с УЦ осуществляется с помощью панели взаимодействия с УЦ, которая доступна по кнопке «Взаимодействие с УЦ» Контрольной панели КриптоПро CSP. Панель взаимодействия с УЦ имеет различный вид в зависимости от выбранного типа УЦ.

КриптоПро CSP для ОС iOS поддерживает работу с удостоверяющими центрами типов КриптоПро УЦ 1.5, КриптоПро УЦ 2.0 и изолированный УЦ Microsoft (Microsoft CA Standalone). Для выбора типа УЦ нажмите кнопку «Тип УЦ». В открывшемся окне (см. рис. 13) выберите необходимый тип УЦ из списка.

Рисунок 13. Окно выбора типа УЦ

2.8.1 Взаимодействие с КриптоПро УЦ 1.5

2.8.1.1 Настройка подключения к УЦ

Для настройки подключения к УЦ откройте панель взаимодействия с УЦ и установите тип УЦ «КриптоПро УЦ 1.5». Панель взаимодействия с УЦ выглядит следующим образом (см. рис. 14).

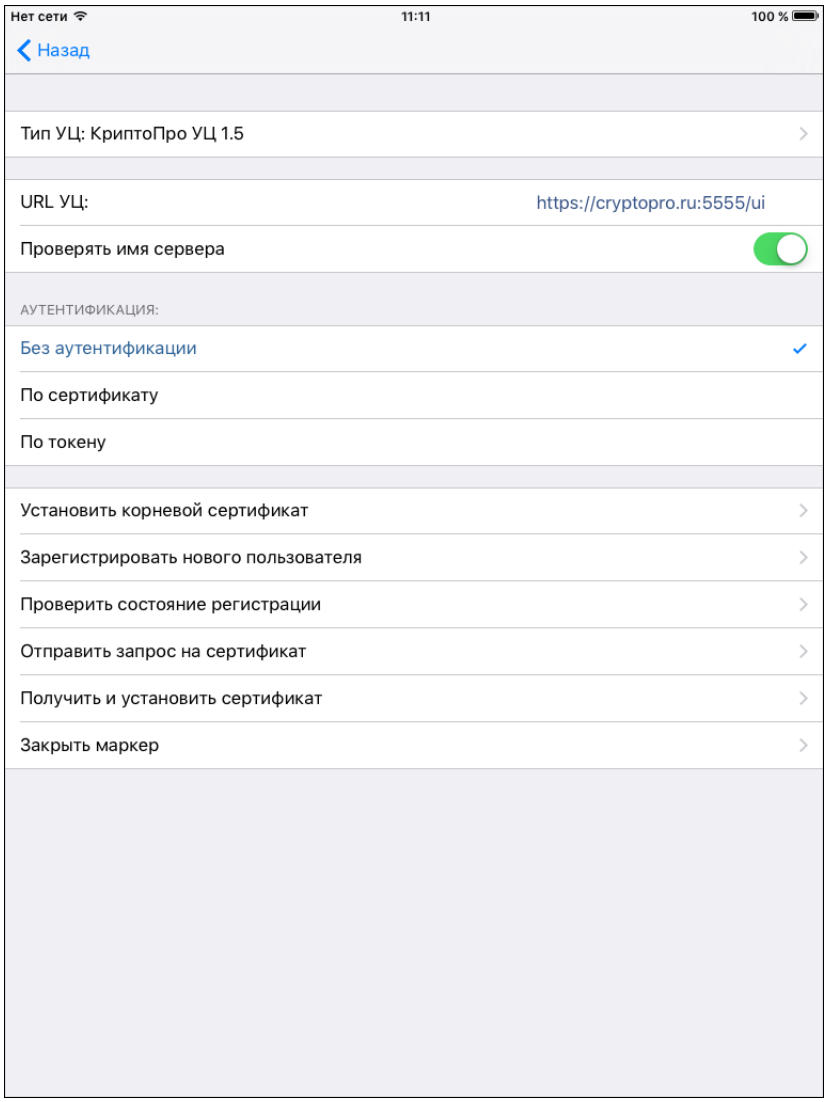

Рисунок 14. Панель взаимодействия с УЦ КриптоПро УЦ 1.5

Для установки адреса УЦ нажмите на «URL УЦ» и введите адрес. Как правило, адрес имеет формат https://<имя сервера>/ui. Для демонстрации работы КриптоПро CSP использовался тестовый УЦ ООО «КРИПТО-ПРО» https://www.cryptopro.ru:5555/ui типа КриптоПро УЦ 1.5.

Опция «Проверять имя сервера» определяет, требуется ли при работе с УЦ проверять соответствие адреса УЦ и имени сервера из сертификата. В целях безопасности рекомендуется не выключать эту опцию.

В случае использования типа УЦ КриптоПро УЦ 1.5 доступны следующие типы аутентификации пользователя УЦ:

- Без аутентификации;
- По сертификату;
- По токену.

Для осуществления аутентификации по сертификату нажмите на кнопку «По сертификату». Откроется окно выбора сертификата для аутентификации (см. рис. 15). После выбора сертификата его отпечаток отобразится в поле «По сертификату» (см. рис. 16), а само поле будет выделено цветом.

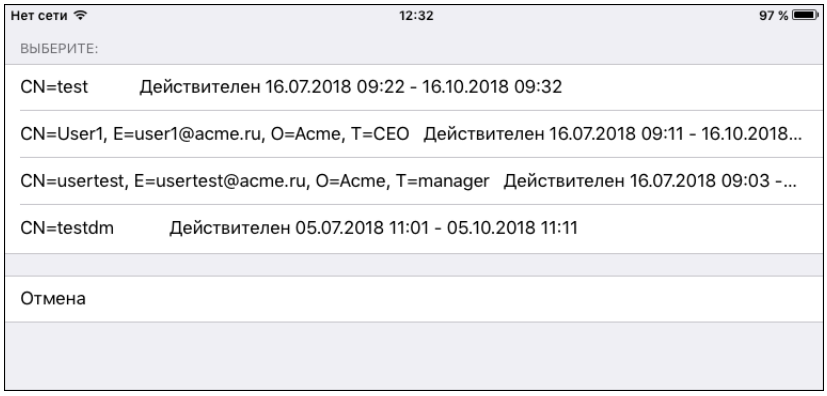

Рисунок 15. Окно выбора сертификата для аутентификации

Рисунок 16. Вид панели при аутентификации по сертификату

После установки данного типа аутентификации при осуществлении запроса к УЦ (например, при отправки запроса на сертификат) будет запрошен пароль от контейнера закрытого ключа, соответствующего выбранному сертификату (см. рис. 17).

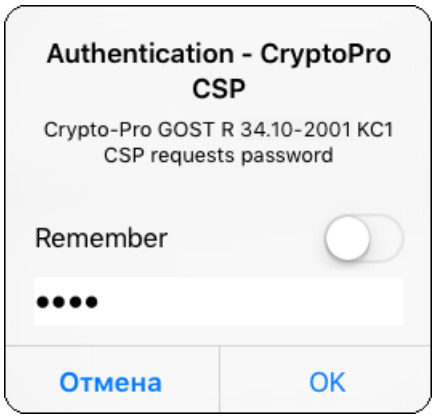

Рисунок 17. Окно ввода пароля контейнера

Для осуществления аутентификации по токену нажмите на кнопку «По токену». Откроется окно ввода идентификатора (ID) и пароля маркера временного доступа, выданного УЦ (см. рис. 18). После ввода и проверки данных ID маркера отобразится в поле «По токену», (см. рис. 19), а само поле будет выделено цветом.

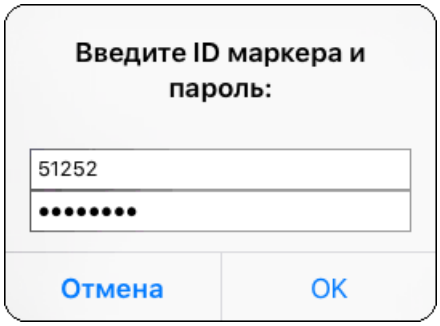

Рисунок 18. Окно ввода данных маркера для аутентификации

Рисунок 19. Вид панели при аутентификации по токену

2.8.1.2 Установка корневого сертификата

Перед началом взаимодействия с выбранным УЦ необходимо установить его корневой сертификат в хранилище устройства. Для установки корневого сертификата УЦ нажмите на кнопку «Установить корневой сертификат» на панели взаимодействия с УЦ. Откроется окно подтверждения установки сертификата, где также содержится отпечаток сертификата (см. рис. 20).

Рисунок 20. Диалоговое окно подтверждения установки корневого сертификата УЦ

В целях безопасности рекомендуется проверить соответствие отпечатка сертификата из сообщения и отпечатка сертификата выбранного УЦ. Отпечаток сертификата УЦ необходимо получить из доверенного источника.

В случае успешного завершения установки корневого сертификата УЦ откроется окно с соответствующим сообщением (см. рис. 21). Аналогичное окно отображается также в случае попытки установки сертификата УЦ, который уже установлен в хранилище устройства.

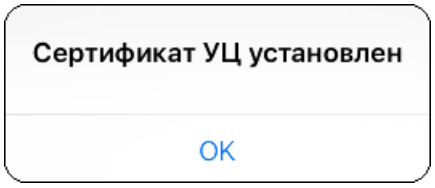

Рисунок 21. Сообщение об успешной установке сертификата УЦ

Если установка сертификата невозможна по причине, например, отсутствия соединения с сервером или некорректно указанного адреса УЦ, откроется окно с уведомлением об ошибке (см. рис. 22).

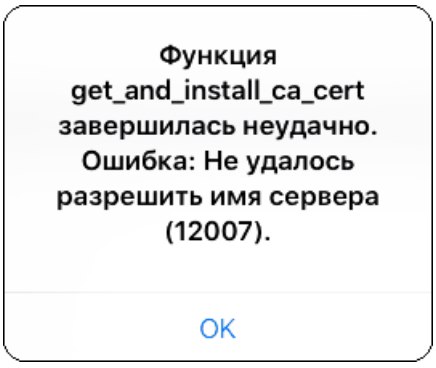

Рисунок 22. Сообщение об ошибке установки сертификата УЦ

2.8.1.3 Регистрация пользователя на УЦ

Для аутентификации пользователя УЦ может быть использован маркер временного доступа. Маркер временного доступа выдается пользователю при его регистрации. Для регистрации нового пользователя нажмите кнопку «Зарегистрировать нового пользователя» панели взаимодействия с УЦ. Откроется окно регистрационной формы (см. рис. 23). Внесите в форму сведения о пользователе и нажмите кнопку «Зарегистрировать».

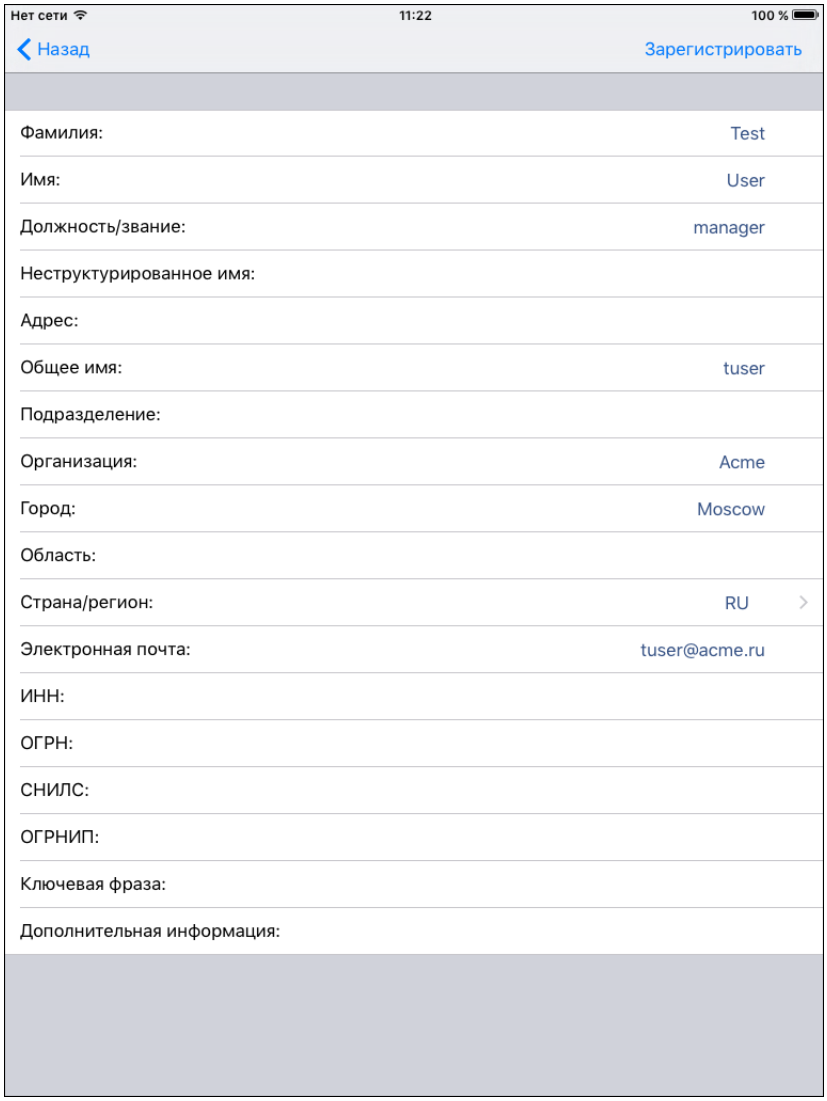

Рисунок 23. Форма регистрации пользователя УЦ

Если введенные данные не будут соответствовать политике имён УЦ (например, не будут заполнены какие-либо из обязательных полей или будет превышена максимальная длина для какого-либо поля), откроется окно с описанием ошибки и форма не будет отправлена на регистрацию.

В случае корректного заполнения регистрационной формы после нажатия на кнопку «Зарегистрировать» запрос уйдет на обработку. По окончанию процесса регистрации откроется окно, содержащее информацию о статусе регистрации пользователя, ID маркера и пароль (см. рис. 24). Можно автоматически настроить панель взаимодействия с УЦ на работу по этому токену и паролю. Для этого в появившемся окне нужно нажать «Да». В противном случае можно будет ввести ID и пароль маркера позже вручную (см. рис. 18), для этого регистрационную информацию необходимо будет запомнить или сохранить.

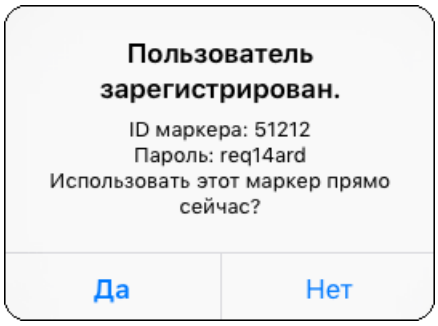

Рисунок 24. Окно с параметрами выданного пользователю токена

2.8.1.4 Проверка состояния запроса на регистрацию

Статус обработки запроса на регистрацию пользователя можно проверить, нажав кнопку «Проверить состояние регистрации» панели взаимодействия с УЦ. В открывшемся окне (см. рис. 25) отобразятся сведения о состоянии регистрации и идентификатор запроса, который может понадобиться при общении с администратором центра регистрации.

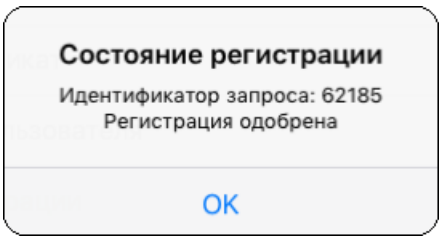

Рисунок 25. Окно проверки состояния регистрации пользователя

2.8.1.5 Создание и отправка запроса на сертификат

Для создания запроса на сертификат нажмите на кнопку «Отправить запрос на сертификат» на панели взаимодействия с УЦ. Откроется окно создания запроса на сертификат (см. рис. 26).

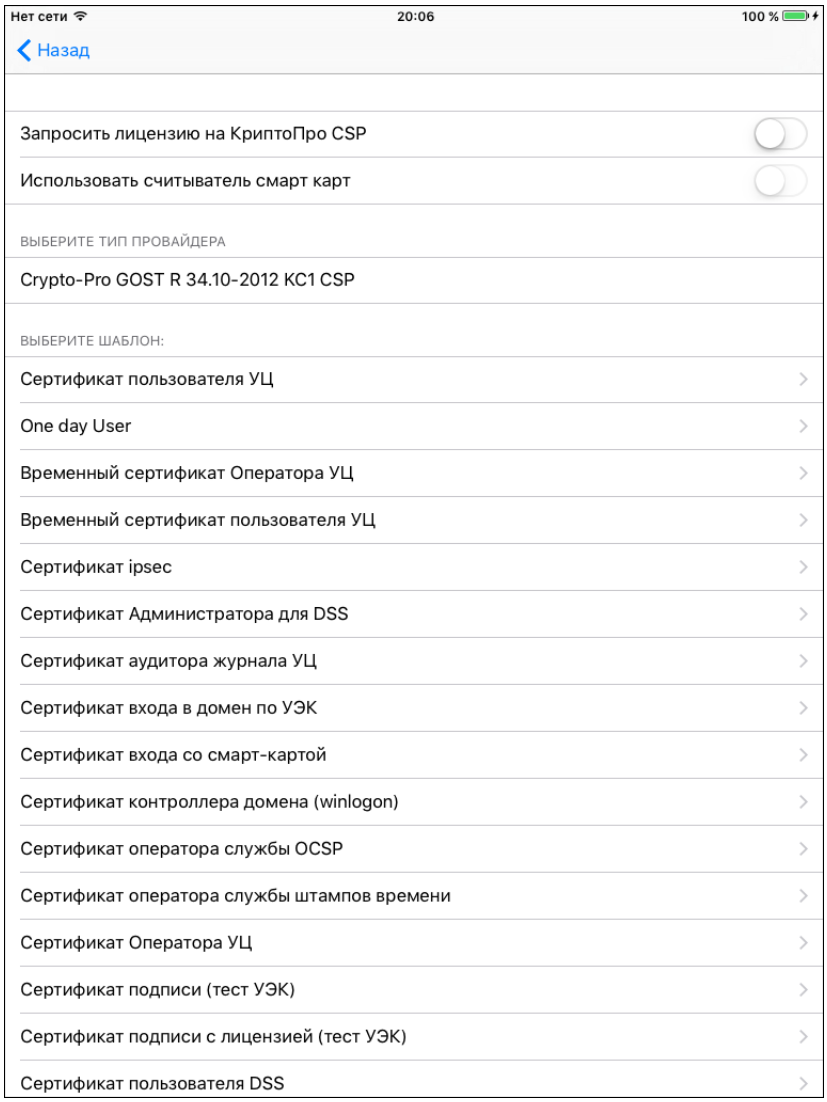

Рисунок 26. Форма запроса на сертификат

Примечание. Установку дополнительных параметров (например, запрос лицензии или выбор типа провайдера) необходимо выполнять до выбора шаблона.

При заполнении формы запроса на сертификат для выбора доступны следующие параметры:

• **запрос лицензии на КриптоПро CSP** (подробнее см. разд. 2.5) — создание запроса на сертификат, содержащий лицензию на КриптоПро CSP. Получение такого сертификата возможно, только если удостоверяющий центр, с которым вы работаете, поддерживает эту функцию. Если администратор УЦ или иное уполномоченное УЦ лицо не сообщило вам, что необходимо использовать эту функцию, не используйте её; в противном случае Ваш запрос, вероятно, будет отклонён на УЦ.

• **использование считывателя смарт-карт** — опция активна в случае наличия считывателя.

• **тип провайдера** — в зависимости от используемых алгоритмов ЭП и хэширования доступны следующие криптопровайдеры:

  - Crypto-Pro GOST R 34.10-2001 KC1 CSP;
  - Crypto-Pro GOST R 34.10-2012 KC1 CSP;
  - Crypto-Pro GOST R 34.10-2012 Strong KC1 CSP.
- **шаблон** — определяет назначение сертификата.

После нажатия на название шаблона откроется окно биологического датчика случайных чисел (ДСЧ) (см. рис. 27). Для генерации случайной последовательности нажимайте на экран устройства.

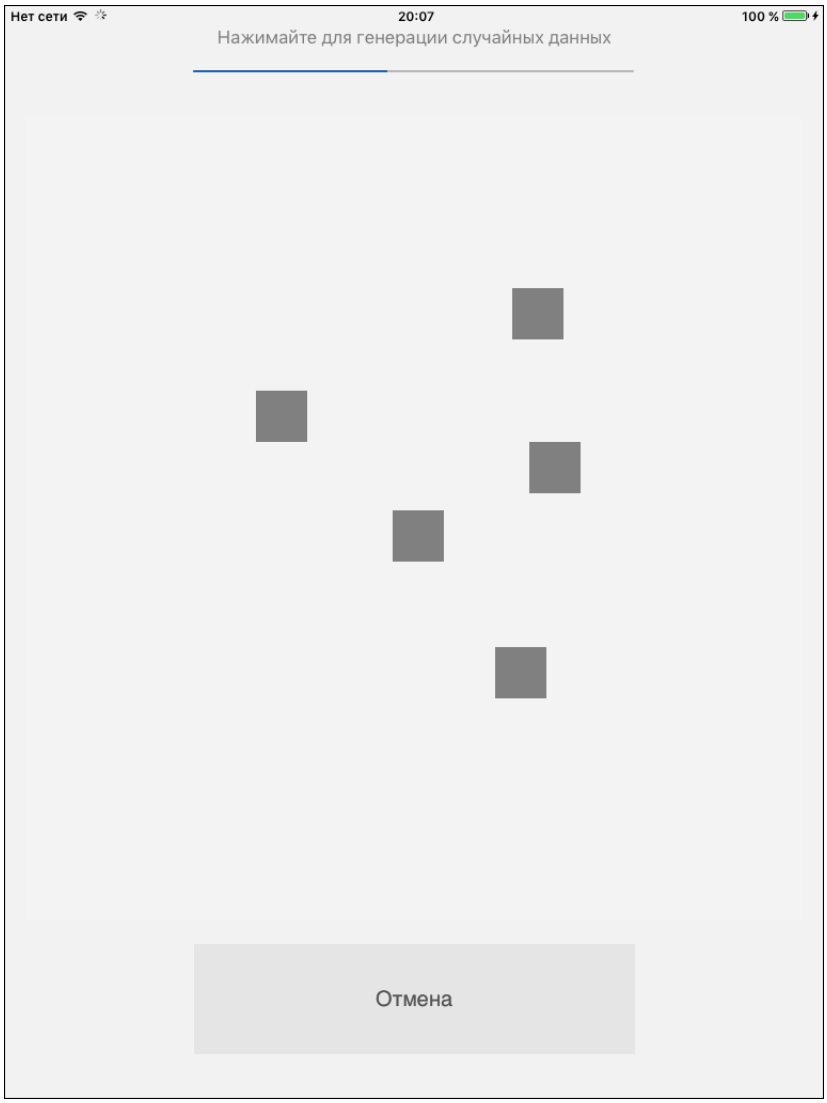

Рисунок 27. Окно биологического ДСЧ

После завершения работы биологического ДСЧ и генерации ключа откроется окно установки пароля на контейнер закрытого ключа (см. рис. 28). Дважды введите пароль и нажмите кнопку «OK». Если оставить строки пустыми, пароль не будет установлен.

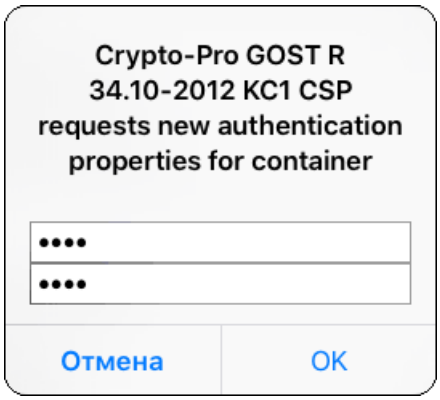

Рисунок 28. Окно установки пароля на контейнер

После этого запрос будет отправлен в УЦ.

2.8.1.6 Получение и установка сертификата

Кнопка «Получить и установить сертификат» на панели взаимодействия с УЦ позволяет просмотреть перечень созданных запросов на сертификат и их статус, установить сертификат, если он выдан, а также просмотреть и распечатать бланки сертификата и запроса на сертификат.

Для просмотра перечня созданных запросов нажмите на кнопку «Получить и установить сертификат». Откроется окно «Запросы на сертификат» (рис. 29), где отображаются идентификаторы, даты отправки и обработки, а также состояния запросов.

Рисунок 29. Перечень запросов на сертификат

Если запрос находится в состоянии **Завершен**, то при нажатии на него откроется бланк выданного сертификата (рис. 30). По кнопке «Напечатать» можно отправить бланк на печать. Для просмотра бланка запроса на сертификат нажмите кнопку «Перейти к запросу». Откроется бланк запроса на сертификат (см. рис. 31), который также можно отправить на печать.

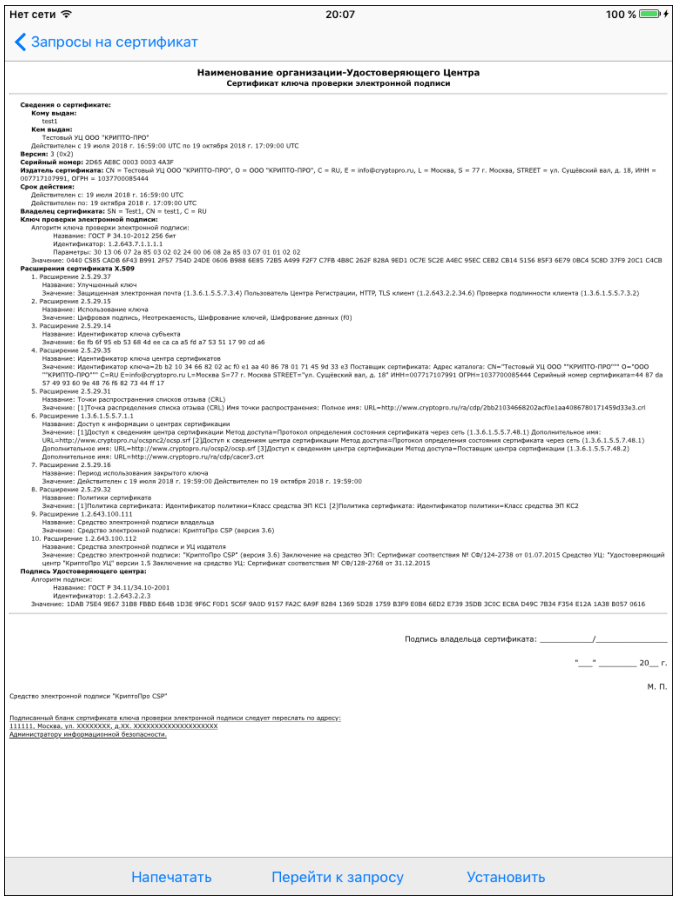

Рисунок 30. Бланк сертификата ключа проверки ЭП

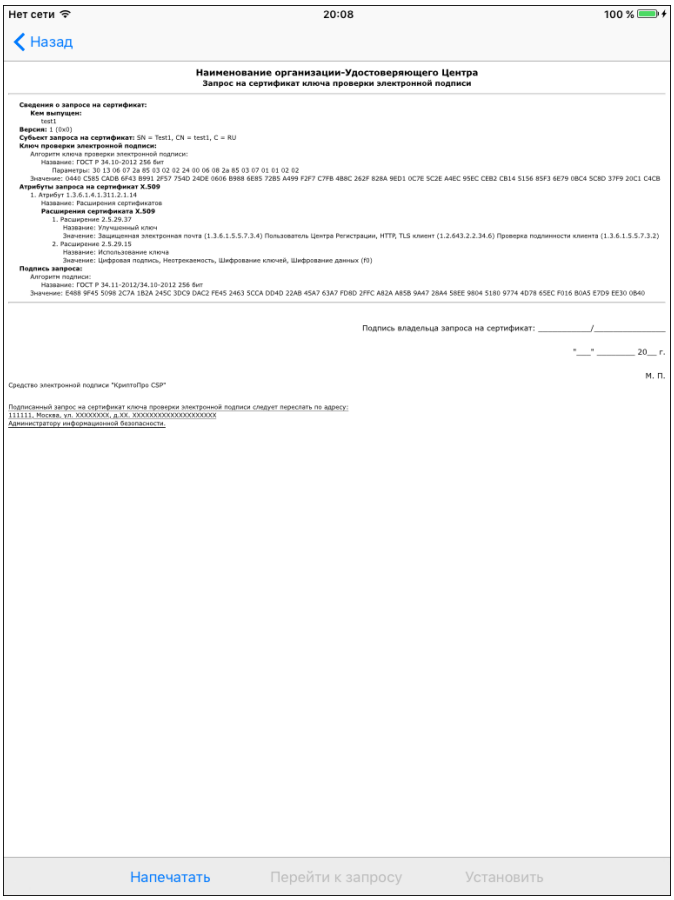

Рисунок 31. Бланк запроса на сертификат

Для установки выданного сертификата нажмите кнопку «Установить» в окне с бланком сертификата. Если на соответствующий контейнер был установлен пароль, введите его в открывшемся окне аутентификации (см. рис. 32).

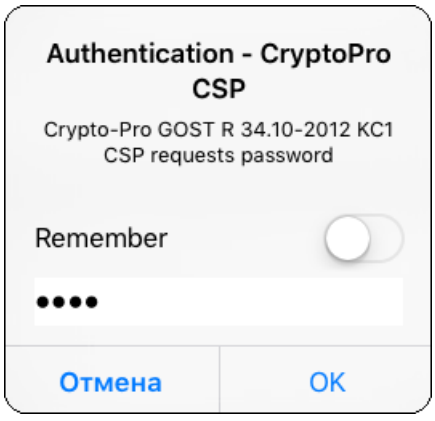

Рисунок 32. Ввод пароля на доступ к контейнеру

После этого сертификат будет установлен в хранилище устройства.

2.8.1.7 Закрытие маркера временного доступа

В случае осуществления аутентификации на УЦ с помощью маркера временного доступа по окончанию работы с УЦ его можно закрыть. Для этого нажмите на кнопку «Закрыть маркер» на панели взаимодействия с УЦ. Откроется окно с запросом подтверждения на закрытие маркера (см. рис. 33).

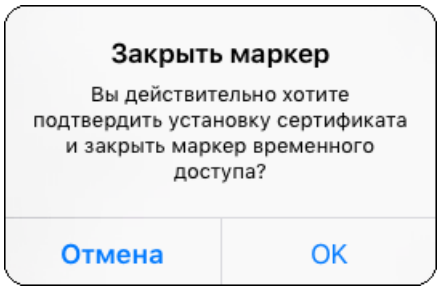

Рисунок 33. Диалоговое окно подтверждения закрытия маркера

В случае успешного закрытия маркера откроется окно с соответствующим сообщением (см. рис. 34).

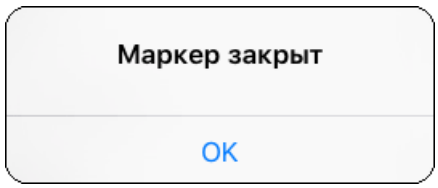

Рисунок 34. Сообщение об успешном закрытии маркера временного доступа

2.8.2 Взаимодействие с КриптоПро УЦ 2.0

Для настройки подключения к УЦ откройте панель взаимодействия с УЦ и установите тип УЦ «КриптоПро УЦ 2.0». Панель взаимодействия с УЦ выглядит следующим образом (см. рис. 35).

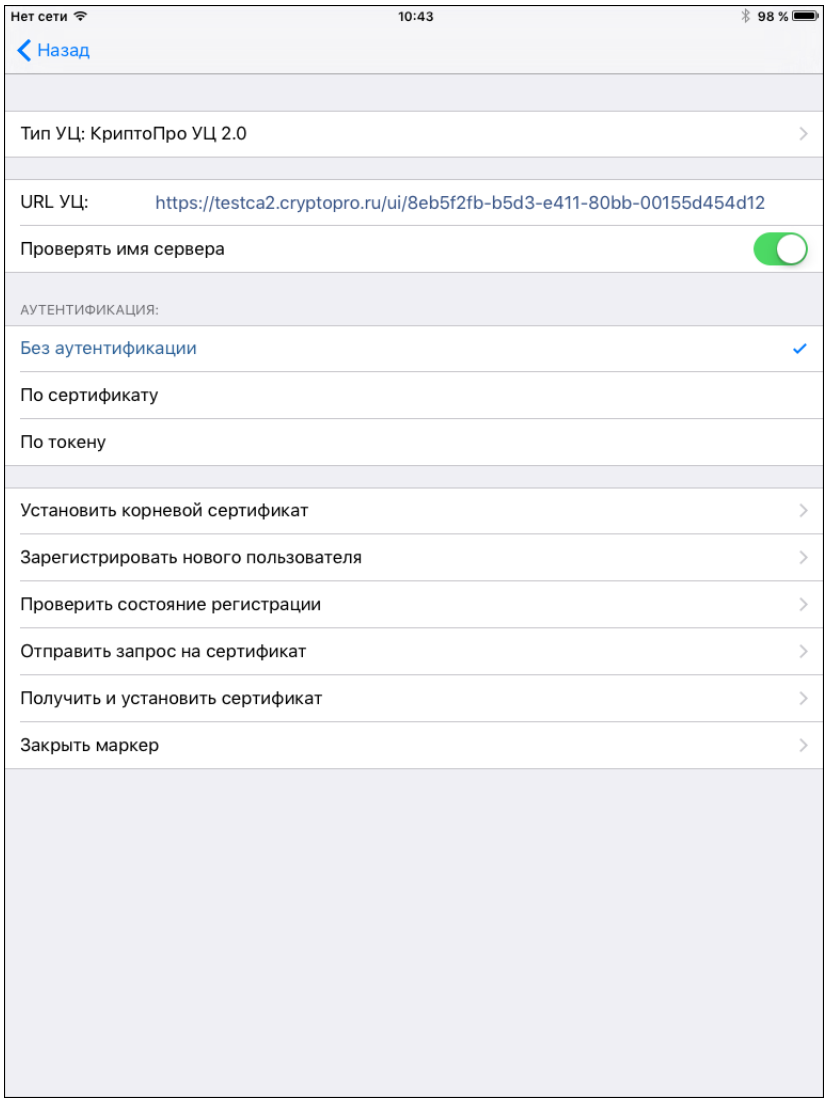

Рисунок 35. Панель взаимодействия с УЦ КриптоПро УЦ 2.0

Для установки адреса УЦ нажмите на «URL УЦ» и введите адрес. Как правило, адрес имеет формат https://<имя сервера>/ui/<id папки>. Для демонстрации работы КриптоПро CSP использовался тестовый УЦ ООО «КРИПТО-ПРО» `https://testca2.cryptopro.ru/` типа КриптоПро УЦ 2.0.

Опция «Проверять имя сервера» определяет, требуется ли при работе с УЦ проверять соответствие адреса УЦ и имени сервера из сертификата. В целях безопасности рекомендуется не выключать эту опцию.

В случае использования типа УЦ КриптоПро УЦ 2.0 доступны те же типы аутентификации пользователя УЦ, что и в случае использования КриптоПро УЦ 1.5. Подробную информацию по настройке аутентификации пользователя на УЦ см. в п. 2.8.1.1.

2.8.2.1 Установка корневого сертификата

Перед началом взаимодействия с выбранным УЦ необходимо установить его корневой сертификат в хранилище устройства. Для установки корневого сертификата УЦ нажмите на кнопку «Установить корневой сертификат» на панели взаимодействия с УЦ. Откроется окно подтверждения установки сертификата, где также содержится отпечаток сертификата (см. рис. 36 и 37).

Примечание. Тестовому УЦ https://testca2.cryptopro.ru/ соответствует 2 корневых сертификата. Окно с запросом на установку второго сертификата отображается автоматически после установки первого.

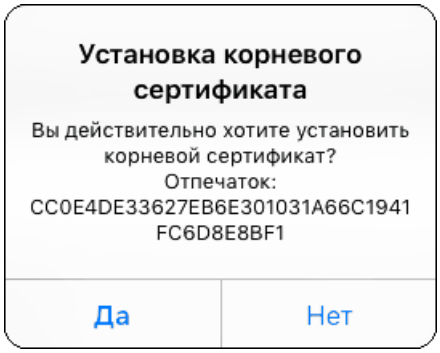

Рисунок 36. Диалоговое окно подтверждения установки первого корневого сертификата УЦ

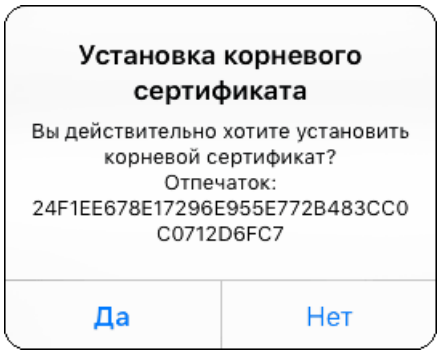

Рисунок 37. Диалоговое окно подтверждения установки второго корневого сертификата УЦ

В целях безопасности рекомендуется проверить соответствие отпечатка сертификата из сообщения и отпечатка сертификата выбранного УЦ. Отпечаток сертификата УЦ необходимо получить из доверенного источника.

В случае успешного завершения установки корневого сертификата УЦ откроется окно с соответствующим сообщением (см. рис. 21). Аналогичное окно отображается также в случае попытки установки сертификата УЦ, который уже установлен в хранилище устройства.

Если установка сертификата невозможна по причине, например, отсутствия соединения с сервером или некорректно указанного адреса УЦ, откроется окно с уведомлением об ошибке (см. рис. 22).

2.8.2.2 Регистрация пользователя на УЦ

Для аутентификации пользователя УЦ может быть использован маркер временного доступа. Маркер временного доступа выдается пользователю при его регистрации. Для регистрации нового пользователя нажмите кнопку «Зарегистрировать нового пользователя» панели взаимодействия с УЦ. Откроется окно

регистрационной формы (см. рис. 38). Внесите в форму сведения о пользователе и нажмите кнопку «Зарегистрировать».

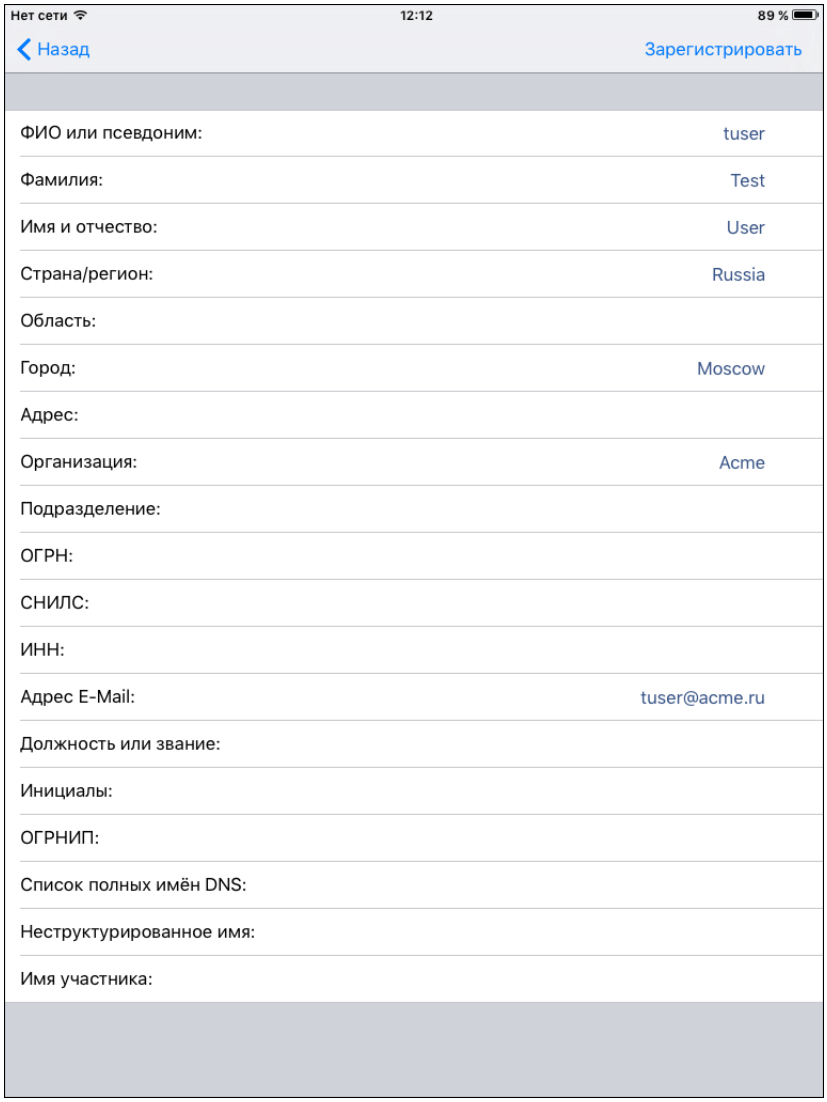

Рисунок 38. Форма регистрации пользователя УЦ

Если введенные данные не будут соответствовать политике имён УЦ (например, не будут заполнены какие-либо из обязательных полей или будет превышена максимальная длина для какого-либо поля), откроется окно с описанием ошибки и форма не будет отправлена на регистрацию.

В случае корректного заполнения регистрационной формы после нажатия на кнопку «Зарегистрировать» запрос уйдет на обработку. В открывшемся окне отобразится информация о состоянии запроса, ID маркера и пароль (см. рис. 39). Можно автоматически настроить панель взаимодействия с УЦ на работу по этому токену и паролю. Для этого в появившемся окне нужно нажать «Да». В противном случае можно будет ввести ID и пароль маркера позже вручную (см. рис. 18), для этого регистрационную информацию необходимо будет запомнить или сохранить.

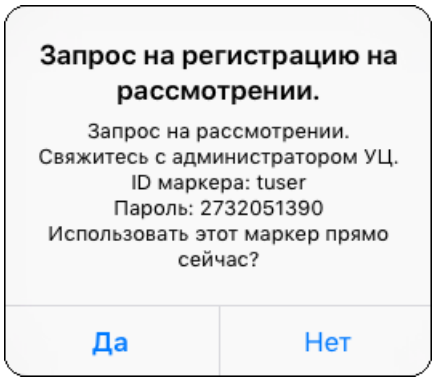

Рисунок 39. Окно с параметрами выданного пользователю токена

2.8.2.3 Проверка состояния запроса на регистрацию

Статус обработки запроса на регистрацию пользователя можно проверить, нажав кнопку «Проверить состояние регистрации» панели взаимодействия с УЦ. В открывшемся окне (см. рис. 40) отобразятся сведения о состоянии регистрации и идентификатор запроса, который может понадобиться при общении с администратором центра регистрации.

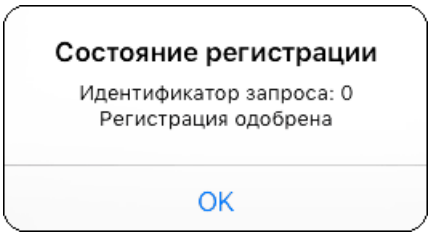

Рисунок 40. Окно проверки состояния регистрации пользователя

2.8.2.4 Создание и отправка запроса на сертификат

Для создания запроса на сертификат нажмите на кнопку «Отправить запрос на сертификат» на панели взаимодействия с УЦ. Откроется окно создания запроса на сертификат (см. рис. 41).

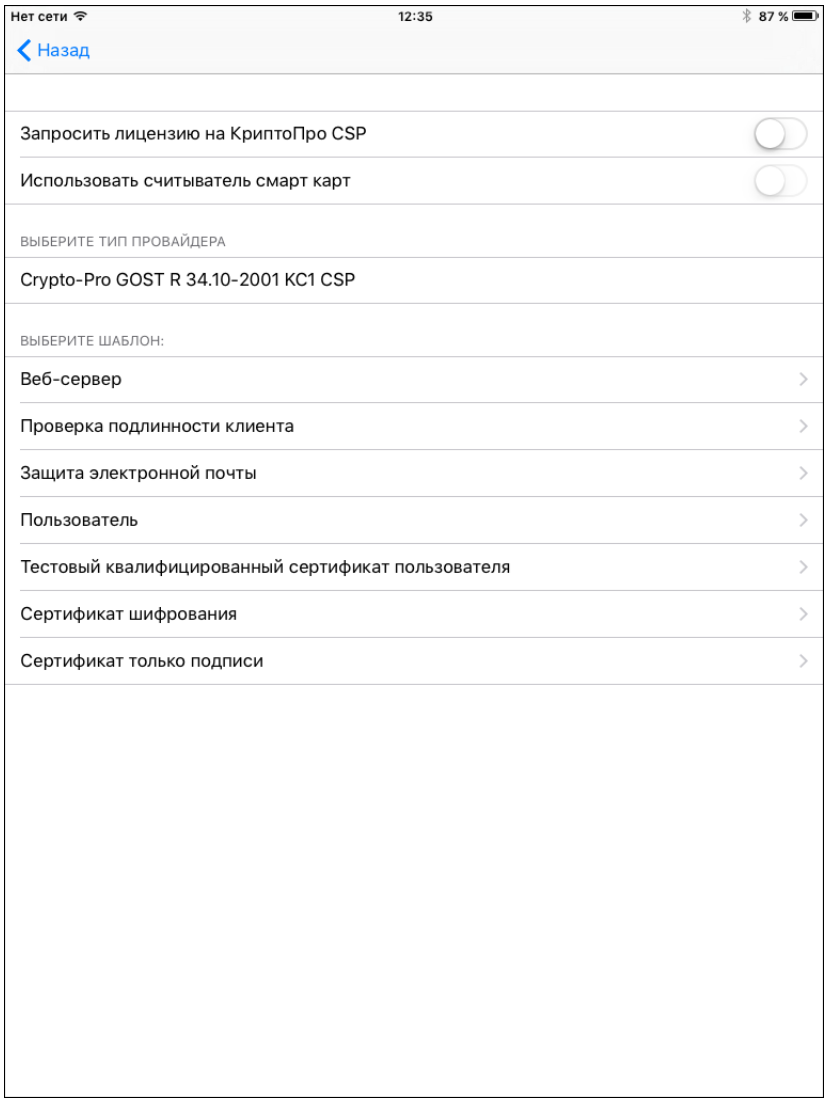

Рисунок 41. Форма запроса на сертификат

Примечание. Установку дополнительных параметров (например, запрос лицензии или выбор типа провайдера) необходимо выполнять до выбора шаблона.

При заполнении формы запроса на сертификат для выбора доступны следующие параметры:

• **запрос лицензии на КриптоПро CSP** (подробнее см. разд. 2.5) — создание запроса на сертификат, содержащий лицензию на КриптоПро CSP. Получение такого сертификата возможно, только если удостоверяющий центр, с которым вы работаете, поддерживает эту функцию. Если администратор УЦ или иное уполномоченное УЦ лицо не сообщило вам, что необходимо использовать эту функцию, не используйте её; в противном случае Ваш запрос, вероятно, будет отклонён на УЦ.

• **использование считывателя смарт-карт** — опция активна в случае наличия считывателя.

• **тип провайдера** — в зависимости от используемых алгоритмов ЭП и хэширования доступны следующие криптопровайдеры:

  – Crypto-Pro GOST R 34.10-2001 KC1 CSP;
  – Crypto-Pro GOST R 34.10-2012 KC1 CSP;
  – Crypto-Pro GOST R 34.10-2012 Strong KC1 CSP.

• **шаблон** — определяет назначение сертификата.

После нажатия на название шаблона откроется окно биологического датчика случайных чисел (ДСЧ) (см. рис. 27). Для генерации случайной последовательности нажимайте на экран устройства.

После завершения работы биологического ДСЧ и генерации ключа откроется окно установки пароля на контейнер закрытого ключа (см. рис. 28). Дважды введите пароль и нажмите кнопку «OK». Если оставить строки пустыми, пароль не будет установлен.

После этого запрос будет отправлен в УЦ.

2.8.2.5 Получение и установка сертификата

Кнопка «Получить и установить сертификат» на панели взаимодействия с УЦ позволяет просмотреть перечень созданных запросов на сертификат и их статус, установить сертификат, если он выдан, а также просмотреть и распечатать бланки сертификата и запроса на сертификат.

Для просмотра перечня созданных запросов нажмите на кнопку «Получить и установить сертификат». Откроется окно «Запросы на сертификат» (рис. 42), где отображаются идентификаторы, даты отправки и обработки, а также состояния запросов.

Рисунок 42. Перечень запросов на сертификат

Если запрос находится в состоянии **Завершен**, то при нажатии на него откроется бланк выданного сертификата (рис. 43). По кнопке «Напечатать» можно отправить бланк на печать. Для просмотра бланка запроса на сертификат нажмите кнопку «Перейти к запросу». Откроется бланк запроса на сертификат (см. рис. 44), который также можно отправить на печать.

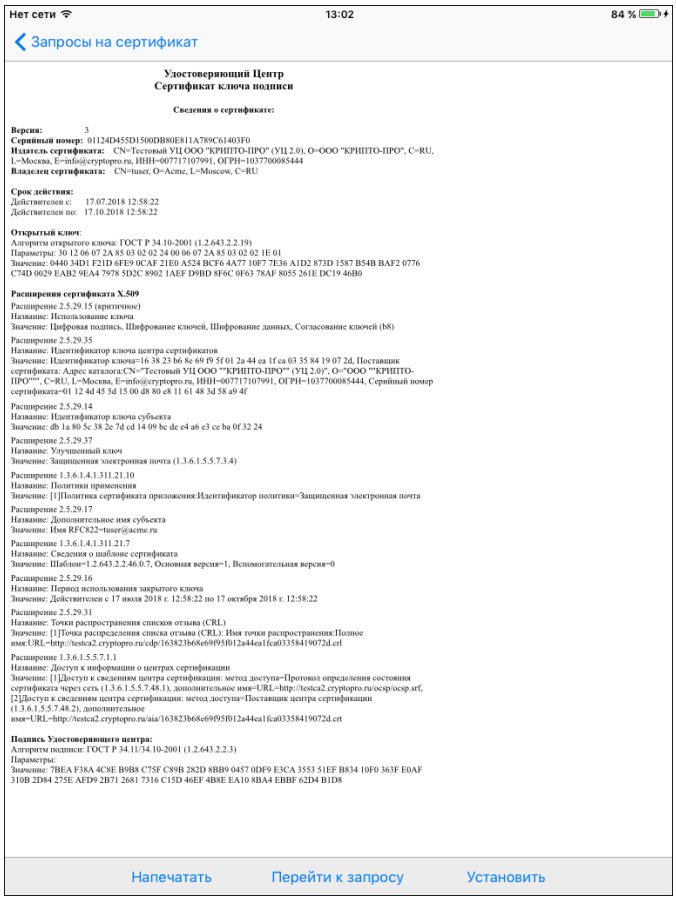

Рисунок 43. Бланк сертификата ключа проверки ЭП

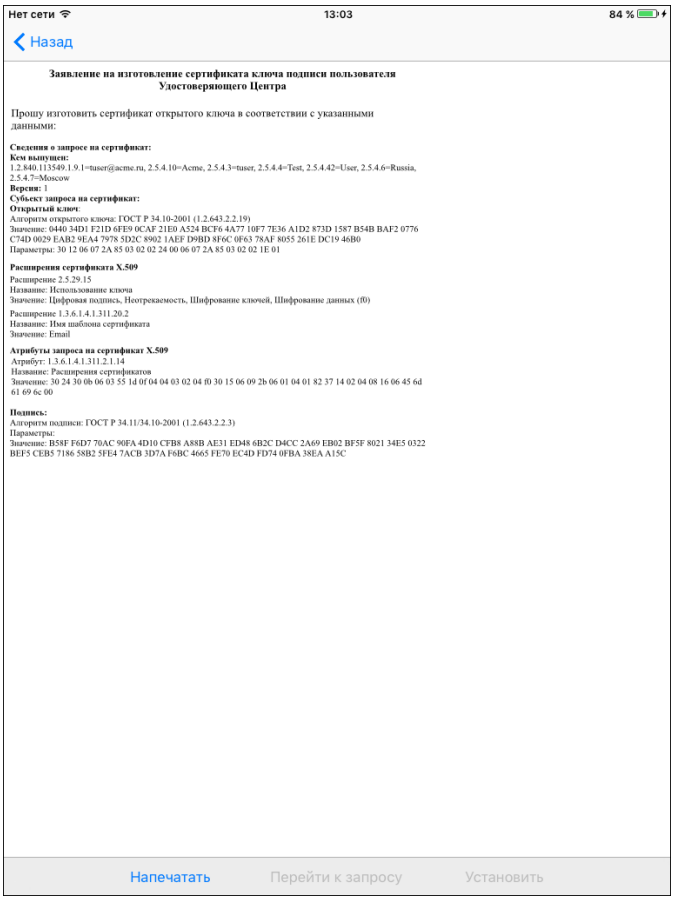

Рисунок 44. Бланк запроса на сертификат

Для установки выданного сертификата нажмите кнопку «Установить» в окне с бланком сертификата. Если на соответствующий контейнер был установлен пароль, введите его в открывшемся окне аутентификации (см. рис. 32). После этого сертификат будет установлен в хранилище устройства.

2.8.2.6 Закрытие маркера временного доступа

В случае осуществления аутентификации на УЦ с помощью маркера временного доступа по окончанию работы с УЦ его можно закрыть. Для этого нажмите на кнопку «Закрыть маркер» на панели взаимодействия с УЦ. Откроется окно с запросом подтверждения на закрытие маркера (см. рис. 33).

В случае успешного закрытия маркера откроется окно с соответствующим сообщением (см. рис. 34).

2.8.3 Взаимодействие с Microsoft УЦ

Для настройки подключения к Microsoft УЦ откройте панель взаимодействия с УЦ и установите тип УЦ «Изолированный Microsoft УЦ». Панель взаимодействия с УЦ выглядит следующим образом (см. рис. 45).

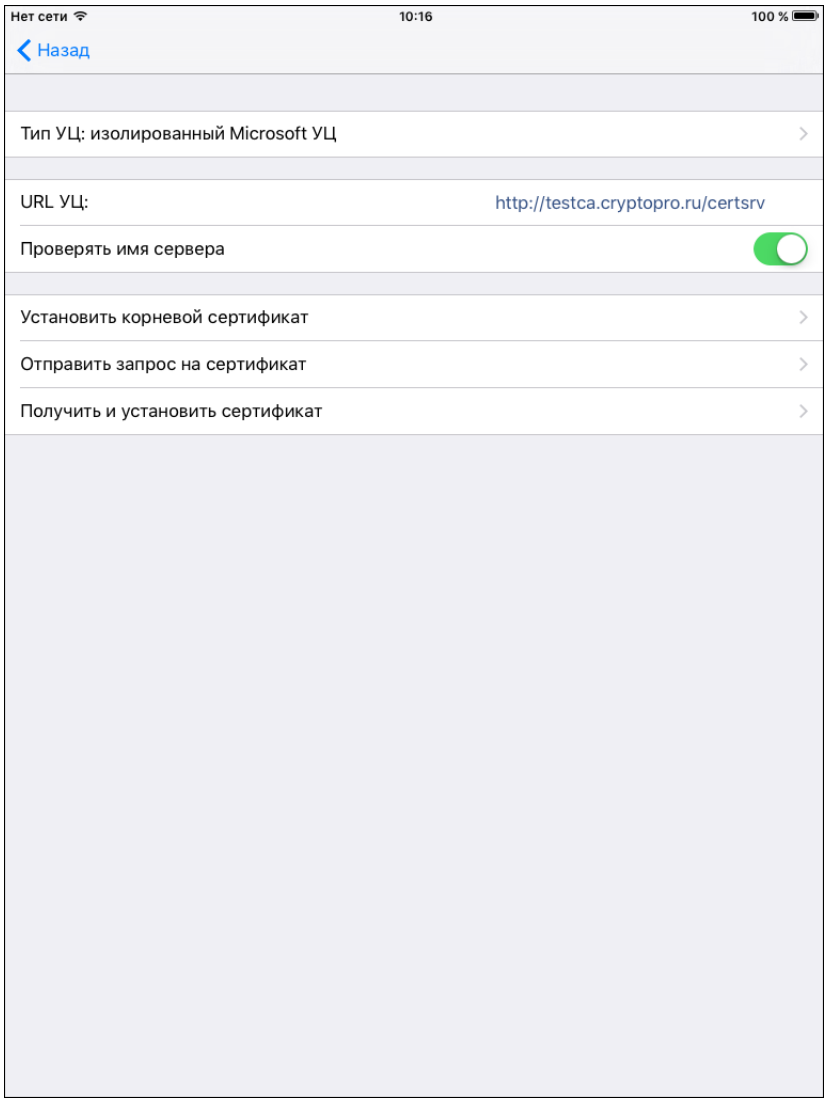

Рисунок 45. Панель взаимодействия с Microsoft УЦ

После выбора типа УЦ введите в поле «URL УЦ» адрес центра. Как правило, он имеет формат http://<имя сервера>/certsrv. Для демонстрации работы КриптоПро CSP использовался тестовый УЦ ООО «КРИПТО-ПРО» https://testca.cryptopro.ru/certsrv/ типа Microsoft УЦ.

Опция «Проверять имя сервера» определяет, требуется ли при работе с УЦ проверять соответствие адреса УЦ и имени сервера из сертификата. В целях безопасности рекомендуется не выключать эту опцию.

2.8.3.1 Установка корневого сертификата

Перед началом взаимодействия с выбранным УЦ необходимо установить его корневой сертификат в хранилище устройства. Для установки корневого сертификата УЦ нажмите на кнопку «Установить корневой сертификат» на панели взаимодействия с УЦ. Откроется окно подтверждения установки сертификата, где также содержится отпечаток сертификата (см. рис. 46).

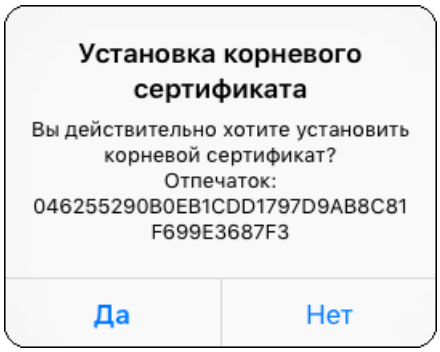

Рисунок 46. Диалоговое окно подтверждения установки корневого сертификата УЦ

В целях безопасности рекомендуется проверить соответствие отпечатка сертификата из сообщения и отпечатка сертификата выбранного УЦ. Отпечаток сертификата УЦ необходимо получить из доверенного источника.

В случае успешного завершения установки корневого сертификата УЦ откроется окно с соответствующим сообщением (см. рис. 21). Аналогичное окно отображается также в случае попытки установки сертификата УЦ, который уже установлен в хранилище устройства.

Если установка сертификата невозможна по причине, например, отсутствия соединения с сервером или некорректно указанного адреса УЦ, откроется окно с уведомлением об ошибке (см. рис. 22).

2.8.3.2 Отправка запроса на сертификат

Для создания запроса на сертификат нажмите на кнопку «Отправить запрос на сертификат» на панели взаимодействия с УЦ. Откроется окно создания запроса на сертификат (см. рис. 47).

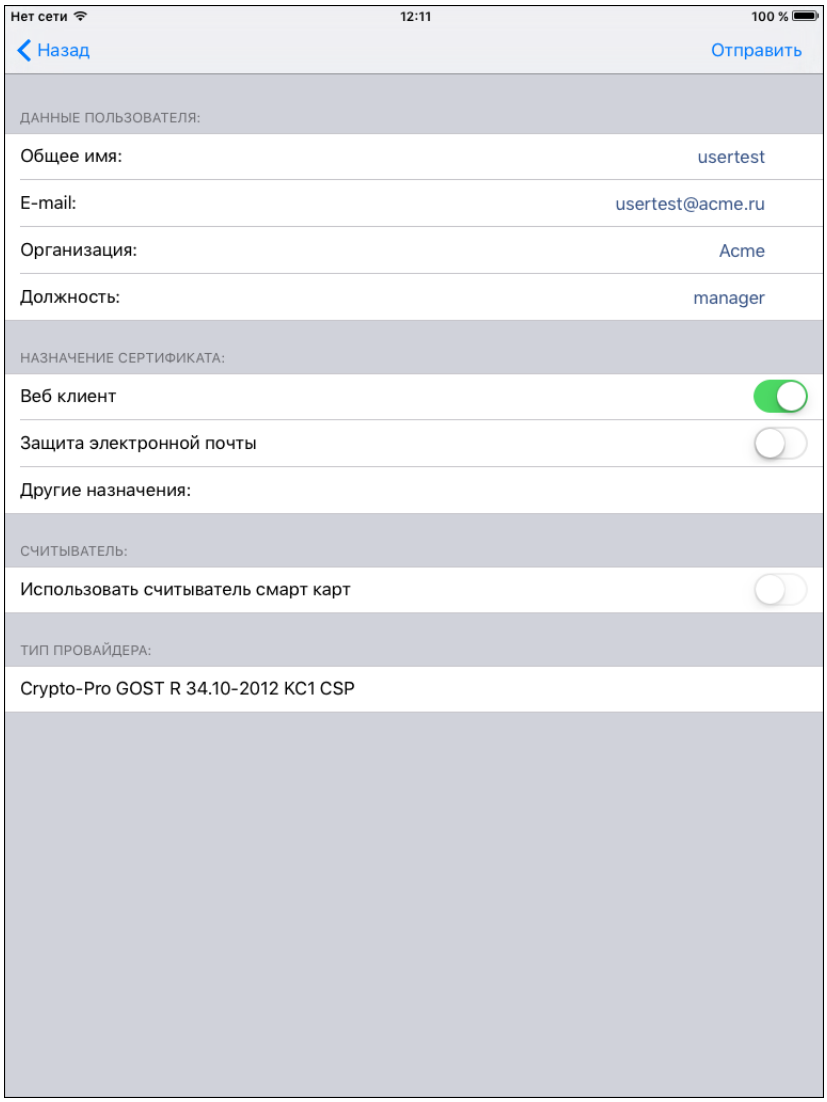

Рисунок 47. Форма запроса на сертификат

При заполнении формы запроса на сертификат для выбора доступны следующие параметры:

- **назначение сертификата**;
- **использование считывателя смарт-карт** — опция активна в случае наличия считывателя;
- **тип провайдера** — в зависимости от используемых алгоритмов ЭП и хэширования доступны следующие криптопровайдеры:
  - Crypto-Pro GOST R 34.10-2001 KC1 CSP;
  - Crypto-Pro GOST R 34.10-2012 KC1 CSP;
  - Crypto-Pro GOST R 34.10-2012 Strong KC1 CSP.

После нажатия на кнопку «Отправить» откроется окно биологического датчика случайных чисел (ДСЧ) (см. рис. 27). Для генерации случайной последовательности нажимайте на экран устройства.

После завершения работы биологического ДСЧ и генерации ключа откроется окно установки пароля на контейнер закрытого ключа (см. рис. 28). Дважды введите пароль и нажмите кнопку «OK». Если оставить строки пустыми, пароль не будет установлен.

После этого запрос будет отправлен в УЦ.

2.8.3.3 Получение и установка сертификата

В зависимости от настроек УЦ запрос на сертификат будет принят автоматически или поставлен в очередь для обработки администратором УЦ.

Если запрос принят автоматически, сертификат будет скачан и установлен в хранилище на устройстве.

Если запрос поставлен в очередь, будет выведено окно с идентификатором запроса. Этот номер необходимо запомнить или записать и использовать в дальнейшем.

Состояние запроса можно узнать, нажав на кнопку «Получить и установить сертификат». В открывшемся окне (см. рис. 48) необходимо ввести идентификатор запроса, полученный ранее. Если запрос одобрен и сертификат выпущен, он будет скачан и установлен в хранилище. Если запрос всё ещё находится на рассмотрении, будет выведено соответствующее сообщение.

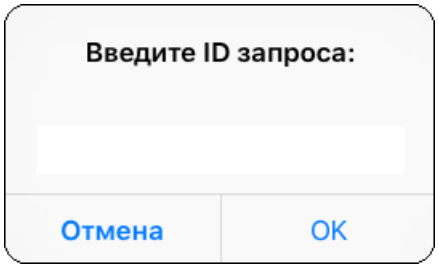

Рисунок 48. Окно ввода идентификатора запроса на сертификат