

127 018, Москва, Сущевский Вал, д.18  
Телефон: (495) 995 4820  
Факс: (495) 995 4820  
<http://www.CryptoPro.ru>  
E-mail: [info@CryptoPro.ru](mailto:info@CryptoPro.ru)



Средство  
Криптографической  
Защиты  
Информации

КриптоPro CSP  
Версия 4.0 КС1  
Инструкция по  
использованию СКЗИ под  
управлением ОС iOS

ЖТЯИ.00087-01 92 02  
Листов 18

**© ООО «КРИПТО-ПРО», 2000-2017. Все права защищены.**

Авторские права на средства криптографической защиты информации типа КриптоPro CSP и эксплуатационную документацию к ним зарегистрированы в Российском агентстве по патентам и товарным знакам (Роспатент).

Настоящий Документ входит в комплект поставки программного обеспечения СКЗИ КриптоPro CSP версии 4.0; на него распространяются все условия лицензионного соглашения. Без специального письменного разрешения ООО "КРИПТО-ПРО" документ или его часть в электронном или печатном виде не могут быть скопированы и переданы третьим лицам с коммерческой целью.

## Содержание

1.Инсталляция СКЗИ КриптоПро CSP .....	4
2.Интерфейс СКЗИ КриптоПро CSP.....	5
2.1. Доступ к контрольной панели СКЗИ .....	5
2.2. Проверка целостности.....	5
2.3. Ввод серийного номера лицензии криптопровайдера «КриптоПро CSP» .....	5
2.4. Удаление ключей и сертификатов.....	6
2.5. Взаимодействие с УЦ .....	6
2.5.1. Взаимодействие с КриптоПро УЦ 1.5 .....	7
<i>Настройка подключения к УЦ .....</i>	7
<i>Установка корневого сертификата .....</i>	8
<i>Регистрация пользователя на УЦ .....</i>	9
<i>Проверка состояния запроса на регистрацию.....</i>	10
<i>Создание и отправка запроса на сертификат .....</i>	11
<i>Получение и установка сертификата.....</i>	13
<i>Закрытие маркера временного доступа .....</i>	14
2.5.2. Взаимодействие с Microsoft УЦ.....	15
<i>Настройка подключения к Microsoft УЦ.....</i>	15
<i>Установка корневого сертификата .....</i>	16
<i>Отправка запроса на сертификат.....</i>	17

## 1. Инсталляция СКЗИ КриптоПро CSP

Инсталляция, деинсталляция и обновление СКЗИ «КриптоПро CSP» 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 КриптоPro CSP

### 2.1. Доступ к контрольной панели СКЗИ

Данный раздел является инструкцией по использованию контрольной панели (панели настройки) средства криптографической защиты информации (СКЗИ) «КриптоPro CSP».

Панель настройки «КриптоPro CSP» доступна из прикладной программы, разработанной на базе «КриптоPro CSP». Метод вызова контрольной панели определяет разработчик прикладной программы.

Контрольная панель СКЗИ «КриптоPro CSP» имеет четыре функции:

- Взаимодействие с УЦ;
- Удаление ключей и сертификатов;
- Управление лицензией;
- Проверка целостности.



Рисунок 1. Контрольная панель СКЗИ «КриптоPro CSP»

### 2.2. Проверка целостности

Функция осуществляет проверку целостности «КриптоPro CSP» и приложения.

### 2.3. Ввод серийного номера лицензии криптопровайдера «КриптоPro CSP»

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

Существует три способа лицензирования «КриптоPro CSP» для 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 «КриптоPro 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».

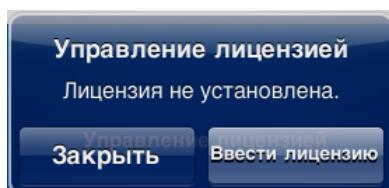


Рисунок 2. Диалоговое окно управления лицензиями

После чего программа выдаст сообщение, информирующее о сроке действия лицензии либо ее отсутствии. В этом диалоговом окне можно ввести новый серийный номер, нажав «Ввести лицензию». После ввода нового серийного номера, ваша текущая лицензия заменится на новую.

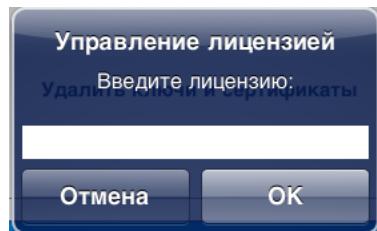


Рисунок 3. Окно ввода лицензии

## 2.4. Удаление ключей и сертификатов

Функция «Удалить ключи и сертификаты» удаляет с устройства все закрытые ключи, ключи электронной подписи и сертификаты как личные, так и корневые. Будьте внимательны при использовании этой функции, поскольку удаленные ключи невозможно восстановить.

## 2.5. Взаимодействие с УЦ

Поддерживается работа с удостоверяющими центрами двух типов: КриптоPro УЦ 1.5 и Microsoft CA Standalone.

## 2.5.1. Взаимодействие с КриптоPro УЦ 1.5

### Настройка подключения к УЦ

После нажатия на кнопку «Взаимодействие с УЦ» откроется панель взаимодействия с удостоверяющим центром. Для работы с КриптоPro УЦ нажмите на «Тип УЦ» и в появившемся окне выберите «КриптоPro УЦ 1.5».

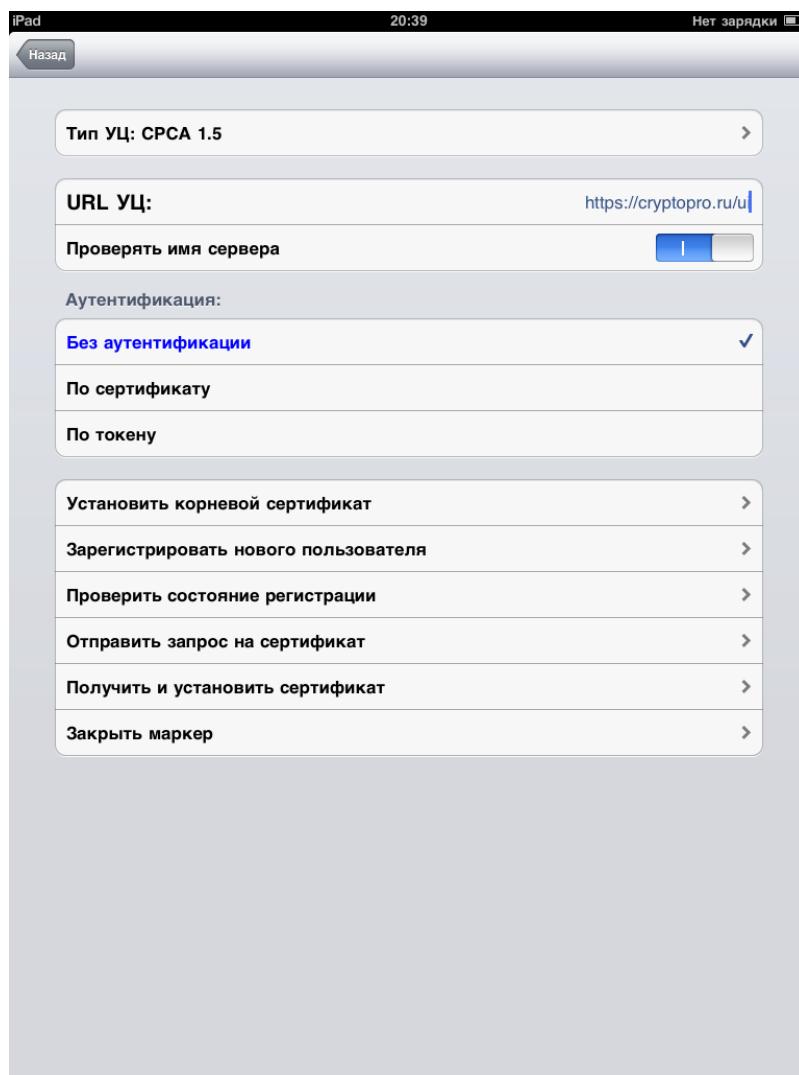


Рисунок 4. Окно взаимодействия с КриптоPro УЦ

Чтобы задать адрес удостоверяющего центра нажмите на «URL УЦ» и введите адрес. Как правило, адрес имеет формат <https://<имя сервера>/ui>.

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.

Далее вы можете выбрать тип аутентификации:

- Без аутентификации;
- По сертификату;
- По токену:

При нажатии на «По токену» появится окно ввода ID маркера и пароля.

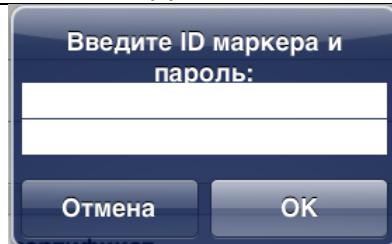


Рисунок 5. Окно ввода данных маркера

При нажатии на «По сертификату» появится окно выбора сертификата из списка установленных.

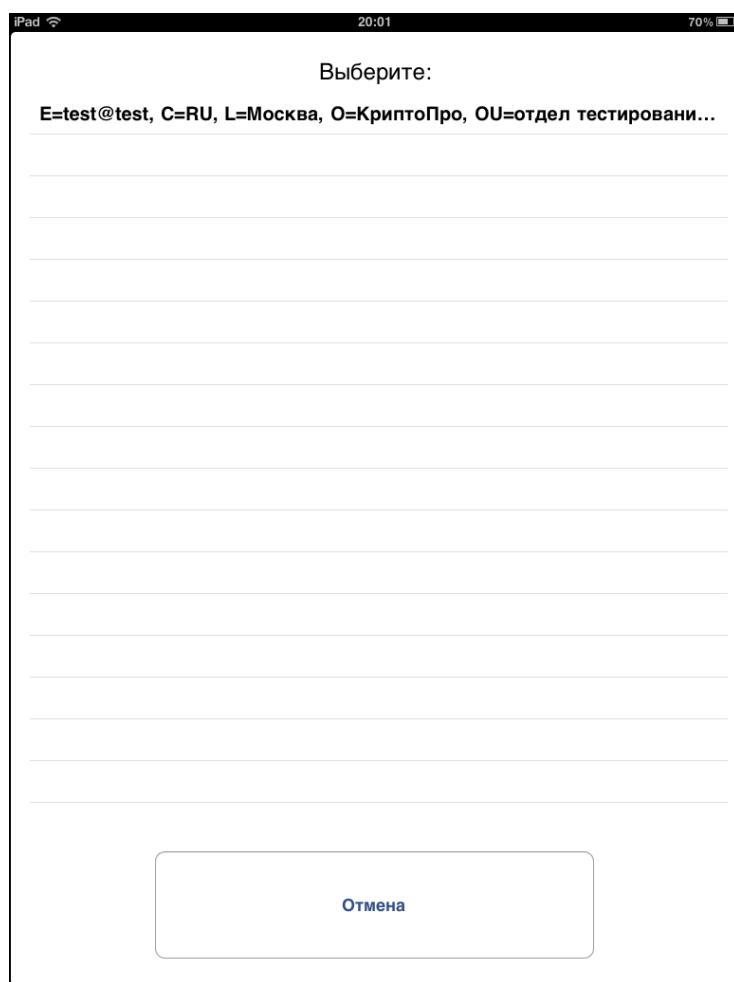


Рисунок 6. Список установленных сертификатов

### **Установка корневого сертификата**

Для работы с УЦ, вам потребуется установить корневой сертификат выбранного вами УЦ. Это можно сделать, нажав на кнопку «Установить корневой сертификат». После нажатия на эту кнопку появится запрос на установку корневого сертификата:

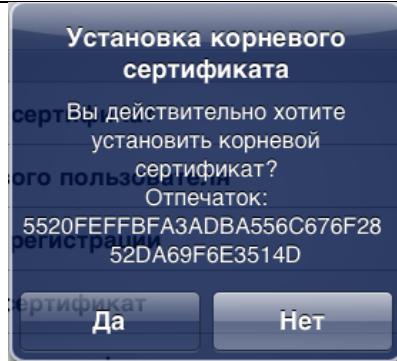


Рисунок 7. Запрос на установку корневого сертификата

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

Если вместо этого уведомления появится сообщение об ошибке, проверьте работу сети.

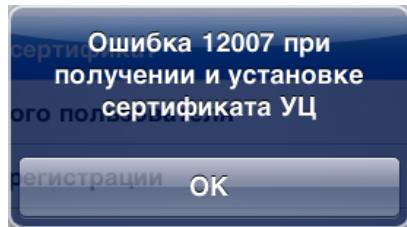


Рисунок. 8. Ошибка соединения с сервером УЦ

### **Регистрация пользователя на УЦ**

Если выбранный удостоверяющий центр позволяет вам зарегистрировать нового пользователя, вы можете сделать это при помощи кнопки «Зарегистрировать нового пользователя». После этого появится окно ввода данных. Для регистрации необходимо ввести данные о пользователе и нажать кнопку «Зарегистрировать». Если введенные данные не будут соответствовать политике имён удостоверяющего центра (например, не будут заполнены какие-то из обязательных полей или будет превышена максимальная длина для какого-то поля), вы получите предупреждение.

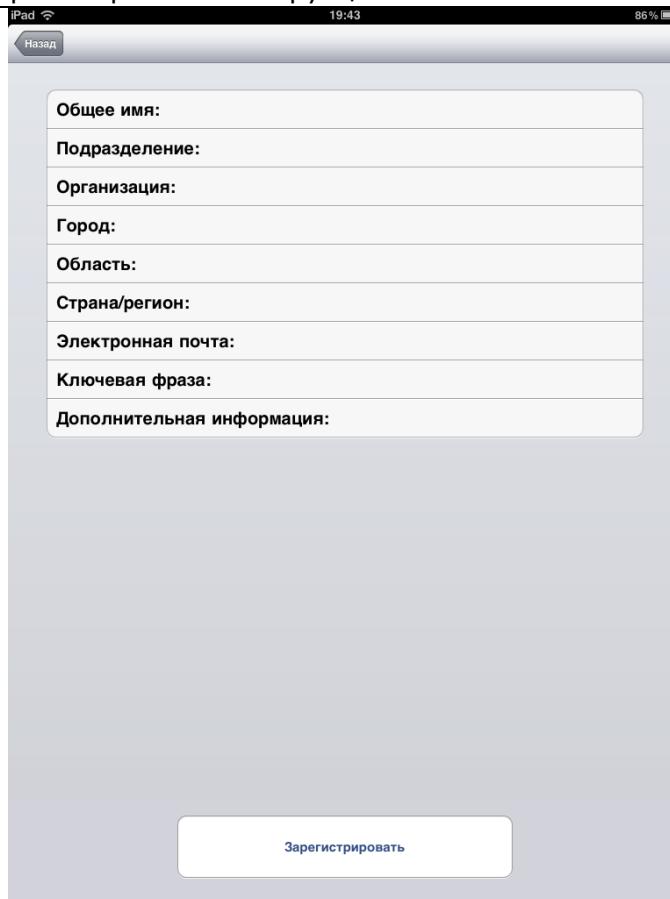


Рисунок 9. Окно ввода данных о пользователе

После нажатия на кнопку «Зарегистрировать» запрос уйдет на обработку. Будет отображена информация о статусе регистрации, содержащая Ваши ID маркера и пароль. 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 позже вручную, для этого регистрационную информацию необходимо будет запомнить или сохранить.

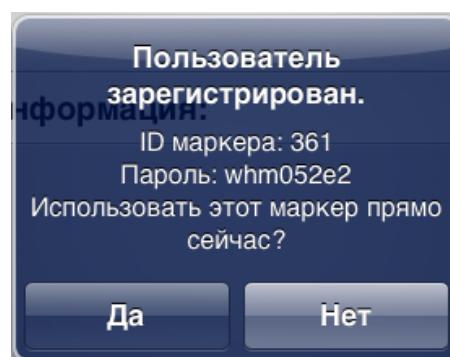


Рисунок 10. Сообщение об успешной регистрации и полученные ID и Пароль

#### **Проверка состояния запроса на регистрацию**

Статус обработки запроса на регистрацию можно проверить, нажав кнопку «Проверить состояние запроса на регистрацию». Если запрос еще обрабатывается, появится сообщение «Запрос в обработке», если регистрация завершена – «Регистрация одобрена». Также окно содержит идентификатор запроса на регистрацию, он может понадобиться при общении с администратором центра регистрации.

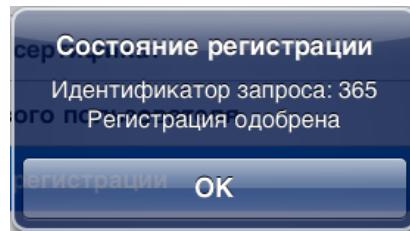


Рисунок 11. Сообщение об успешной регистрации пользователя

### **Создание и отправка запроса на сертификат**

Для создания запроса на сертификат, нужно нажать кнопку «Отправить запрос на сертификат». Откроется панель выбора шаблона сертификата.

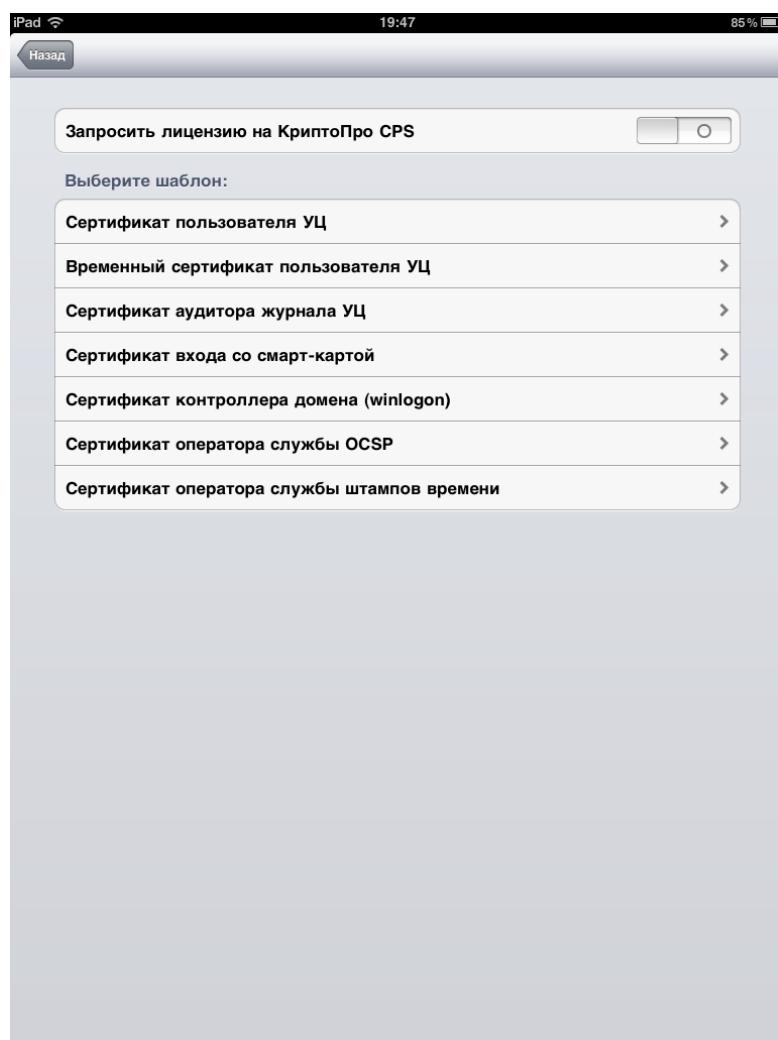


Рисунок 12. Выбор шаблона сертификата

При выборе шаблона, можно также выбрать создание запроса на сертификат, содержащий лицензию на КриптоPro 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.

После нажатия на название шаблона запустится биологический датчик случайных чисел.

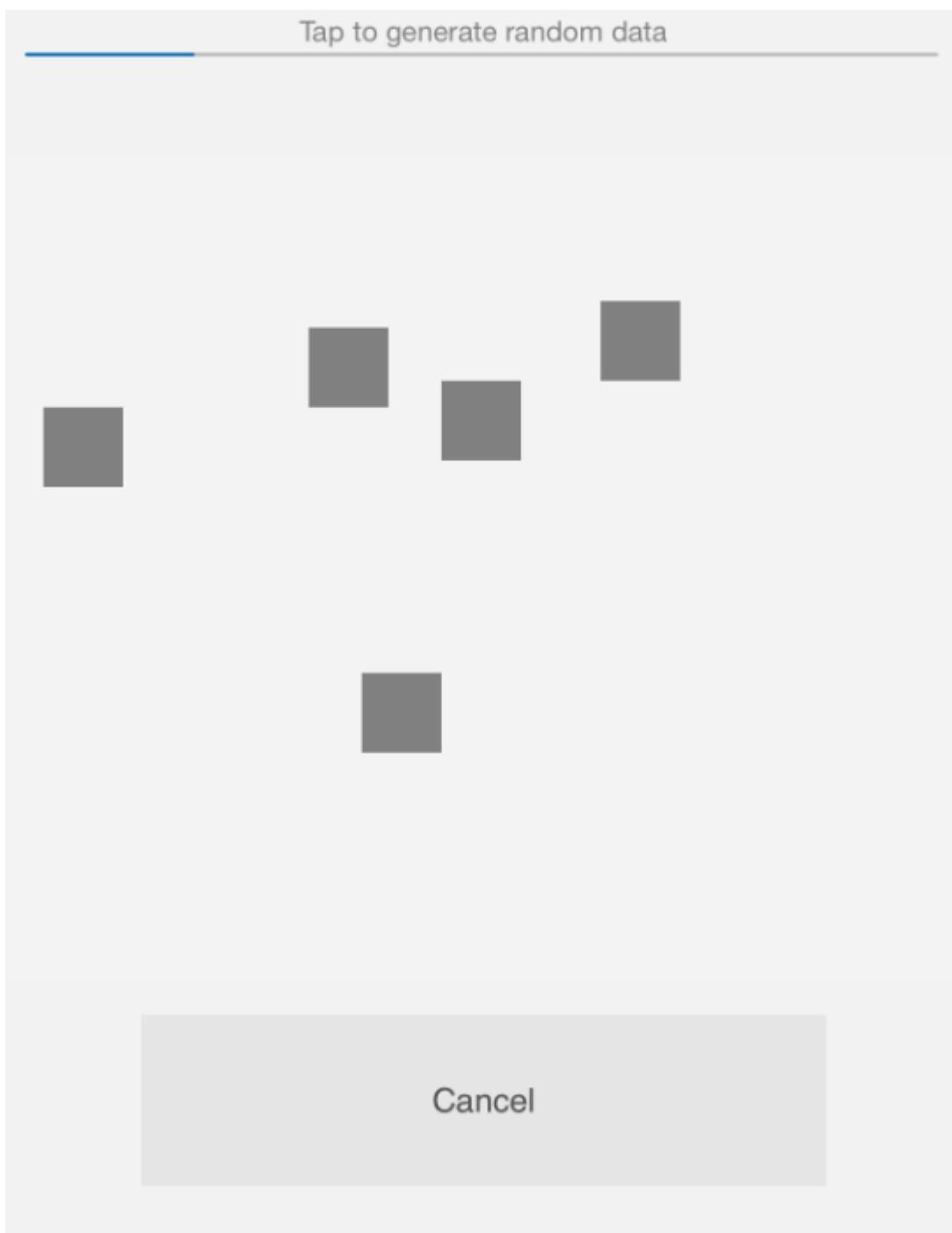


Рисунок 13. Биологический датчик

Когда ключ сгенерируется, появится сообщение с просьбой задать пароль. В двух строках нужно ввести желаемый пароль. Первая строка ввод пароля, вторая – подтверждение. Если оставить строки пустыми пароль не будет установлен.



Рисунок 14. Сообщение ввода пароля

### Получение и установка сертификата

Кнопка «Получить и установить сертификат» позволяет просмотреть состояние запроса на сертификат, установить сертификат, если он выдан, а также посмотреть и распечатать бланки сертификата и запроса на сертификат.

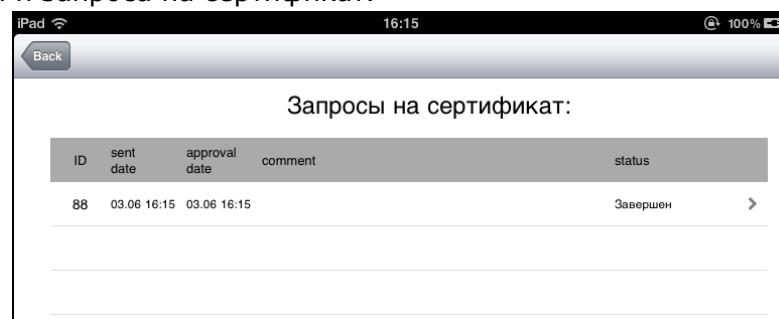


Рисунок 15. Состояние запроса на сертификат

Наименование организации-Удостоверяющего Центра Бланк сертификата открытого ключа	
<b>Сведения о сертификате:</b>	
Кому выдан:	Test Center CRYPTO-PRO
Когда выдан:	03.06.2014 г. 12:05:16 UTC по 4 октября 2014 г. 7:09:41 UTC
Срок действия:	3 (всеги)
Издаёт сертификата:	Test Center CRYPTO-PRO, О = CRYPTO-PRO, С = RU, E = info@cryptopro.ru
Срок действия:	3 июня 2011 г. 12:05:16 UTC
Действителен:	по 4 октября 2014 г. 7:09:41 UTC
Владелец сертификата:	CH = gffg
Открытый ключ:	Альгоритм: ГОСТ Р 34.10-2001 Идентификатор: 1.2.643.2.2.14 Номер сертификата: 03 02 24 00 06 07 2e 85 03 02 02 1e 01 Значение: 0940 A2B8 323B FEB1 4834 0D6E F950 AB2C FA1A 8691 678A 1B0D 3B8B 2A49 ECFS A1E9 D5F3 F91C 33EC 41BD 03B0 0CED EFF5 3E60 2C57 3649 FD24 12A9 4B6D 9412 D738
<b>Расширение сертификата X.509</b>	
1. Расширение 2.5.2.37	Назначение: Идентификация открытого ключа
Значение: Электронная почта (1.3.6.1.5.5.7.3.4) Пользователь Центра Регистрации, HTTP, TLS клиент (1.2.643.2.2.34.6) Проверка подлинности клиента (1.3.6.1.5.5.7.3.2)	
2. Расширение 2.5.2.38	Назначение: Использование ключа
Значение: Шифрование паролей, Неотрекаемость, Шифрование ключей, Шифрование данных (R)	
3. Расширение 2.5.2.39	Назначение: Идентификатор открытого ключа
Значение: 03 02 24 00 06 07 2e 85 03 02 02 1e 01	
4. Расширение 2.5.2.39	Назначение: Идентификация открытого ключа
Значение: Электронная почта (1.3.6.1.5.5.7.3.4) Пользователь Центра Регистрации, HTTP, TLS клиент (1.2.643.2.2.34.6) Проверка подлинности клиента (1.3.6.1.5.5.7.3.2)	
5. Расширение 2.5.2.39	Назначение: Идентификация открытого ключа-Ed25519 (8.5.0.29.5.91.17.94.1e.95.9a.05.30.38.37.7a.10.2a)
6. Расширение 1.3.6.1.5.5.7.41	Назначение: Установление списка отзыва (CRL)
Значение: [1]Путь распространения списка отзыва (CRL) Имя точки распространения: Полное имя: URL=http://www.cryptopro.ru/CertEnroll/Test%20Center%20CRYPTO-PRO(2).crl	
Помощь: Документация и поддержка в центре сертификации	
Значение: [1]Доступ к скрипции центра сертификации: Метод доступа-Приятельство состояния сертификата через сеть (1.3.6.1.5.5.7.48.1) Дополнительное имя: URL=http://www.cryptopro.ru/CertEnroll/pk-site_Test%20Center%20CRYPTO-PRO(2).crt	
Помощь: Установка сертификата	
Альгоритм подписи:	Название: ГОСТ Р 34.10-2001 Идентификатор: 1.2.643.2.2.3
Значение: 7197 1P96 20FF FDF5 50E5 8989 8840 661D DA15 A811 2AD6 2F87 ESFL DC98 88E9 4481 A17C 31E8 5912 B862 1476 E795 IC88 E1D2 E64D 0AAA 7E88 CAE7 SAC0 C9C4 90AA	
Подпись владельца сертификата: _____ / _____ _____=_____ 20 г. М. П.	
Свидетельство криптографической защиты информации: "КриптоPro CSP".	
Подписаны бланк сертификата открытого ключа следует переслать по адресу: 11111, Москва, ул. XXXXXXXX, д. XX, XXXXXXXXXXXXXXXXXX Административному информационному центру.	
<input type="button" value="Напечатать"/> <input type="button" value="Перейти к запросу"/> <input type="button" value="Установить"/>	

Рисунок 16. Бланк сертификата открытого ключа/ключа проверки электронной подписи

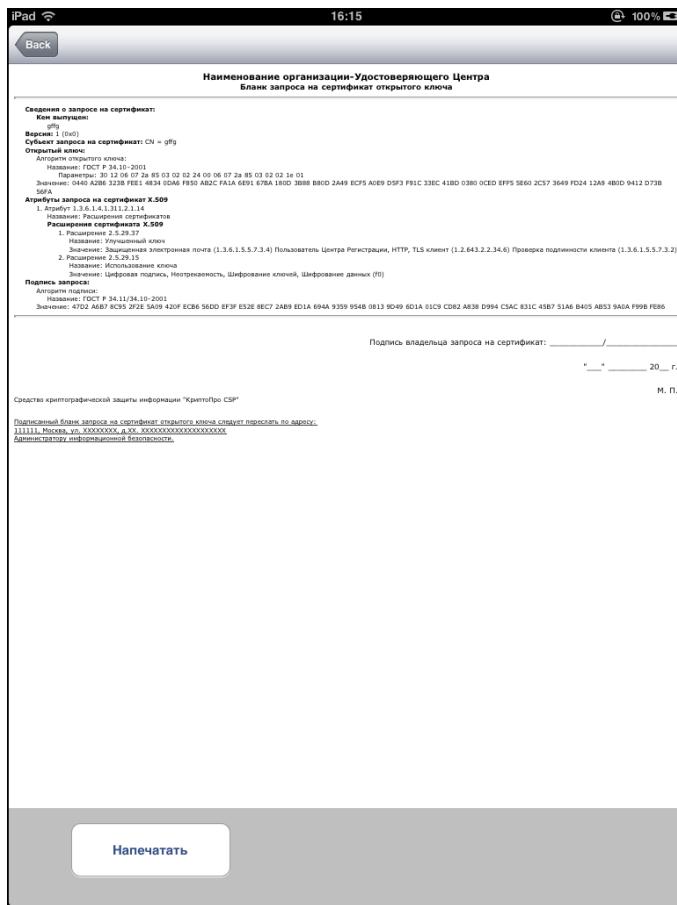


Рисунок 17 Бланк запроса на сертификат открытого ключа/ключа проверки электронной подписи

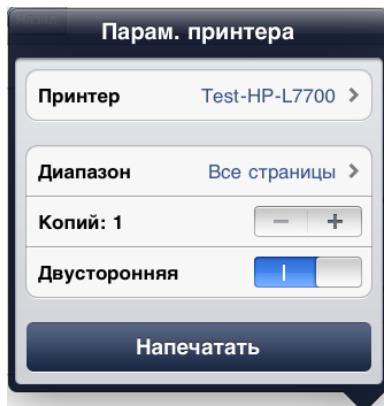


Рисунок 18. Печать запроса

### **Закрытие маркера временного доступа**

После получения сертификата и закрытого ключа/ключа электронной подписи, маркер временного доступа можно закрыть, нажав кнопку в самом низу экрана – «Закрыть маркер временного доступа».

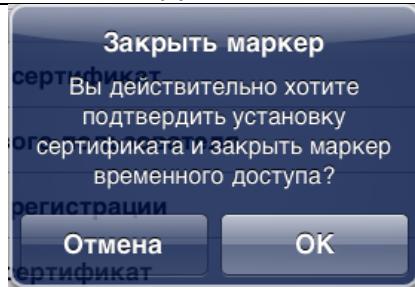


Рисунок 19. Закрытие маркера

## 2.5.2. Взаимодействие с Microsoft УЦ

### Настройка подключения к Microsoft УЦ

Для работы с Microsoft УЦ нажмите на «Тип УЦ» и в появившемся окне выберите «Изолированный Microsoft УЦ».

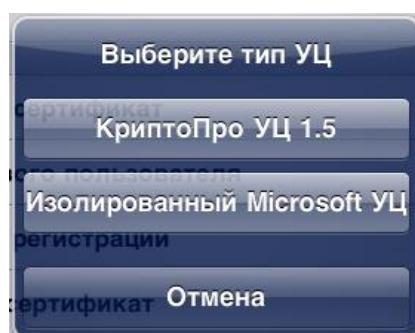


Рисунок20. Выбор типа УЦ

После выбора типа УЦ введите в поле «URL УЦ» адрес центра. Как правило, он имеет формат `http://<имя сервера>/certsrv`.

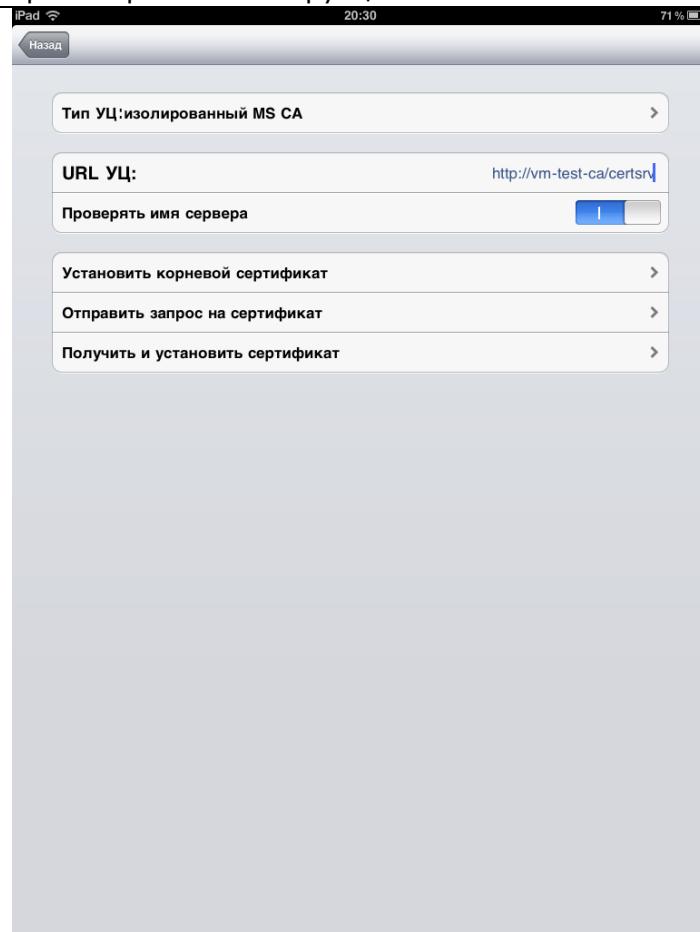


Рисунок 21. Выбор типа УЦ

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.

### Установка корневого сертификата

Для работы с УЦ Вам потребуется установить корневой сертификат выбранного УЦ. Это можно сделать, нажав «Установить корневой сертификат». После нажатия на эту кнопку появится запрос на установку корневого сертификата:

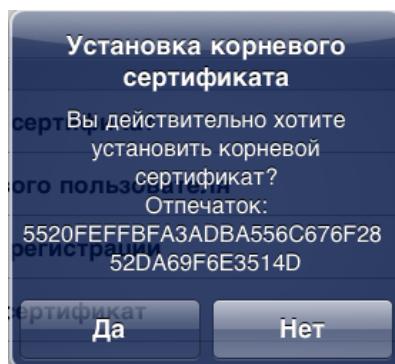


Рисунок 22. Запрос на установку корневого сертификата

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

Если вместо этого уведомления появится сообщение об ошибке, проверьте работу сети.

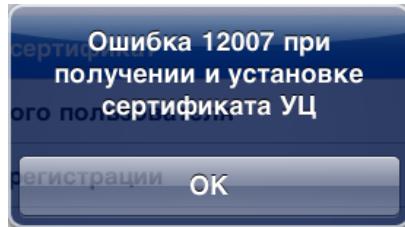


Рисунок 23. Ошибка соединения с сервером УЦ

#### Отправка запроса на сертификат

После нажатия на «Отправить запрос на сертификат» запустится создание и отправка запроса на сертификат. Для этого заполните необходимые поля и выберите назначение сертификата.

Общее имя:	test
E-mail:	test@test.ru
Организация:	ООО КриптоПро
Должность:	

Назначение сертификата:

Веб клиент

Задача электронной почты

Другие назначения:

**Отправить**

Рисунок 24. Отправка запроса на сертификат

После нажатия на кнопку «Отправить» запустится биологический датчик случайных чисел и будет создан закрытый ключ/ключ электронной подписи. После создания ключа появится сообщение с просьбой задать пароль. В двух строках нужно ввести желаемый пароль. Первая строка ввод пароля, вторая – подтверждение. Если оставить строки пустыми, пароль не будет установлен.



Рисунок 24. Сообщение ввода пароля

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

Если запрос принят автоматически, сертификат будет выкачен и установлен.

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

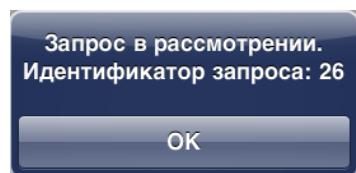


Рисунок 25. Состояние запроса на сертификат

Состояние запроса можно узнать, нажав на «Получить и установить сертификат» и введя соответствующий RequestID. Если сертификат всё ещё находится на рассмотрении, будет выведено следующее сообщение:

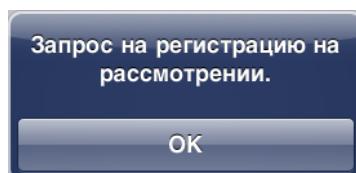


Рисунок 27. Статус запроса

Если сертификат был выпущен, он будет установлен.