

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



Средство Криптографической Защиты Информации	КриптоПро CSP Версия 3.9 Инструкция по использованию СКЗИ под управлением ОС iOS
---	--

ЖТЯИ.00083-01 90 03-01
Листов 18

© ООО "КРИПТО-ПРО", 2000-2016. Все права защищены.

Авторские права на средство криптографической защиты информации КриптоПро CSP и эксплуатационную документацию зарегистрированы в Российском агентстве по патентам и товарным знакам (Роспатент).

Документ входит в комплект поставки программного обеспечения СКЗИ КриптоПро CSP v. 3.9, 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»	6
2.4.	Удаление ключей и сертификатов	6
2.5.	Взаимодействие с УЦ.....	6
2.5.1.	Взаимодействие с КриптоПро УЦ 1.5	6
2.5.1.1.	Настройка подключения к УЦ.....	6
2.5.1.2.	Установка корневого сертификата.....	8
2.5.1.3.	Регистрация пользователя на УЦ.....	9
2.5.1.4.	Проверка состояния запроса на регистрацию.....	10
2.5.1.5.	Создание и отправка запроса на сертификат	10
2.5.1.6.	Получение и установка сертификата	12
2.5.1.7.	Закрытие маркера временного доступа.....	14
2.5.2.	Взаимодействие с Microsoft УЦ.....	15
2.5.2.1.	Настройка подключения к Microsoft УЦ.....	15
2.5.2.2.	Установка корневого сертификата.....	16
2.5.2.3.	Отправка запроса на сертификат	16

1. Установка СКЗИ КриптоПро CSP

Установка, 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 КриптоПро CSP

2.1. Доступ к контрольной панели СКЗИ

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

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

Контрольная панель СКЗИ КриптоПро CSP имеет четыре функции:

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



Рис. 1. Контрольная панель СКЗИ КриптоПро CSP

2.2. Проверка целостности

Функция осуществляет проверку целостности КриптоПро CSP и приложения.

2.3. Ввод серийного номера лицензии криптопровайдера «КриптоПро CSP»

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 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».

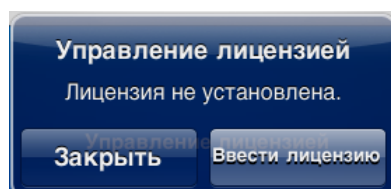


Рис. 2. Диалоговое окно управления лицензиями.

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.

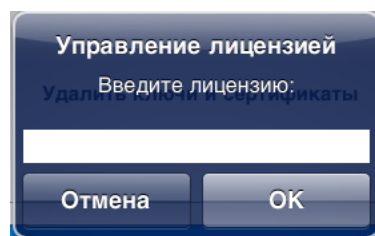


Рис. 3. Окно ввода лицензии.

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: КриптоПро УЦ 1.5 и Microsoft CA Standalone.

2.5.1. Взаимодействие с КриптоПро УЦ 1.5

2.5.1.1. Настройка подключения к УЦ

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

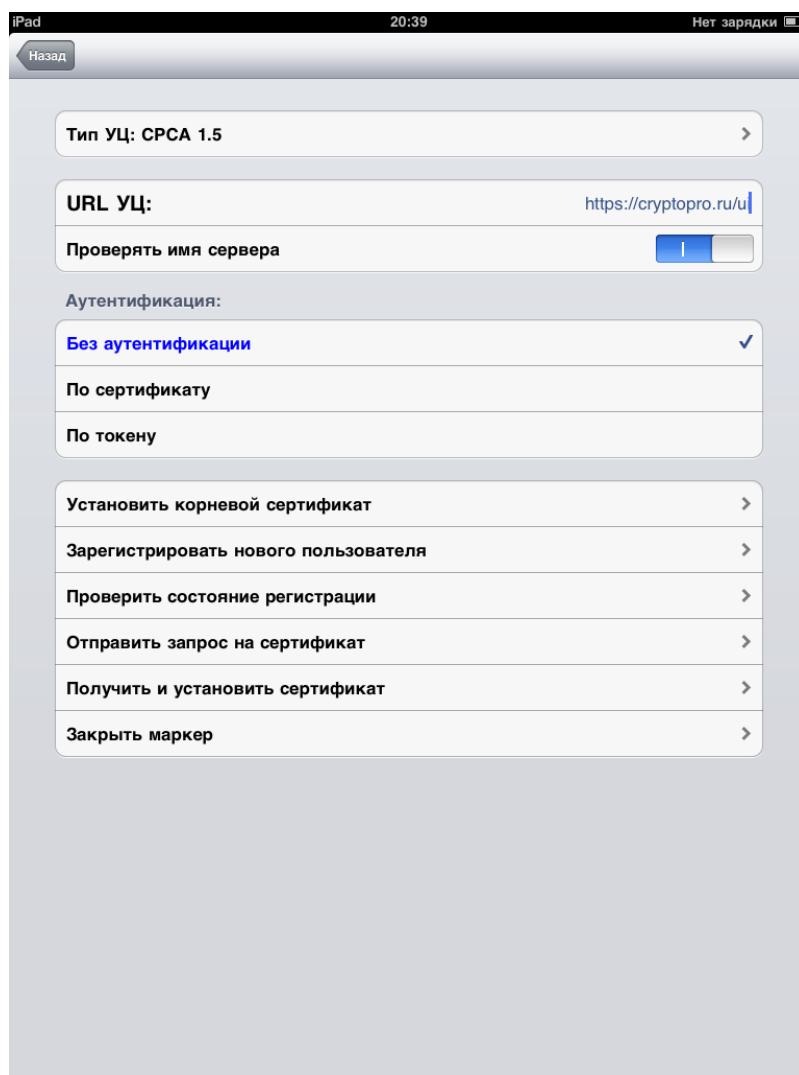


Рис. 4. Окно взаимодействия с КриптоПро УЦ.

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.

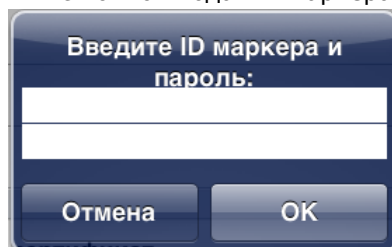


Рис. 5. Окно ввода данных маркера.

При нажатии на “По сертификату” появится окно выбора сертификата из списка установленных.

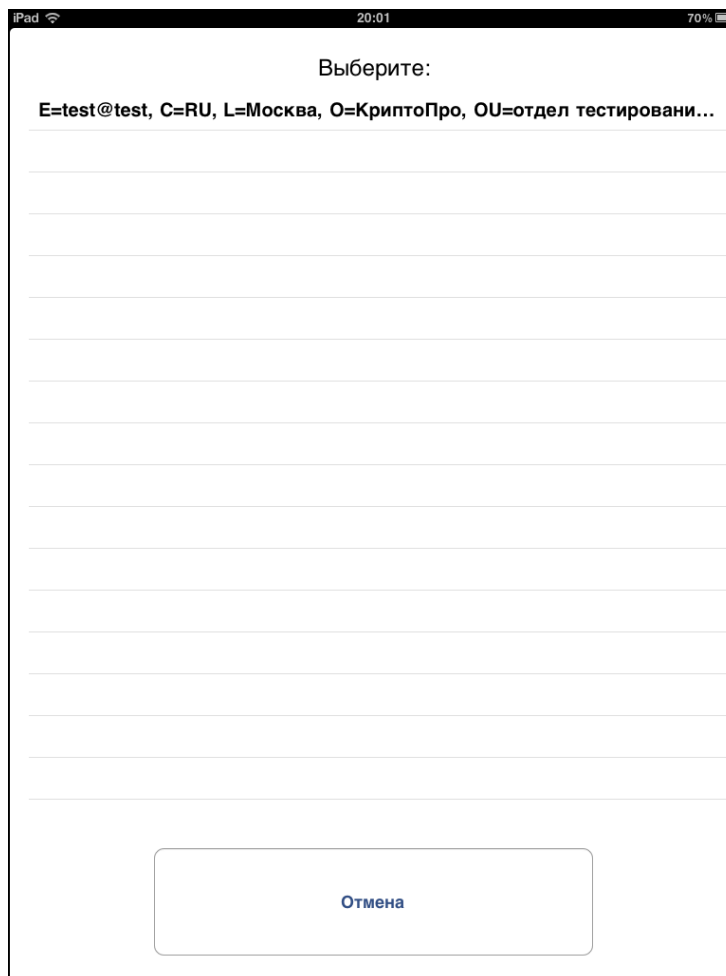


Рис. 6. Список установленных сертификатов.

2.5.1.2. 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:

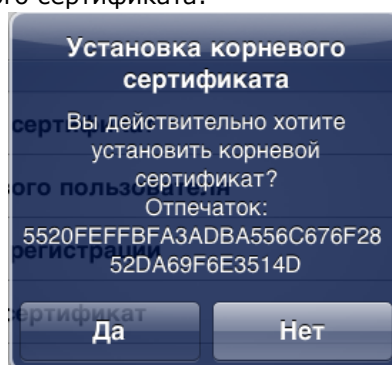


Рис. 7. Запрос на установку корневого сертификата.

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.

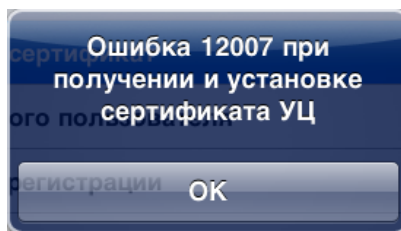


Рис. 8. Ошибка соединения с сервером УЦ.

2.5.1.3. 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.

Рис. 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.

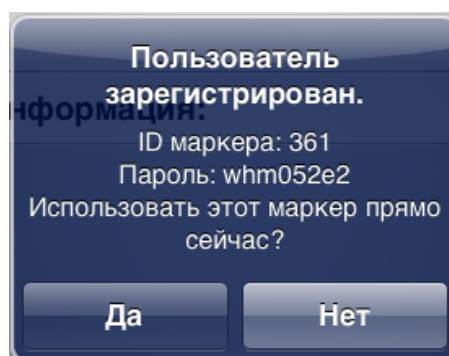


Рис. 10. Сообщение об успешной регистрации и полученные ID и Пароль.

2.5.1.4. 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.

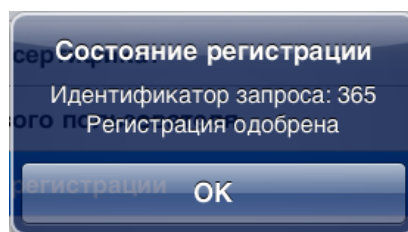


Рис. 11. Сообщение об успешной регистрации пользователя.

2.5.1.5. Создание и отправка запроса на сертификат

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

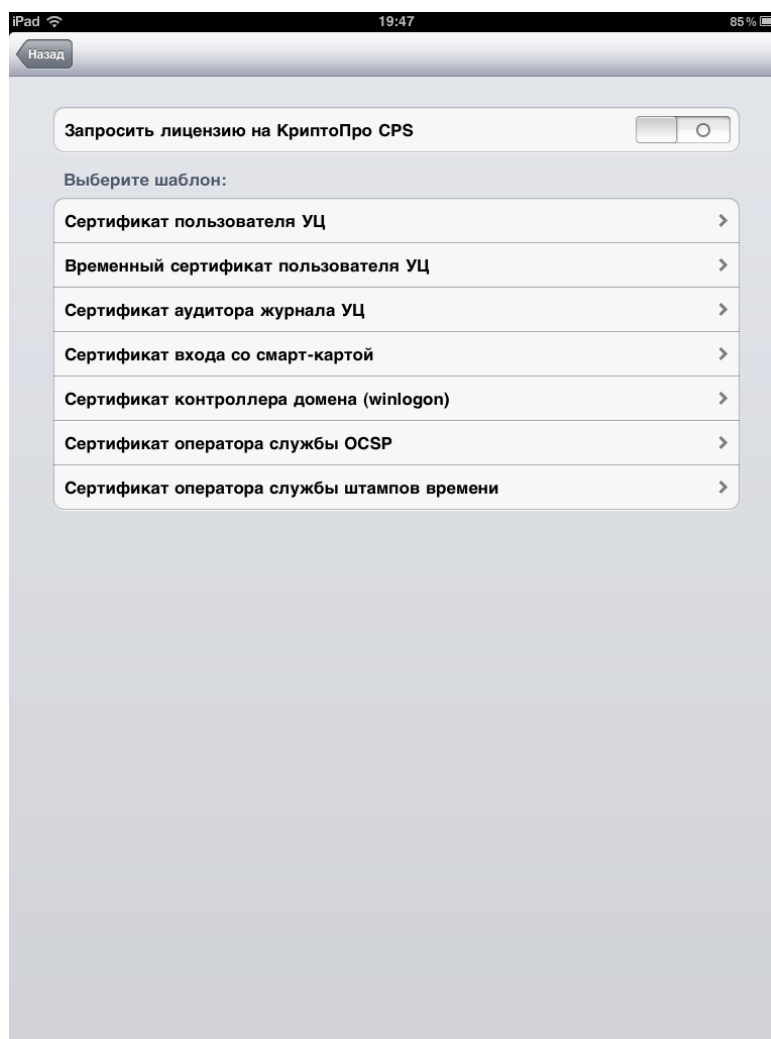


Рис. 12. Выбор шаблона сертификата.

При выборе шаблона, можно также выбрать 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.

После нажатия на название шаблона запустится биологический датчик случайных чисел.

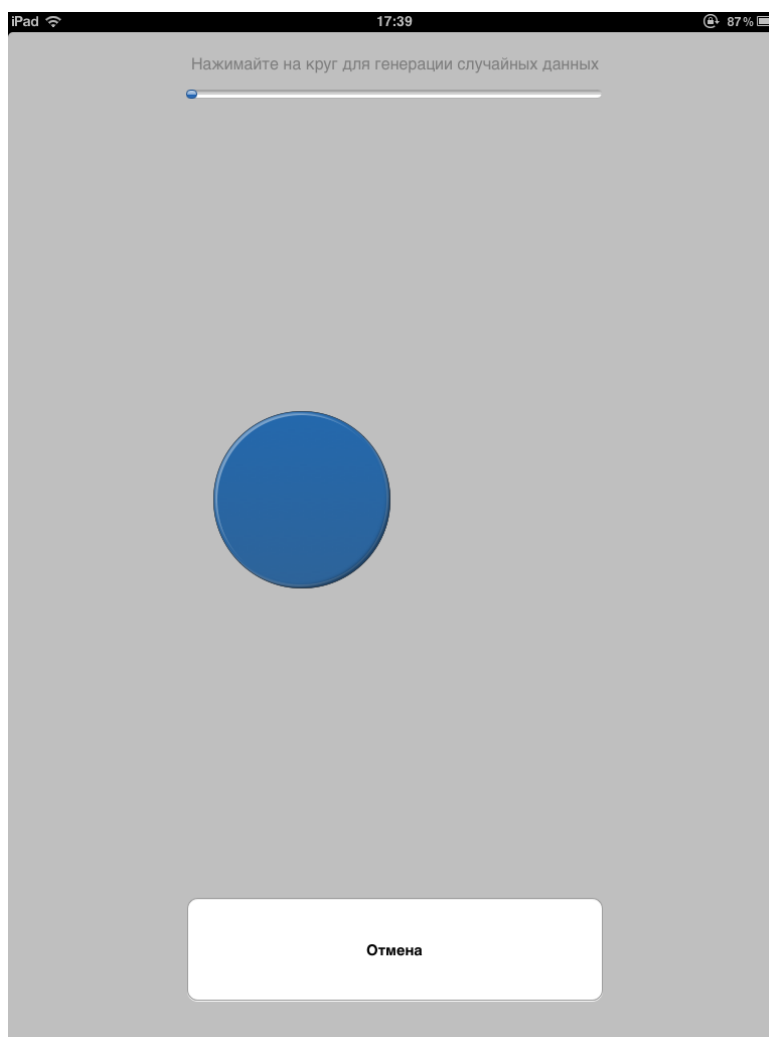


Рис. 13. Биологический датчик.

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.



Рис. 14. Сообщение ввода пароля.

2.5.1.6. 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.

Наименование организации-Удостоверяющего Центра
Бланк запроса на сертификат открытого ключа

Сведения о запросе на сертификат:
Кем выдывается:
Версия: 1 (0x01)
Субъект запроса на сертификат: CN = gff
Открытый ключ:
Алгоритм открытого ключа:
Название: ГОСТ Р 34.10-2001
Параметры: 20 12 06 07 2a 85 03 02 24 08 06 07 2a 85 03 02 02 1a 01
Значение: 0440 A2B6 2228 FE61 4834 0DA6 F850 AB2C FALA 6491 67BA 180D 3B88 B80D 2A49 8C9F A0E9 D9F3 F91C 33EC 418D 0380 0CED E9F5 5660 2C37 3649 FC24 12A9 480D 9412 D73B 56FA
Атрибуты запроса на сертификат X.509
1. Атрибут 1.3.6.1.4.1.311.2.1.14
Название: Расширение сертификата
Расширение сертификата X.509
1. Расширение 2.5.29.37
Название: Уполномоченный ключ
Значение: Защищенная 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 2.5.29.15
Название: Использование ключа
Значение: Цифровая подпись, Непроверенность, Шифрование ключей, Шифрование данных (0)

Подпись запроса:
Алгоритм подписи:
Название: ГОСТ Р 34.11/34.10-2001
Значение: 4702 AB87 8C95 373E 3A09 420F 8CB6 56D0 873F 653E 8EC7 1AB9 8D1A 694A 9259 9548 0813 9C49 6D1A 03C9 CD82 AB39 D994 CSAC 831C 4387 51A6 8405 AB52 840A F998 F856

Подпись владельца запроса на сертификат: _____

Средство криптографической защиты информации "КриптоПро CSP"

Печатный бланк запроса на сертификат открытого ключа следует присылать по адресу:
111111, Москва, ил. XXXXXXXX, в ОУ XXXXXXXXXXXXXXXXXXXX
Административный информационный ресурс

Напечатать

Рис. 17. Бланк запроса на сертификат открытого ключа/ключа проверки электронной подписи.

Парам. принтера

Принтер Test-HP-L7700 >

Диапазон Все страницы >

Копий: 1 - +

Двусторонняя ☒

Напечатать

Рис. 18. Печать запроса.

2.5.1.7. Заккрытие маркера временного доступа

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

Заккрыть маркер

Вы действительно хотите
подтвердить установку
сертификата и закрыть маркер
временного доступа?

Отмена OK

Рис.19. Заккрытие маркера

2.5.2. Взаимодействие с Microsoft УЦ

2.5.2.1. Настройка подключения к Microsoft УЦ

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

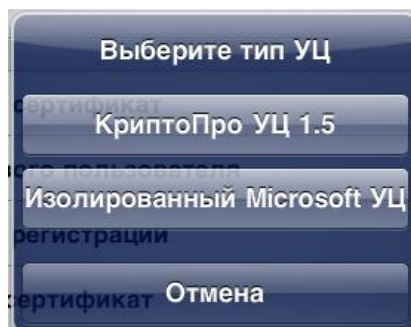


Рис.20. Выбор типа УЦ

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

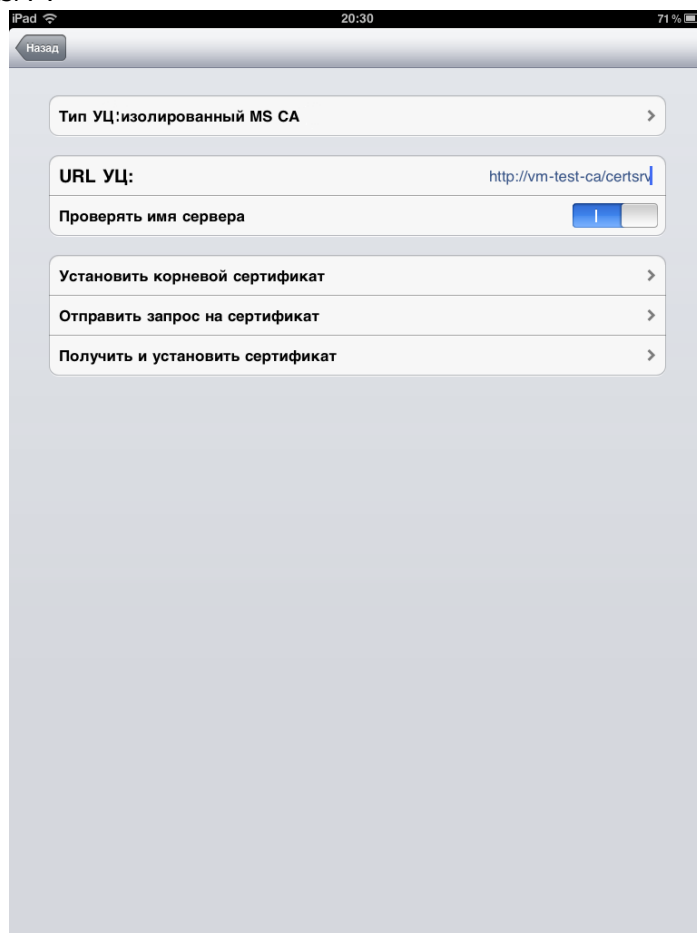


Рис.21. Выбор типа УЦ

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.

2.5.2.2. 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:

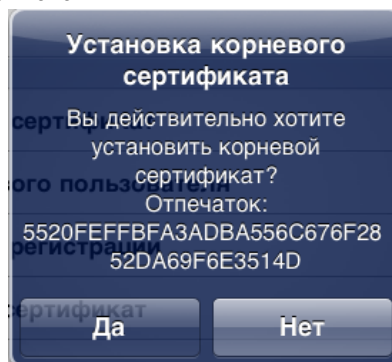


Рис. 22. Запрос на установку корневого сертификата.

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.

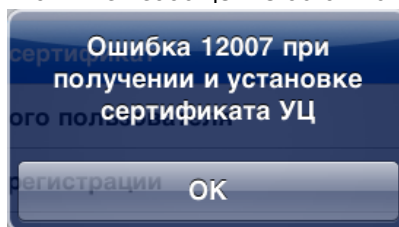


Рис. 23. Ошибка соединения с сервером УЦ.

2.5.2.3. 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.

Назад

Данные пользователя:

Общее имя: тест

E-mail: test@test.ru

Организация: ООО КриптоПро

Должность:

Назначение сертификата:

Веб клиент ☐

Защита электронной почты ☐

Другие назначения:

Отправить

Рис. 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.

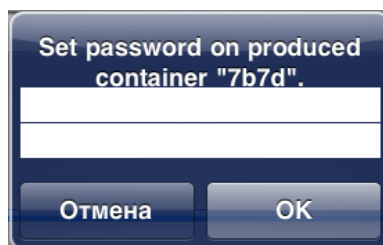


Рис. 24. Сообщение ввода пароля.

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

Если запрос принят автоматически, сертификат будет выкачан и установлен.

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

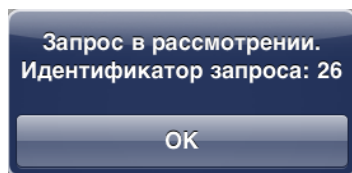


Рис. 26. Состояние запроса на сертификат

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:

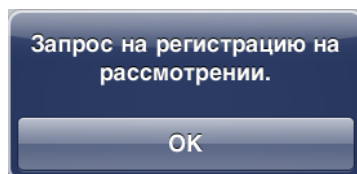


Рис. 27. Статус запроса

Если сертификат был выпущен, он будет установлен.