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 Android

ЖТЯИ.00101-01 92 03
Листов 17

2019 г

Содержание

Список определений и сокращений

CRL	Список отозванных сертификатов (Certificate Revocation List)
АРМ	Автоматизированное рабочее место
АС	Автоматизированная система
ГМД	Гибкий магнитный диск
ДСЧ	Датчик случайных чисел
HDD	Жесткий магнитный диск (Hard Disk Drive)
НСД	Несанкционированный доступ
ОС	Операционная система
ПАК	Программно-аппаратный комплекс
ПО	Программное обеспечение
Регистрация	Присвоение определенных атрибутов (адреса, номера ключа, прав использования и т.п.) абоненту
Регламент	Совокупность инструкций и другой регламентирующей документации, обеспечивающей функционирование автоматизированной системы во всех режимах
СВТ	Средства вычислительной техники
Сертификат	Электронный документ, подтверждающий принадлежность открытого ключа или ключа проверки электронной подписи и определенных атрибутов конкретному абоненту
Сертификация	Процесс изготовления сертификата открытого ключа или ключа проверки электронной подписи абонента в центре сертификации
СКЗИ	Средство криптографической защиты информации
СОС	Список отозванных сертификатов (Certificate Revocation List)
СС	Справочник сертификатов открытых ключей и ключей проверки электронной подписи. Сетевой справочник
СФ	Среда функционирования
ЦС	Центр Сертификации (Удостоверяющий Центр)
ЦР	Центр Регистрации
ЭД	Электронный документ
ЭП	Электронная подпись

1 Инсталляция СКЗИ КриптоПро CSP

Инсталляция, деинсталляция и обновление СКЗИ КриптоПро CSP 5.0 КС1 под управлением ОС Android производится в составе прикладной программы, разработанной с применением СКЗИ, либо с помощью дистрибутива, полученного по доверенному каналу. При этих действиях следует руководствоваться документацией от производителя прикладной программы или разработчика СКЗИ.

При установке программного обеспечения СКЗИ КриптоПро CSP необходимо соблюдать требования, указанные в документах ЖТЯИ.00101-01 95 01. Правила пользования и ЖТЯИ.00101-01 91 11. Руководство администратора безопасности. Использование СКЗИ под управлением ОС Android.

2 Интерфейс СКЗИ КриптоПро CSP

Данный раздел является инструкцией по использованию контрольной панели (панели настройки) СКЗИ КриптоПро CSP 5.0 КС1 под управлением ОС Android.

2.1 Доступ к контрольной панели СКЗИ

Панель настройки КриптоПро CSP 5.0 КС1 доступна из прикладной программы, разработанной на базе СКЗИ или из главного меню устройства. В первом случае метод вызова контрольной панели определяет разработчик прикладной программы.

Контрольная панель СКЗИ КриптоПро CSP 5.0 КС1 содержит следующие вкладки:
- **Лицензия**
- **Настройки**
- **Целостность**

Вкладка **Лицензия** предназначена для просмотра информации о версии установленного ПО СКЗИ КриптоПро CSP, информации о лицензии и ввода нового серийного номера (подробнее см. Ввод серийного номера лицензии КриптоПро CSP).

Вкладка **Настройки** предназначена для управления ключевыми носителями и журналированием в СКЗИ.

Вкладка **Целостность** позволяет проверить целостность приложения и содержит информацию об используемых библиотеках криптопровайдера.

2.2 Ввод серийного номера лицензии КриптоПро CSP

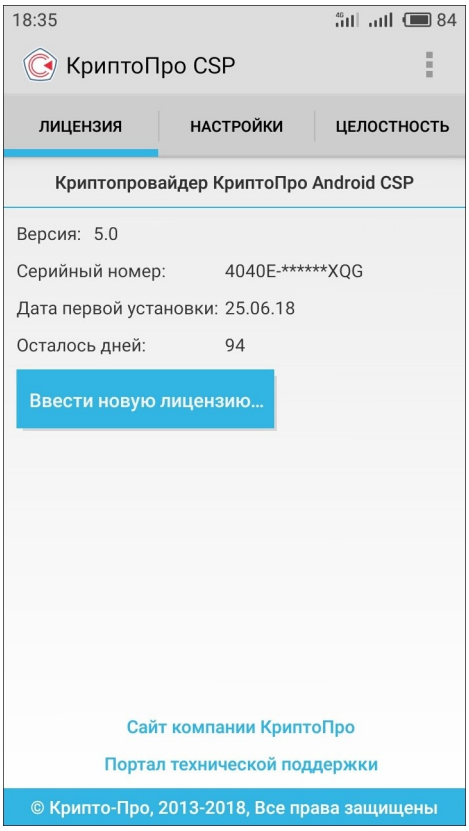
При установке программного обеспечения КриптоПро CSP 5.0 КС1 под управлением ОС Android без ввода лицензии пользователю предоставляется лицензия с ограниченным сроком действия. Для использования СКЗИ после окончания этого срока необходимо приобрести лицензию у организации-разработчика или организации, имеющей права распространения продукта.

Существует два способа лицензирования СКЗИ КриптоПро CSP 5.0 КС1 для Android:

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

2) Ввод лицензии пользователем через контрольную панель.

Для ввода номера лицензии через контрольную панель откройте вкладку **Лицензия** и нажмите кнопку **Ввести новую лицензию**. В открывшемся диалоговом окне введите 25-значный номер лицензии и нажмите кнопку **OK** (см. рис. 1).



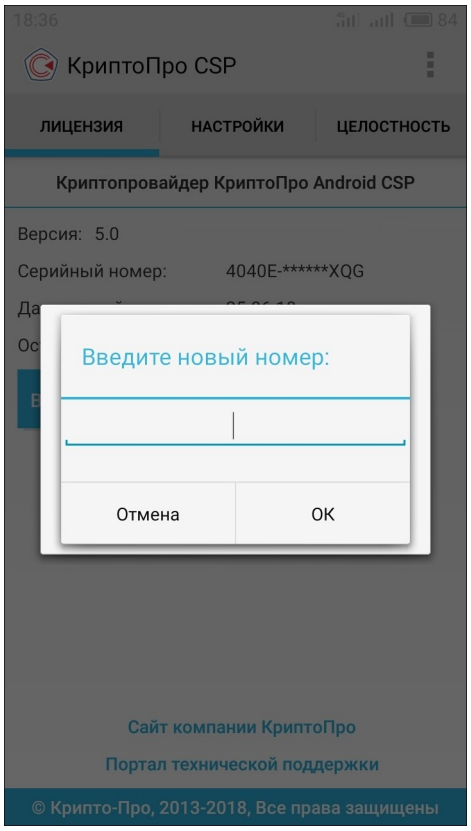


Рисунок 1. Ввод серийного номера лицензии

После ввода нового серийного номера текущая лицензия заменится на новую. В случае, если был указан неверный номер лицензии, будет выдана ошибка (см. рис. 2).

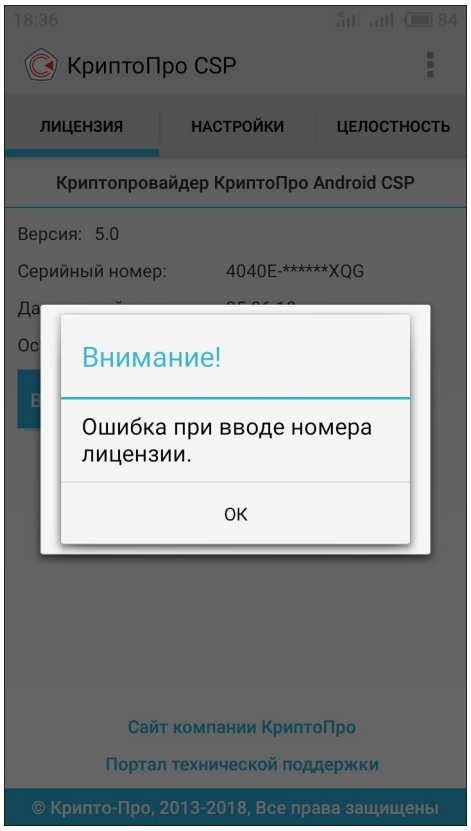


Рисунок 2. Ошибка при вводе некорректного номера лицензии

2.3 Управление ключевыми носителями и журналированием

Управление ключевыми носителями и журналированием осуществляется с помощью вкладки **Настройки** контрольной панели СКЗИ (см. рис. 3).

Для того, чтобы указать тип текущего отделяемого ключевого носителя, необходимо указать данный тип носителя в выпадающем меню «Текущий отделяемый ключевой носитель».

Для установки уровня журналирования событий криптопровайдера необходимо указать в выпадающем меню «Уровень логирования (CSP)» одно из значений — Easy, Medium, Hard.

Также с помощью вкладки **Настройки** возможно указать доступные типы хранилищ, установив флаг напротив соответствующей записи, и отключить предупреждения, выводящиеся пользователю при использовании ключей ЭП ГОСТ Р 34.10-2001.

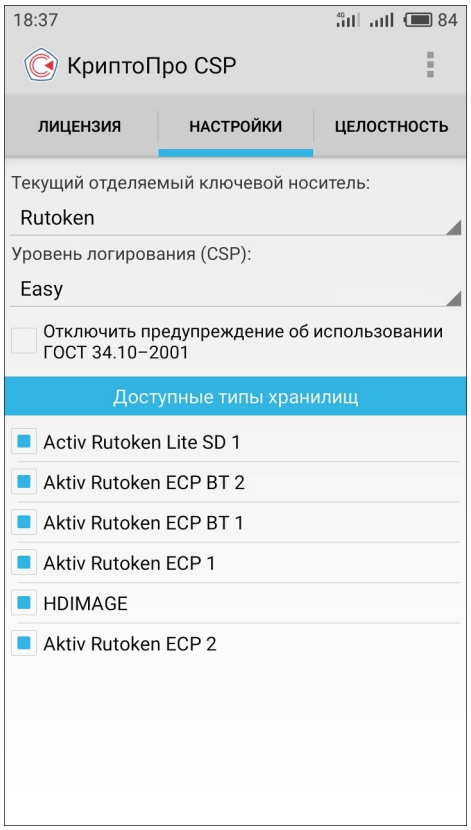


Рисунок 3. Вкладка **Настройки** контрольной панели КриптоПро CSP

2.4 Проверка целостности

Контроль целостности СКЗИ КриптоПро CSP 5.0 КС1 под управлением ОС Android осуществляется автоматически каждый раз при запуске приложения. Результаты проверки целостности, а также перечень контролируемых библиотек криптопровайдера и соответствующие значения хэш-функции представлены на вкладке **Целостность** (см. рис. 4).

Для ручного запуска процесса проверки целостности перейдите на вкладку **Целостность** и нажмите кнопку **Проверить**. По окончанию проверки результат будет отображен во вкладке.

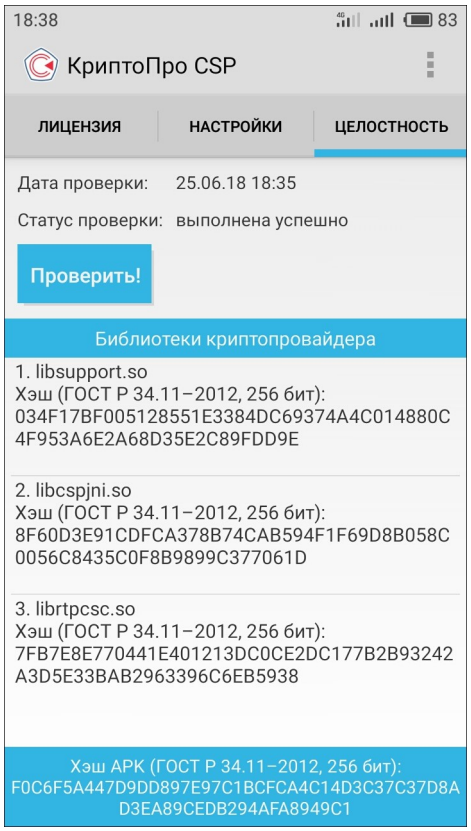


Рисунок 4. Вкладка **Целостность** контрольной панели КриптоПро CSP

2.5 Панель управления КриптоПро CSP

Для перехода в панель управления СКЗИ КриптоПро CSP нажмите на кнопку в верхнем правом углу и выберите в выпадающем меню «Панель управления». Откроется **Панель управления** КриптоПро CSP(см. рис. 5).

Панель управления КриптоПро CSP содержит информацию о ключевых контейнерах и сертификатах, упорядоченных по 4 хранилищам: Личные, Промежуточные УЦ, Корневые УЦ и Адресаты. Нажмите на сертификат для просмотра информации о нем.

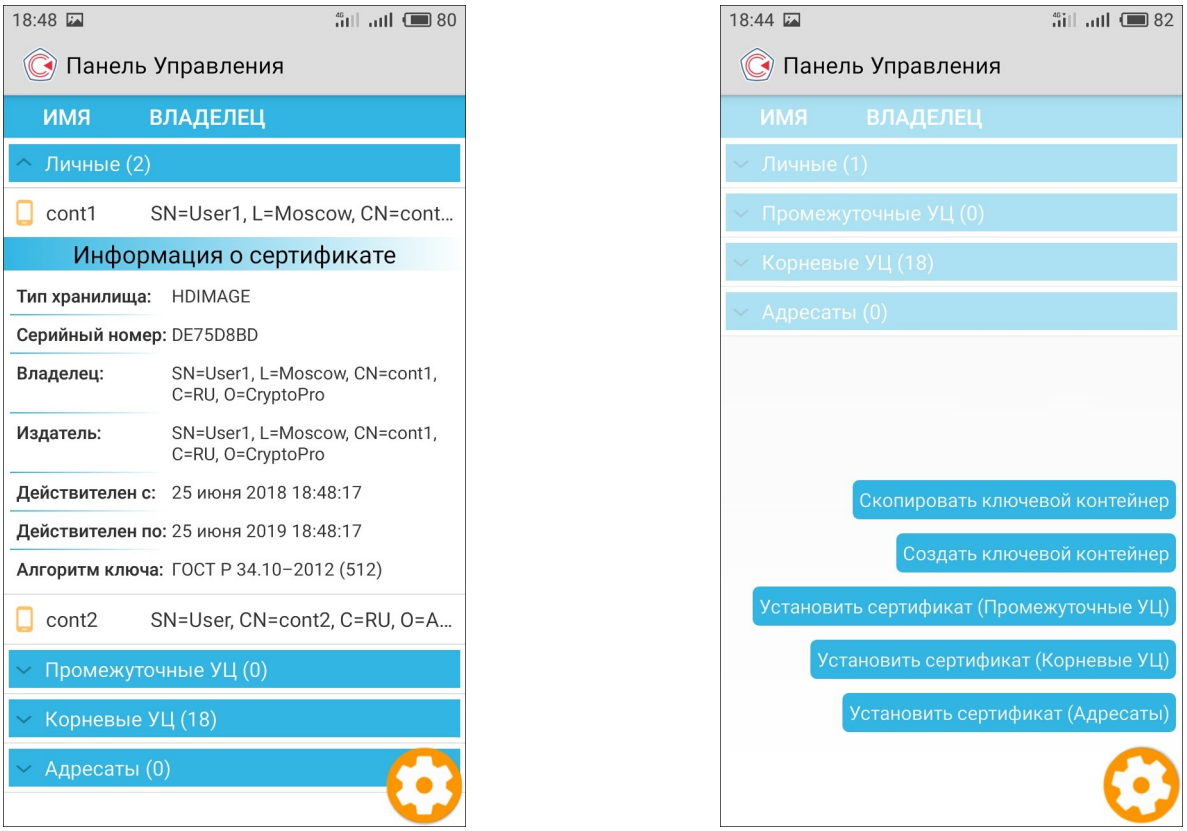


Рисунок 5. Панель управления КриптоПро CSP

Для вызова контекстного меню нажмите кнопку  , далее выберите необходимое действие.

С помощью **Панели управления** КриптоПро CSP возможны следующие действия:

- копирование ключевого контейнера;
- создание ключевого контейнера;
- установка сертификата в хранилище (Промежуточные УЦ, Корневые УЦ, Адресаты).

2.5.1 Создание ключевого контейнера

Для создания ключевого контейнера в контекстном меню Панели управления выберите **Создать ключевой контейнер**. Откроется окно «Создание ключевого контейнера» (см. рис. 6). Заполните поля на вкладке **Контейнер**, указав тип и имя контейнера, алгоритм и тип ключа, далее заполните сведения о сертификате на вкладке **Сертификат**. Нажмите кнопку **Создать** для создания контейнера с указанными параметрами.

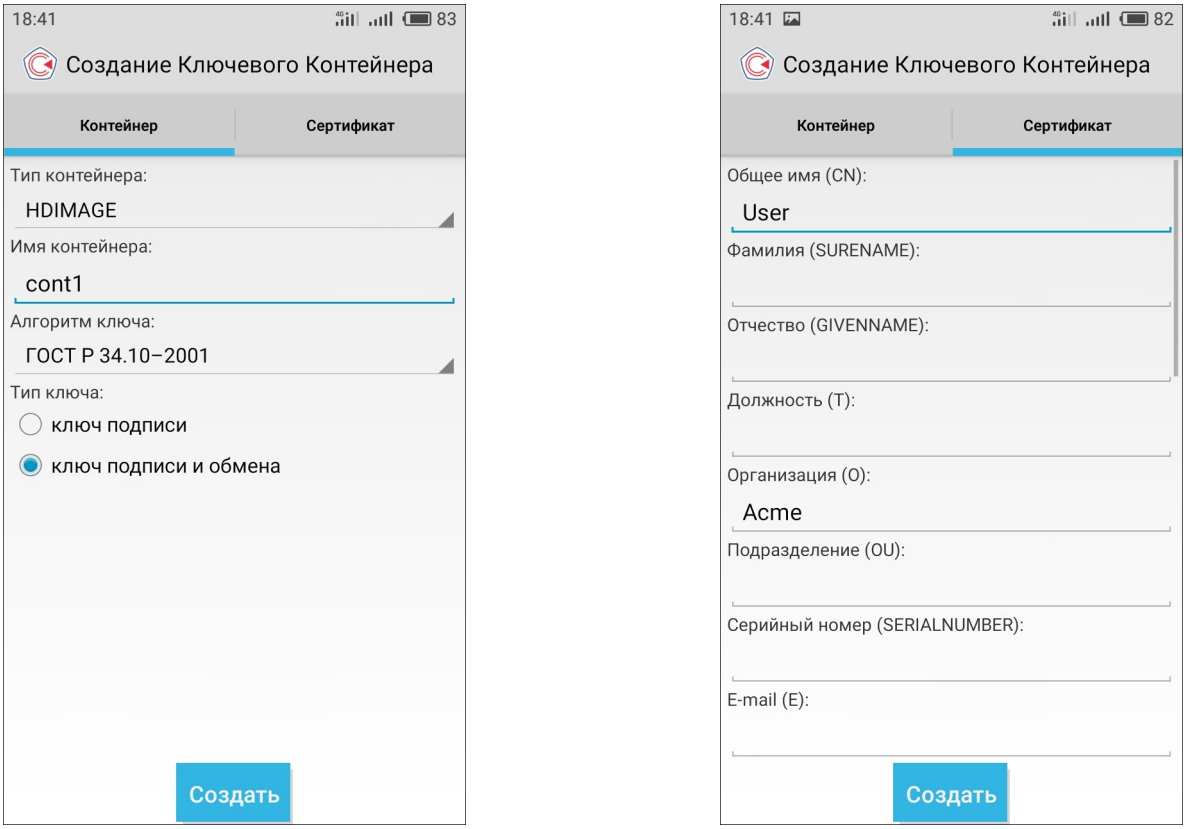


Рисунок 6. Создание ключевого контейнера

При создании контейнера и генерации ключа откроется окно генерации начальной последовательности ДСЧ с помощью биологического ДСЧ (см. рис. 7). Для генерации случайной последовательности нажимайте на экран до завершения работы ДСЧ.

По окончании формирования случайной последовательности откроется окно ввода ПИН на доступ к ключу создаваемого контейнера (см. рис. 8). Введите пин-код и подтвердите его повторным вводом, затем нажмите кнопку **OK**. Созданный контейнер появится в списке хранилища **Личные** Панели управления.

Рисунок 7. Окно биологического ДСЧ

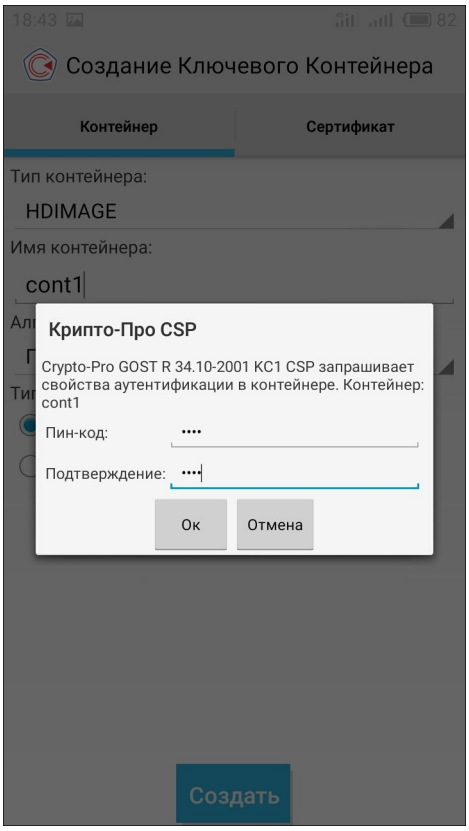


Рисунок 8. Установка пин-кода на доступ к ключу

2.5.2 Копирование ключевого контейнера

Для копирования ключевого контейнера в контекстном меню Панели управления выберите **Создать ключевой контейнер**. Откроется окно «Копирование ключевого контейнера» (см. рис. 9). По кнопке выберите в хранилище устройства контейнер, который вы хотите скопировать, и нажмите кнопку **Копировать**. Если на доступ к контейнеру установлен пин-код, то он будет запрошен. Введите пин-код и нажмите кнопку **OK**. Скопированный контейнер появится в списке хранилища **Личные** Панели управления.

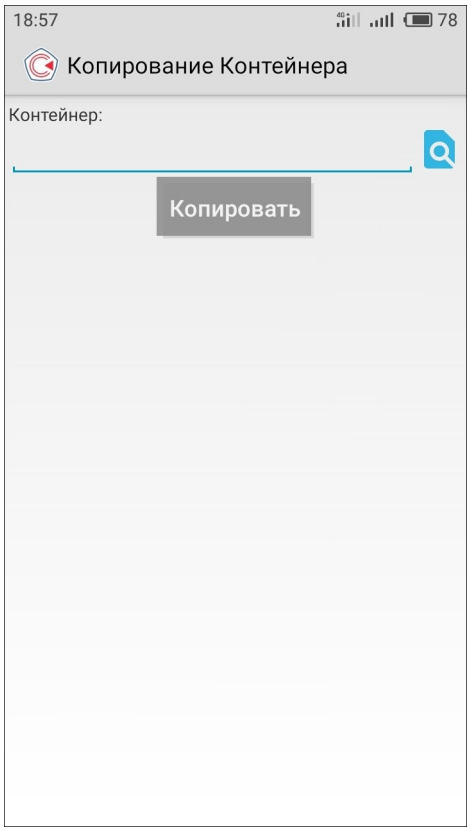


Рисунок 9. Копирование ключевого контейнера

2.5.3 Удаление ключевого контейнера

Для удаления контейнера откройте Панель управления и долгим нажатием выберите контейнер, который вы хотите удалить. Откроется меню действий с контейнером. Нажмите на кнопку . Откроется окно подтверждения удаления контейнера, нажмите кнопку **OK** (см. рис. 10).

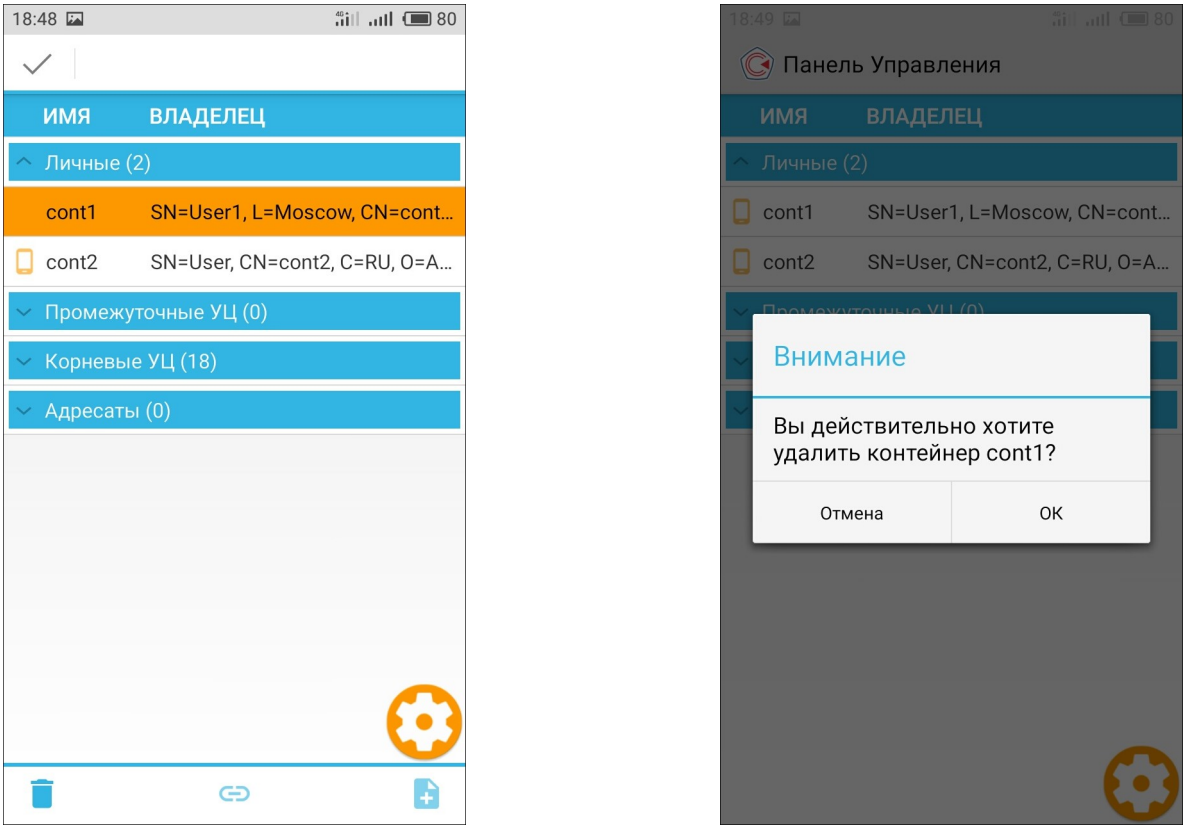


Рисунок 10. Удаление ключевого контейнера

2.5.4 Создание цепочки сертификатов

Для создания цепочки сертификатов откройте Панель управления и долгим нажатием выберите контейнер с сертификатом, для которого вы хотите построить цепочку. Нажмите на кнопку . Откроется окно «Цепочка сертификатов». При необходимости проверки построенной цепочки установите флаг в соответствующее поле. Нажмите кнопку **Построить**, в случае успешного выполнения операции построенная цепочка сертификатов отобразиться в окне ниже (см. рис. 11).

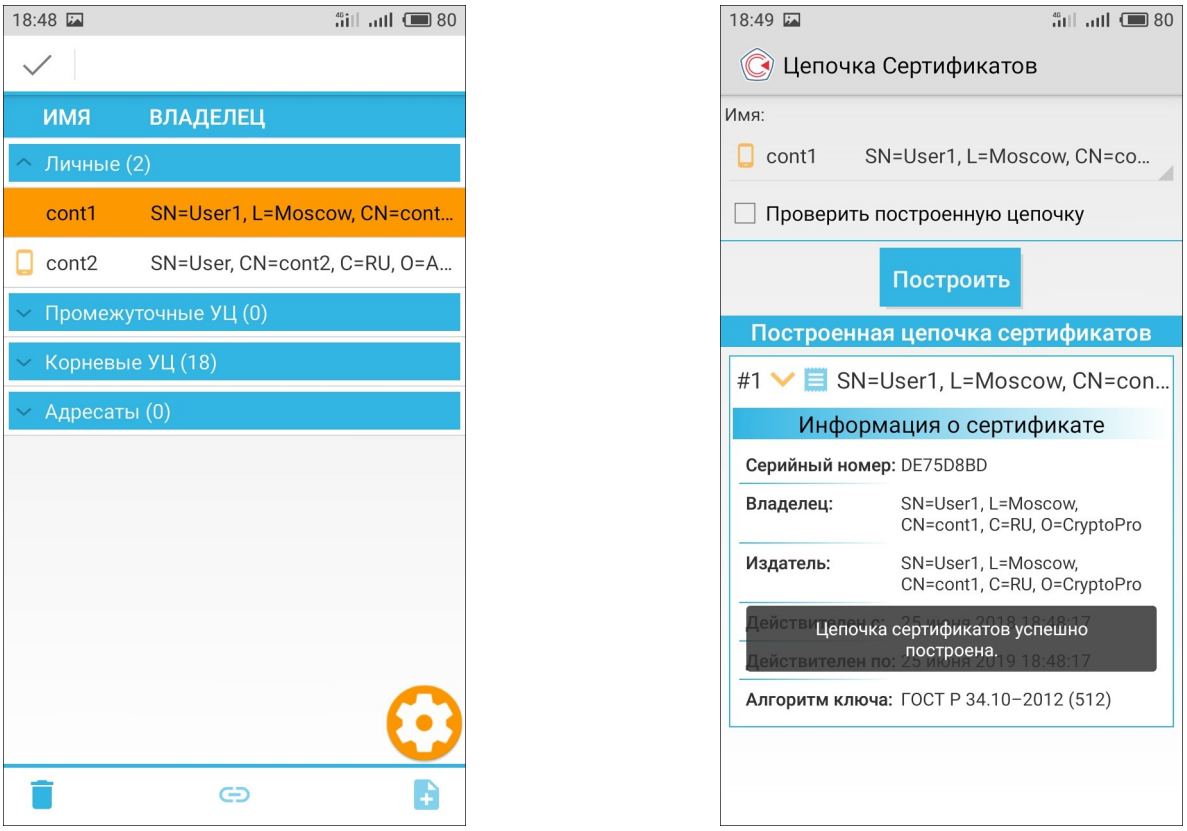
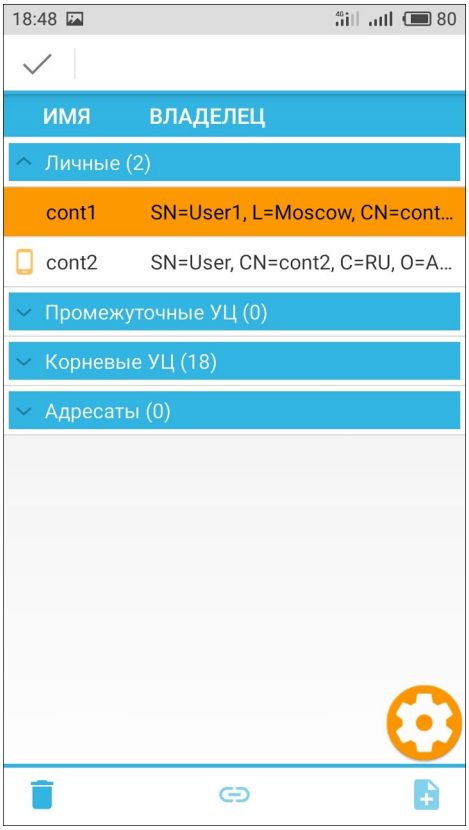


Рисунок 11. Создание цепочки сертификатов

2.5.5 Установка сертификата в контейнер

Для установки сертификата в соответствующий ему контейнер откройте Панель управления и долгим нажатием выберите необходимый контейнер. Нажмите на кнопку . Откроется окно «Установка Сертификата» (см. рис. 12). По кнопке выберите в хранилище устройства сертификат, который необходимо установить в указанный контейнер, и нажмите кнопку **Установить**. Если на доступ к контейнеру установлен пин-код, то он будет запрошен. Введите пин-код и нажмите кнопку **OK**. В случае успешного выполнения операции данные о сертификате в контейнере обновятся в Панели управления.



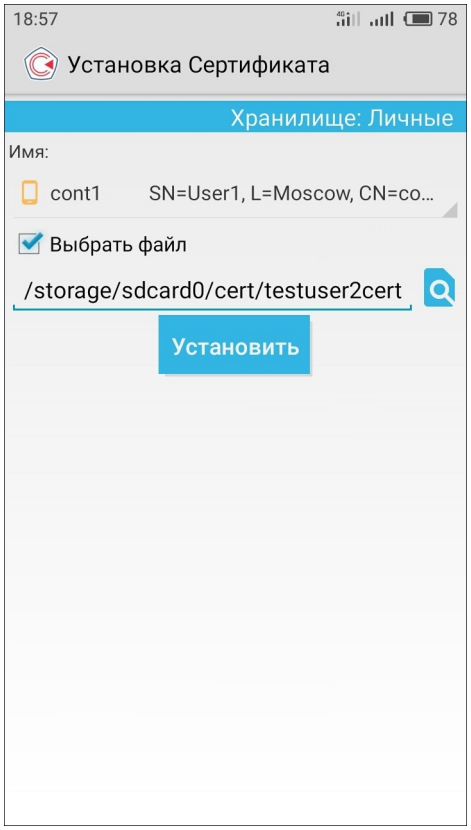


Рисунок 12. Установка сертификата в контейнер

2.5.6 Установка сертификата в хранилище

Для установки сертификата в хранилище (Промежуточные УЦ, Корневые УЦ или Адресаты) в контекстном меню Панели управления выберите **Установить сертификат**. Откроется окно «Копирование ключевого контейнера» (см. рис. 13). По кнопке выберите в хранилище устройства сертификат, который необходимо установить в указанное хранилище (поле Имя заполнится автоматически после выбора сертификата) и нажмите кнопку **Установить**. Установленный сертификат

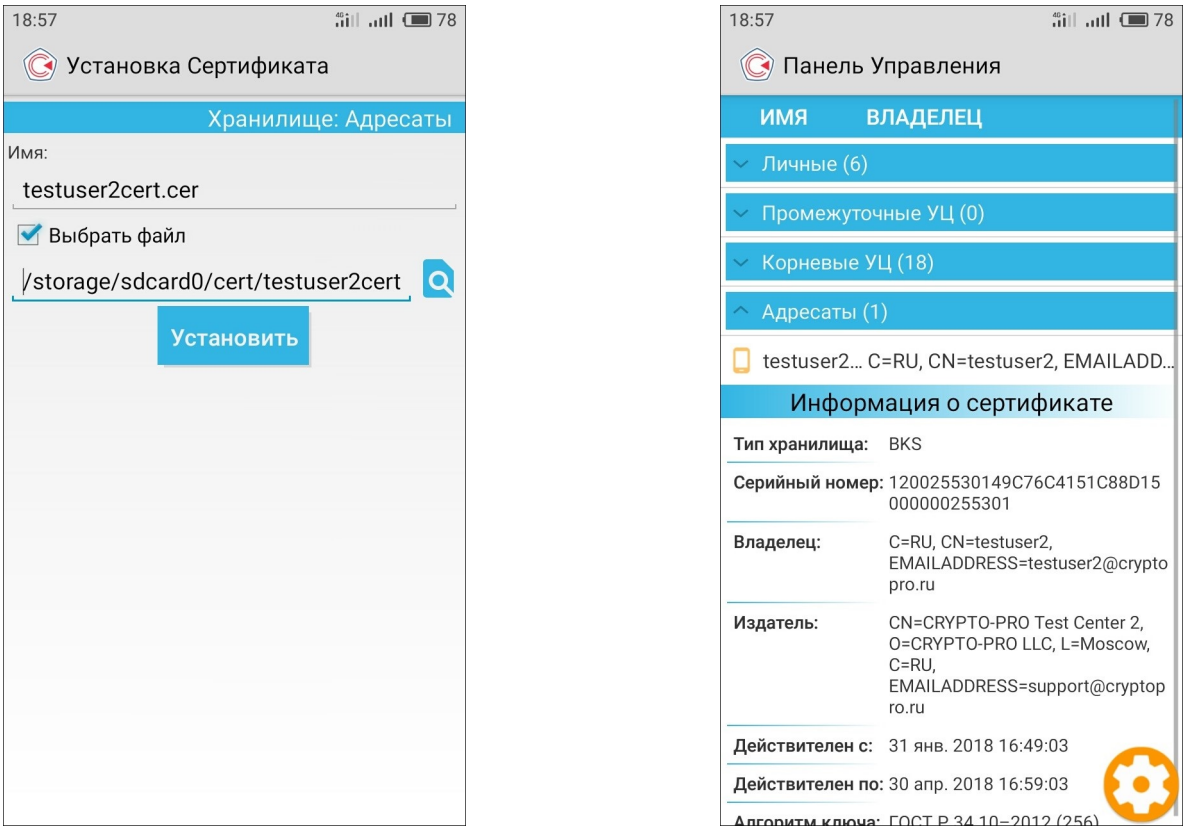


Рисунок 13. Установка сертификата в хранилище