

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



Средство

Криптографической

Защиты

Информации

КриптоПро CSP

Версия 5.0 R2 KC1

Исполнение 1-Base

Инструкция

по использованию СКЗИ
под управлением ОС Android

ЖТЯИ.00101-02 92 03
Листов 25

© ООО «КРИПТО-ПРО», 2000-2022. Все права защищены.

Авторские права на средство криптографической защиты информации КриптоПро CSP и эксплуатационную документацию к нему зарегистрированы в Российском агентстве по патентам и товарным знакам (Роспатент). Документ входит в комплект поставки программного обеспечения СКЗИ КриптоПро CSP версии 5.0 R2 КС1; 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	4
2.1	Доступ к контрольной панели СКЗИ	4
2.2	Ввод серийного номера лицензии	4
2.3	Проверка целостности СКЗИ	7
2.4	Операции с ключевыми контейнерами	8
2.4.1	Создание ключевого контейнера	9
2.4.2	Загрузка ключевого контейнера с устройства	11
2.4.3	Управление ключевым контейнером	12
2.4.4	Копирование ключевого контейнера	13
2.4.5	Удаление ключевого контейнера	14
2.4.6	Просмотр информации о ключевом контейнере	15
2.4.7	Просмотр сертификата из ключевого контейнера	16
2.4.8	Установка сертификата в ключевой контейнер	17
2.4.9	Экспорт сертификата из ключевого контейнера	18
2.4.10	Изменение пароля ключевого контейнера	19
2.5	Операции с сертификатами	20
2.5.1	Просмотр информации о сертификате	21
2.5.2	Установка сертификата в хранилище	22
2.5.3	Управление сертификатом	23
2.5.4	Построение цепочки сертификатов	24
2.5.5	Удаление сертификата	24
2.6	Настройки	25

1 Установка СКЗИ КристоПро CSP

Установка, деинсталляция и обновление СКЗИ КристоПро CSP 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 КристоПро CSP необходимо соблюдать требования, указанные в документах «ЖТЯИ.00101-02 95 01. КристоПро CSP. Правила пользования» и «ЖТЯИ.00101-02 91 11. КристоПро CSP. Руководство администратора безопасности. Android».

2 Интерфейс СКЗИ КристоПро CSP

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


2.1 Доступ к контрольной панели СКЗИ

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

Главный экран СКЗИ КристоПро CSP содержит вкладки **Лицензия** и **Целостность**.

Вкладка **Лицензия** предназначена для просмотра информации о версии установленного ПО СКЗИ КристоПро CSP, информации о лицензии и ввода нового серийного номера лицензии.

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

Боковая панель управления СКЗИ предоставляет доступ к вкладкам **Сертификаты**, **Ключевые контейнеры** и **Настройки**. Чтобы открыть боковую панель, нажмите кнопку .

Вкладка **Сертификаты** содержит перечень установленных на устройстве сертификатов.

Вкладка **Ключевые контейнеры** содержит информацию о ключевых контейнерах на устройстве, а также предоставляет функции загрузки и создания нового ключевого контейнера.


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

2.2 Ввод серийного номера лицензии

При установке программного обеспечения КристоПро CSP без ввода лицензии пользователю предоставляется временная лицензия с ограниченным сроком действия на 3 месяца. Для полноценного использования СКЗИ необходимо приобрести лицензию у организации-разработчика или организации, имеющей права распространения продукта.

Существует два способа лицензирования СКЗИ КристоПро CSP для Android:

- 1) Лицензия на приложение — производитель приложения поставляет его вместе с лицензией на КристоПро CSP. Ввод лицензии пользователем не требуется.
- 2) Ввод лицензии пользователем через контрольную панель.

Для ввода номера лицензии через контрольную панель нажмите кнопку  на вкладке **Лицензия**. В открывшемся диалоговом окне введите номер лицензии и нажмите кнопку **ОК** (см. [рис. 1](#)).

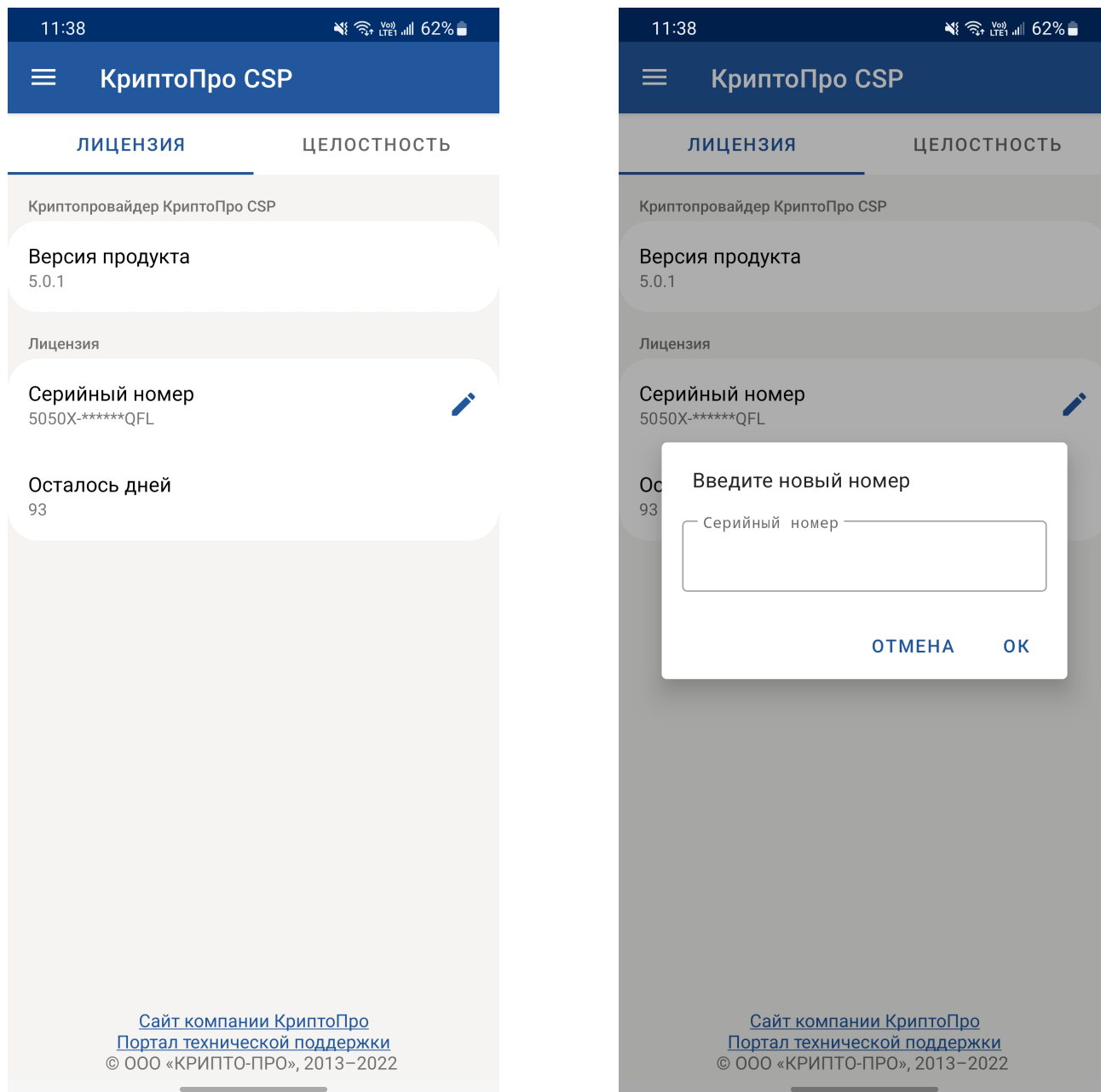


Рисунок 1. Ввод серийного номера лицензии

После ввода нового серийного номера текущая лицензия заменится на новую. Если был указан неверный номер лицензии, будет выдана ошибка (см. [рис. 2](#)).

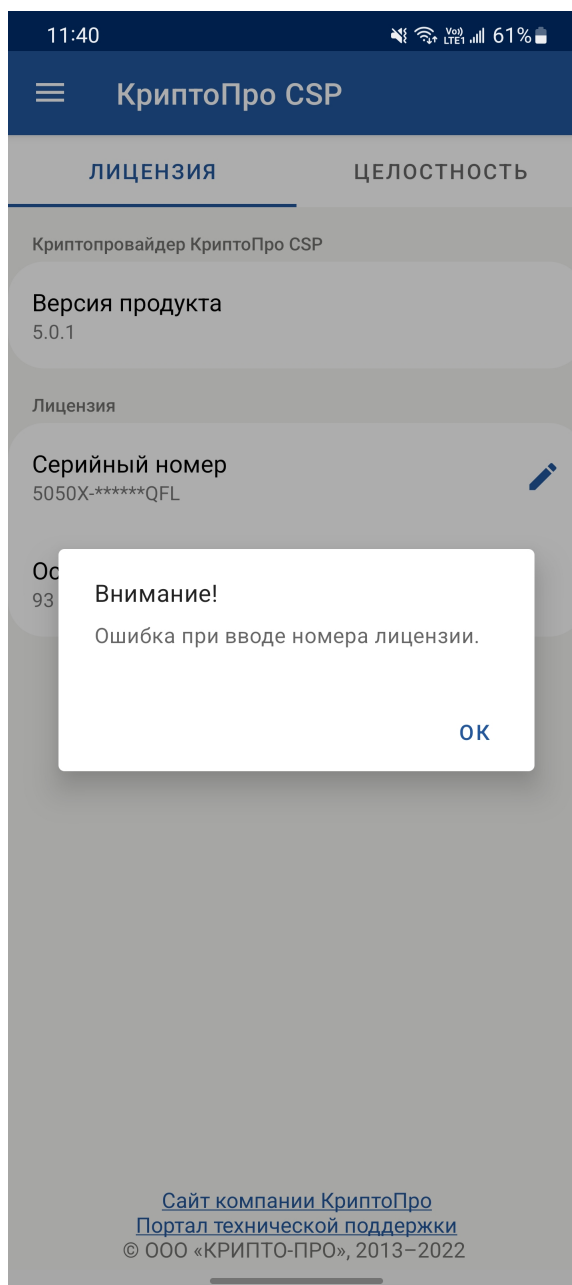



Рисунок 2. Ошибка при вводе некорректного номера лицензии

2.3 Проверка целостности СКЗИ

Контроль целостности СКЗИ осуществляется автоматически каждый раз при запуске приложения. Результаты проверки целостности отображаются в поле **Статус**. Также вкладка содержит перечень контролируемых библиотек криптопровайдера и соответствующие значения хэш-функций.

Для ручного запуска процесса проверки целостности нажмите кнопку .

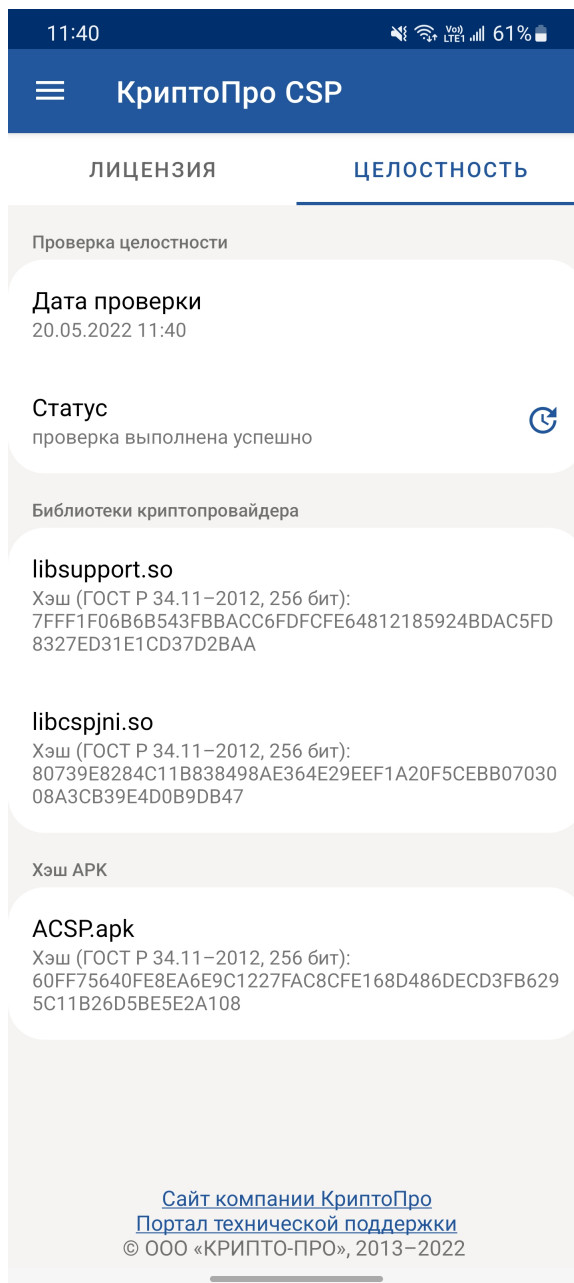


Рисунок 3. Вкладка Целостность

2.4 Операции с ключевыми контейнерами

На вкладке **Ключевые контейнеры** доступны следующие операции с ключевыми контейнерами:

- просмотр перечня доступных ключевых контейнеров;
- создание нового ключевого контейнера и отправка запрос на сертификат;
- загрузка существующего контейнера с устройства.

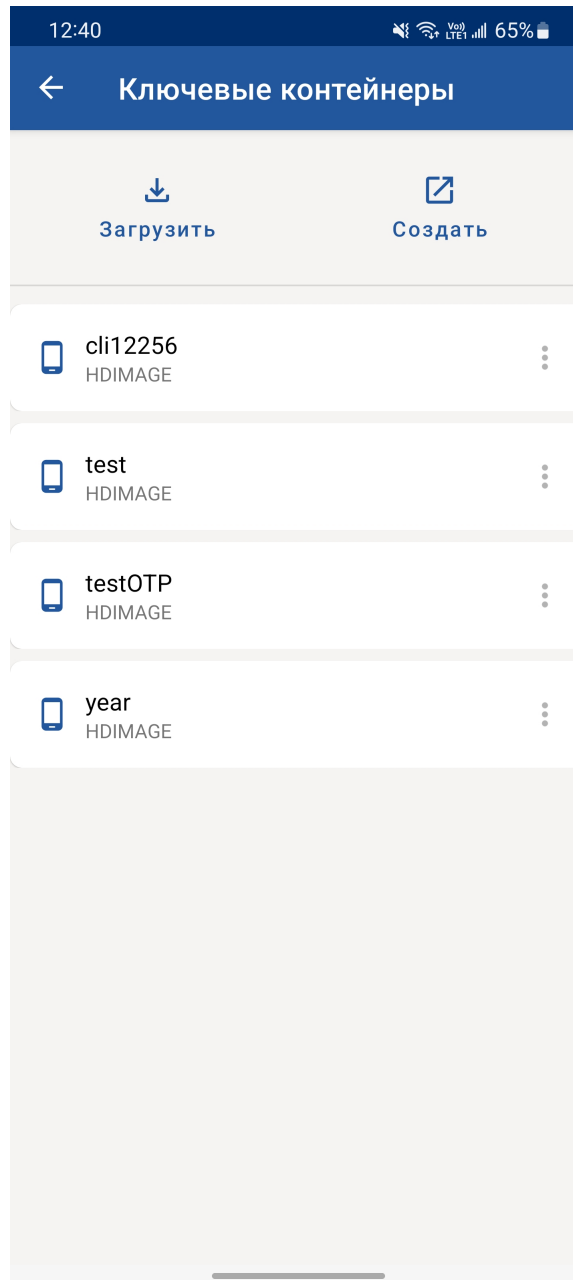



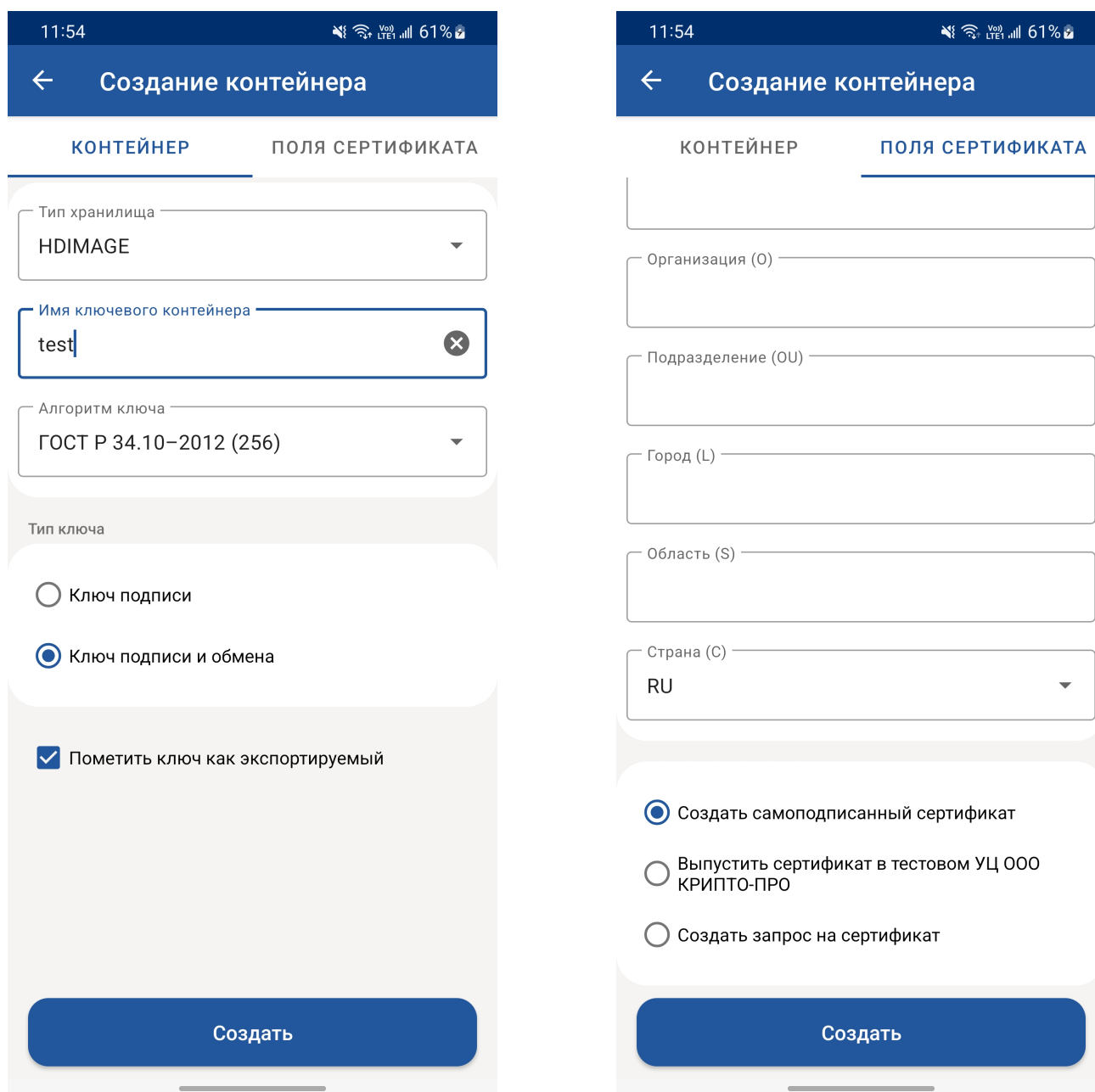
Рисунок 4. Вкладка **Ключевые контейнеры**

Чтобы обновить перечень доступных ключевых контейнеров, потяните экран сверху вниз.

2.4.1 Создание ключевого контейнера

Для создания ключевого контейнера нажмите кнопку **Создать**  на вкладке **Ключевые контейнеры** (см. [рис. 4](#)).

Откроется окно «Создание контейнера» (см. [рис. 5](#)). Заполните поля на вкладке **Контейнер**, указав тип хранилища контейнера, имя контейнера, алгоритм и тип ключа, признак экспортируемости ключа. Далее перейдите на вкладку **Поля сертификата** и заполните сведения о сертификате (см. [рис. 5](#)), указав способ выпуска сертификата (самоподписанный сертификат или сертификат, выпущенный в тестовом УЦ ООО «КРИПТО-ПРО») или выбрав создание запроса на сертификат. Нажмите кнопку **Создать** для создания контейнера с указанными параметрами.



The image displays two screenshots of the "Создание контейнера" (Container Creation) screen in the CryptoPro CSP application. The left screenshot shows the "КОНТЕЙНЕР" (Container) tab, and the right screenshot shows the "ПОЛЯ СЕРТИФИКАТА" (Certificate Fields) tab.

КОНТЕЙНЕР (Left Screenshot):

- Тип хранилища: HDIMAGE
- Имя ключевого контейнера: test
- Алгоритм ключа: ГОСТ Р 34.10-2012 (256)
- Тип ключа:
 - ☐ Ключ подписи
 - ☒ Ключ подписи и обмена
- ☒ Пометить ключ как экспортируемый
- Кнопка: Создать

ПОЛЯ СЕРТИФИКАТА (Right Screenshot):

- Организация (O):
- Подразделение (OU):
- Город (L):
- Область (S):
- Страна (C): RU
- Способ выпуска сертификата:
 - ☒ Создать самоподписанный сертификат
 - ☐ Выпустить сертификат в тестовом УЦ ООО КРИПТО-ПРО
 - ☐ Создать запрос на сертификат
- Кнопка: Создать

Рисунок 5. Создание ключевого контейнера

При создании контейнера и генерации ключа откроется окно генерации начальной последовательности ДСЧ с помощью биологического ДСЧ (см. [рис. 6](#)). 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. 7](#)). Введите пин-код и подтвердите его повторным вводом, затем нажмите кнопку **ОК**. Созданный контейнер появится в списке доступных контейнеров в окне **Ключевые контейнеры**.



Рисунок 6. Окно биологического ДСЧ

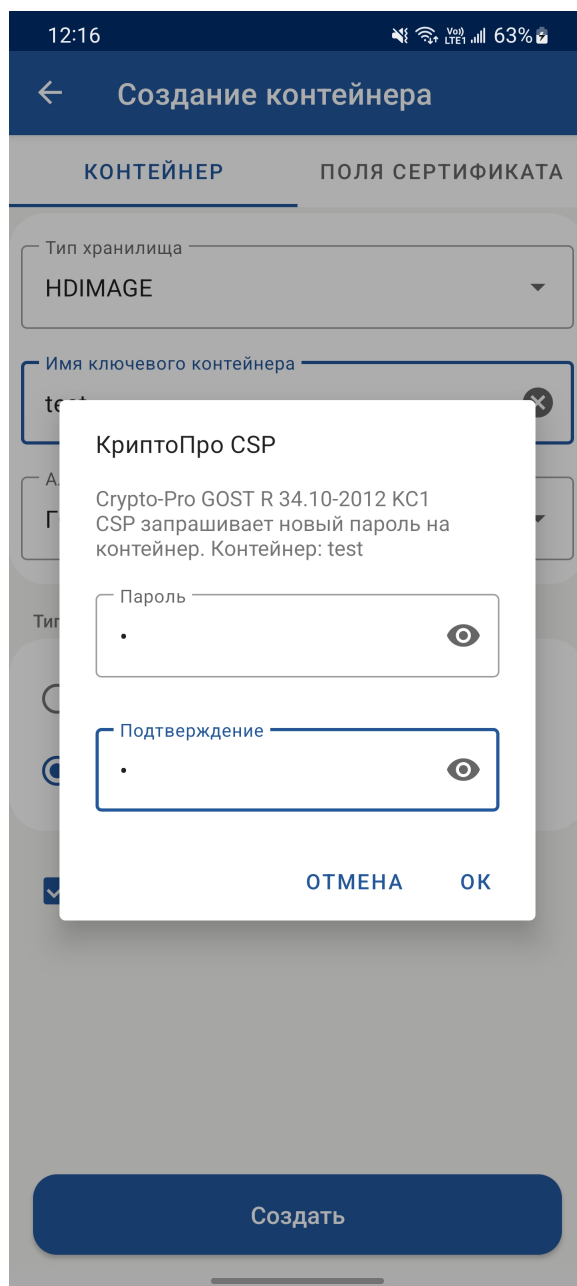



Рисунок 7. Установка пин-кода на доступ к ключу

2.4.2 Загрузка ключевого контейнера с устройства

Чтобы загрузить ранее созданный контейнер с устройства, нажмите кнопку **Загрузить**  на вкладке **Ключевые контейнеры** (см. [рис. 4](#)). В открывшемся проводнике выберете конечную папку с ключевым контейнером и нажмите кнопку **Использовать эту папку** для подтверждения выбора (см. [рис. 8](#)).

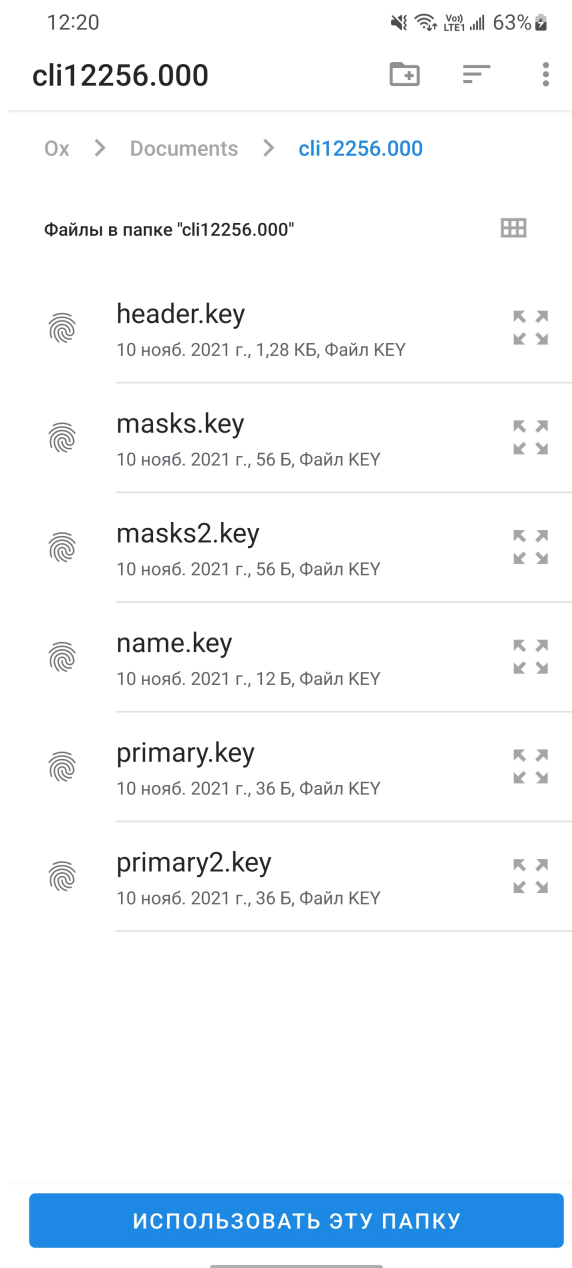



Рисунок 8. Выбор ключевого контейнера в проводнике

2.4.3 Управление ключевым контейнером

На вкладке **Ключевые контейнеры** у необходимого контейнера нажмите на кнопку . В открывшемся меню (см. [рис. 9](#)) доступны следующие действия с ключевым контейнером:

- Копирование ключевого контейнера;
- Удаление ключевого контейнера;
- Просмотр информации о ключевом контейнере;
- Просмотр сертификата из ключевого контейнера;
- Установка сертификата в ключевой контейнер;
- Экспорт сертификата из ключевого контейнера;
- Изменение пароля ключевого контейнера.

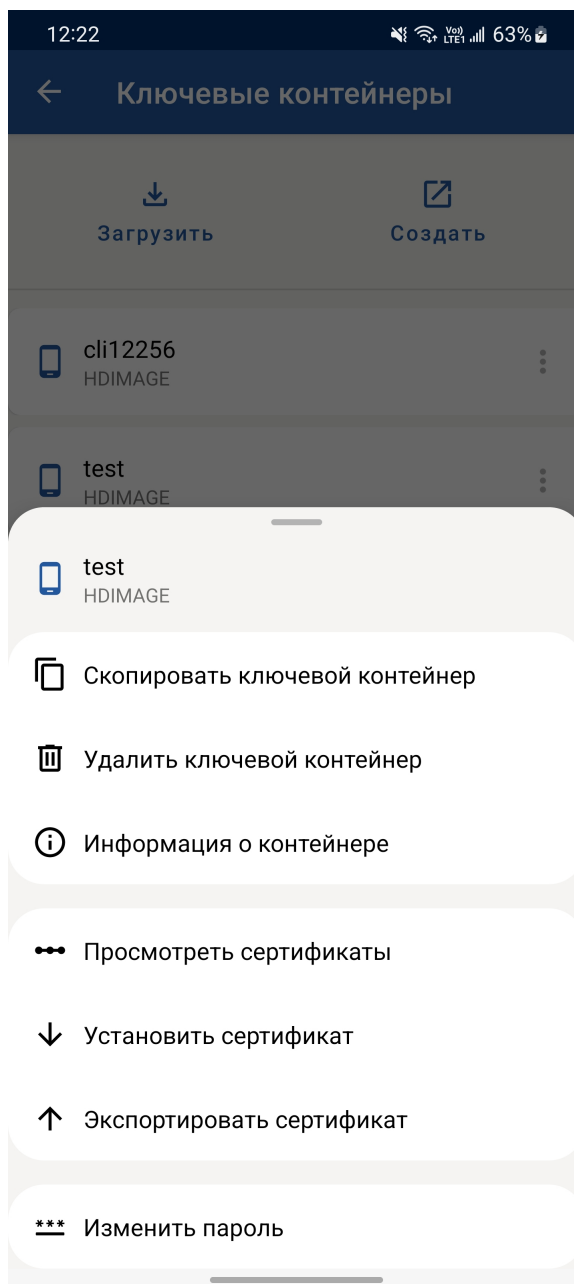



Рисунок 9. Управление контейнером

2.4.4 Копирование ключевого контейнера

Для копирования ключевого контейнера на вкладке **Ключевые контейнеры** нажмите на кнопку  у необходимого контейнера, в открывшемся меню нажмите кнопку **Скопировать ключевой контейнер**. Откроется окно «Копирование контейнера» (см. [рис. 10](#)).

Укажите имя для копии контейнера, текущий пароль от копируемого контейнера, новый пароль для копии и подтвердите его повторным вводом. Нажмите кнопку **Копировать** для копирования контейнера с указанными параметрами. Скопированный контейнер появится в перечне доступных контейнеров вкладки **Ключевые контейнеры**.

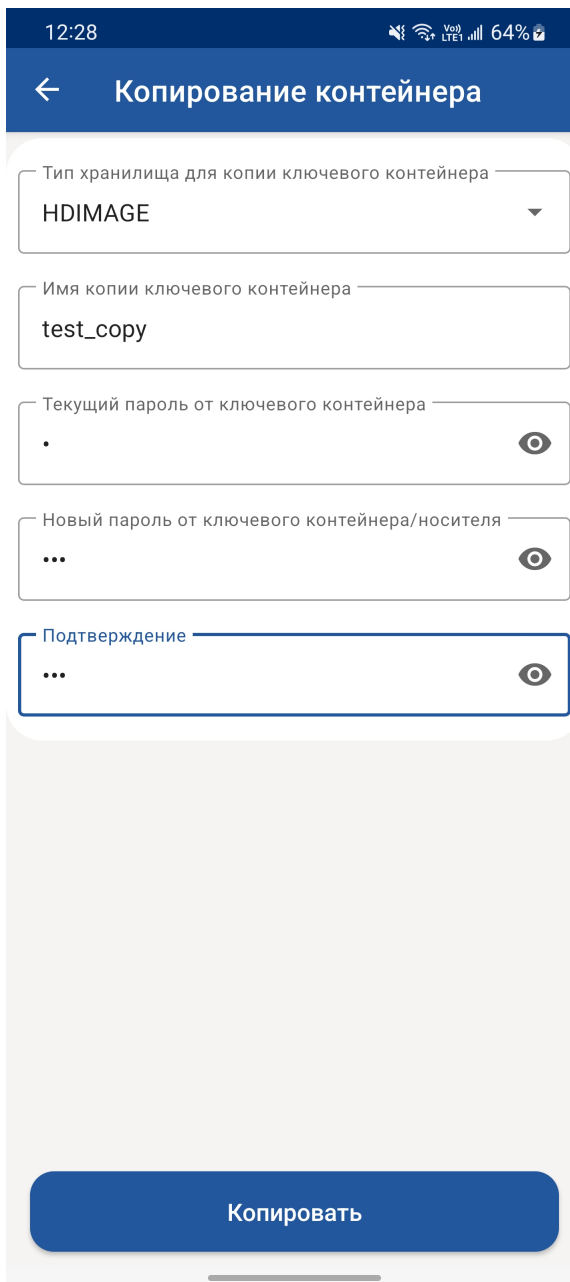



Рисунок 10. Копирование ключевого контейнера

2.4.5 Удаление ключевого контейнера

Для удаления ключевого контейнера на вкладке **Ключевые контейнеры** смахните справа налево необходимый контейнер или нажмите на кнопку  у необходимого контейнера, в открывшемся меню нажмите кнопку **Удалить ключевой контейнер**. Откроется окно подтверждения удаления контейнера, нажмите кнопку **ОК** (см. [рис. 11](#)).

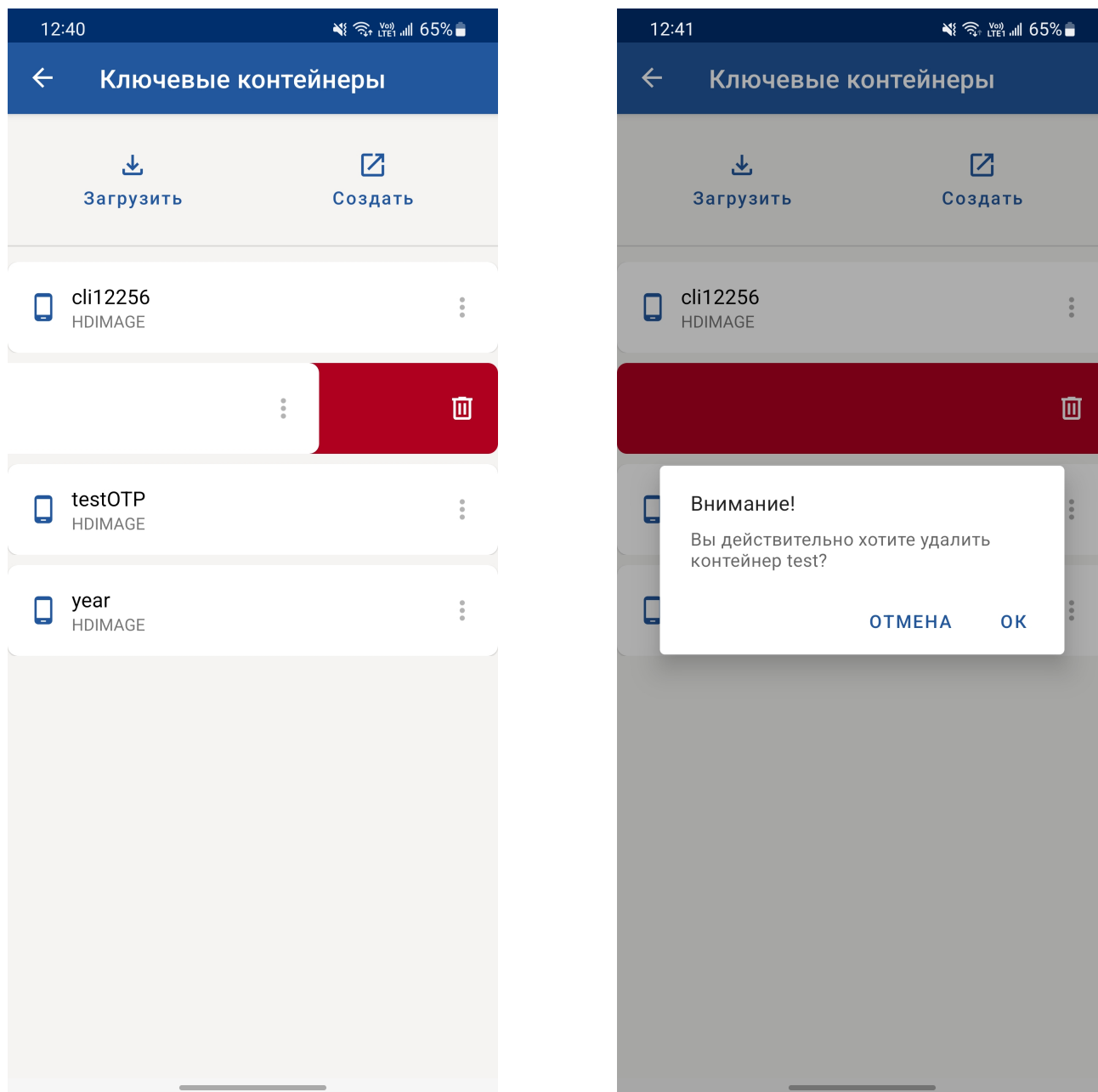



Рисунок 11. Удаление ключевого контейнера

2.4.6 Просмотр информации о ключевом контейнере

Для просмотра информации о контейнере (наличие сертификата в контейнере, алгоритм, длина и срок действия ключа, признак экспортности ключа) на вкладке **Ключевые контейнеры** нажмите на кнопку  у необходимого контейнера, в открывшемся меню нажмите кнопку **Информация о контейнере**.

Откроется окно «Информация о контейнере» (см. [рис. 12](#)).

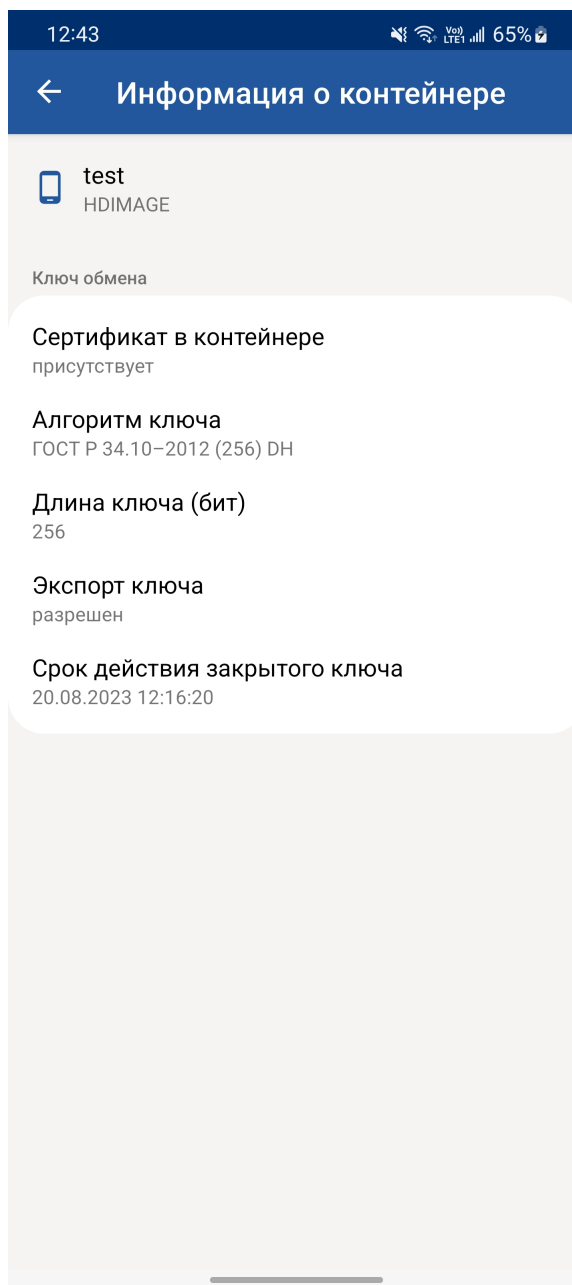




Рисунок 12. Просмотр информации о ключевом контейнере

2.4.7 Просмотр сертификата из ключевого контейнера

Для просмотра информации о сертификате, установленном в ключевом контейнере, на вкладке **Ключевые контейнеры** нажмите на кнопку  у необходимого контейнера, в открывшемся меню нажмите кнопку **Просмотреть сертификаты**.

Откроется окно «Просмотр сертификатов» (см. [рис. 13](#)). Нажмите на сертификат, чтобы увидеть расширенные свойства сертификата (сроки действия, алгоритм ключа и другие).

Чтобы построить цепочку сертификатов, нажмите кнопку . Откроется окно **Цепочка сертификатов** с построенной цепочкой.

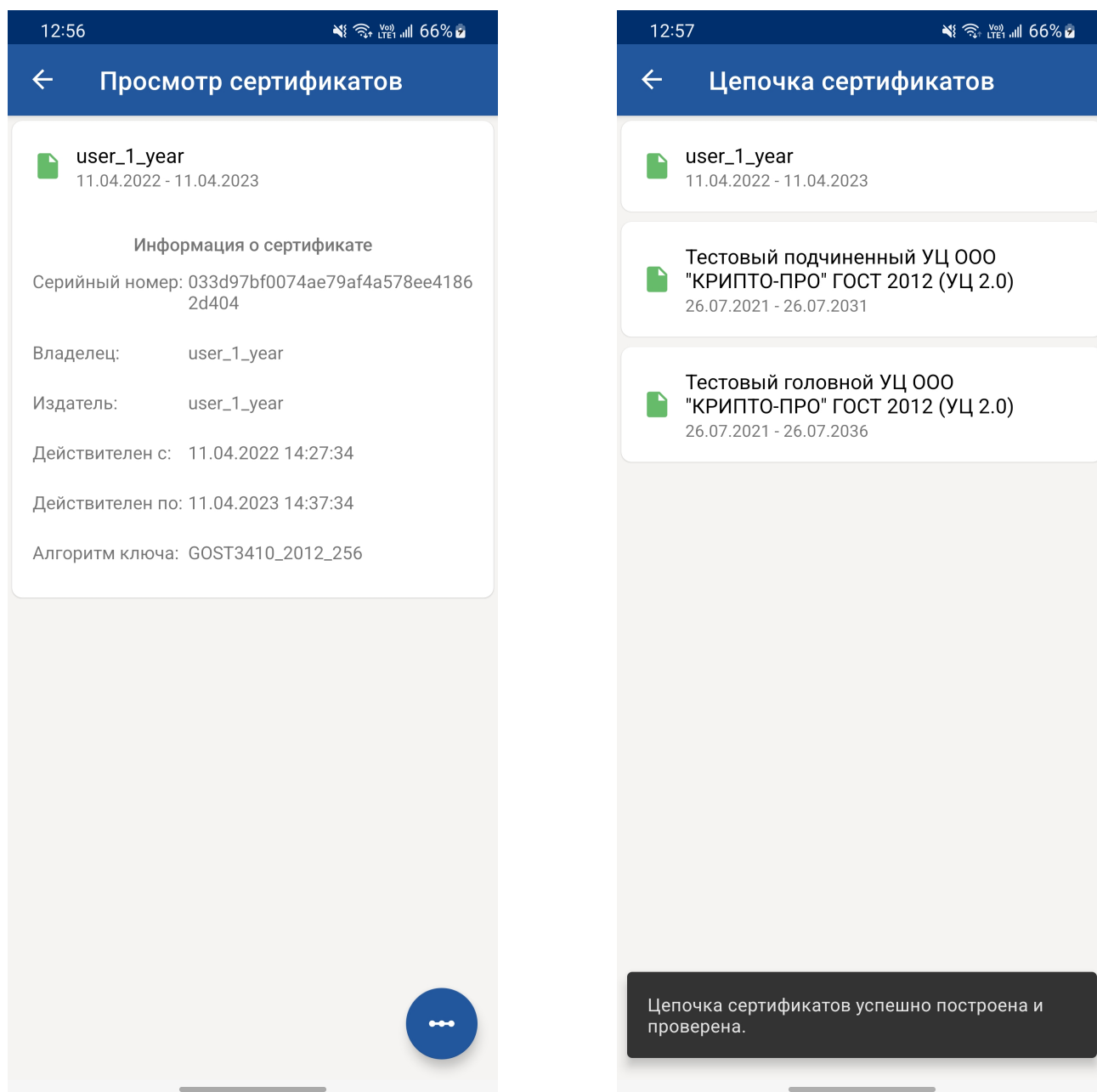



Рисунок 13. Просмотр сертификата (цепочки сертификатов) из ключевого контейнера

2.4.8 Установка сертификата в ключевой контейнер

Чтобы установить сертификат или цепочку сертификатов в контейнер, на вкладке **Ключевые контейнеры** нажмите на кнопку  у необходимого контейнера, в открывшемся меню нажмите кнопку **Установить сертификат**.

Откроется окно «Установка сертификата» (см. [рис. 14](#)). Нажмите кнопку **Расположение файла сертификата** и выберите в проводнике файл с необходимым сертификатом (.cert, .crt) или цепочкой (.p7b). Нажмите кнопку **Установить** для установки выбранного сертификата/цепочки в контейнер.

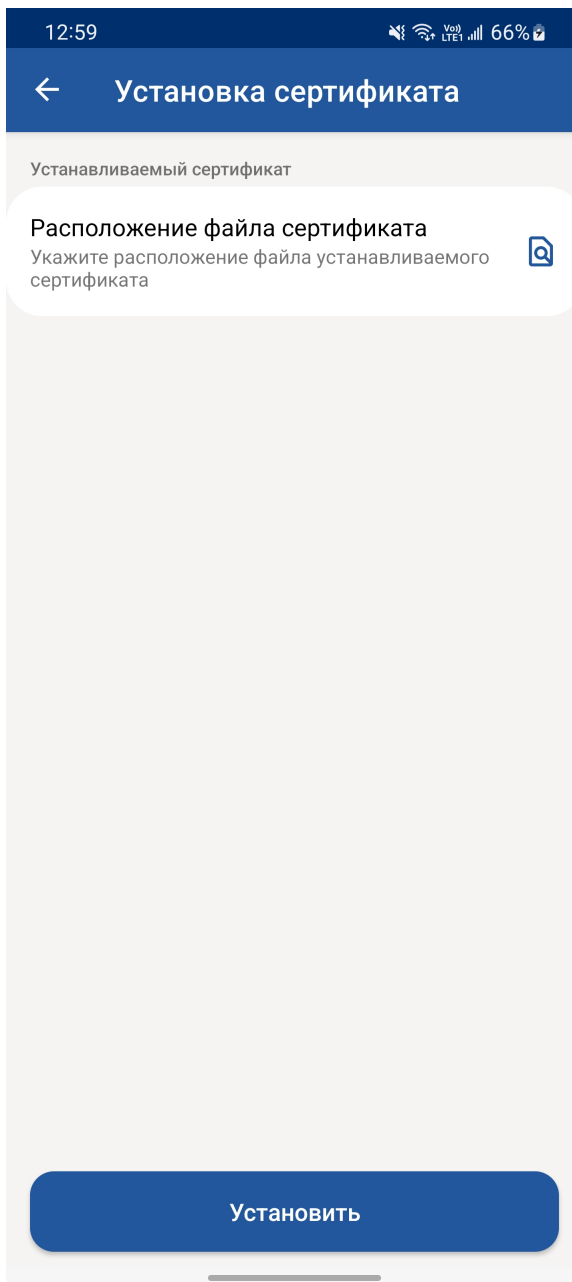



Рисунок 14. Установка сертификата в ключевой контейнер

2.4.9 Экспорт сертификата из ключевого контейнера

Чтобы экспортировать сертификат или цепочку сертификатов из ключевого контейнера, на вкладке **Ключевые контейнеры** нажмите на кнопку  у необходимого контейнера, в открывшемся меню нажмите кнопку **Экспортировать сертификат**.

Откроется окно «Экспорт сертификата» (см. [рис. 15](#)). Установите переключатель в соответствующее поле для выбора объекта экспорта — сертификат или цепочка сертификатов. Нажмите кнопку **Экспортировать** для экспорта сертификата или цепочки. В открывшемся проводнике выберете конечную папку, в которую необходимо экспортировать сертификат или цепочку. Нажмите кнопку **Сохранить** для сохранения файла сертификата или цепочки в указанную папку.

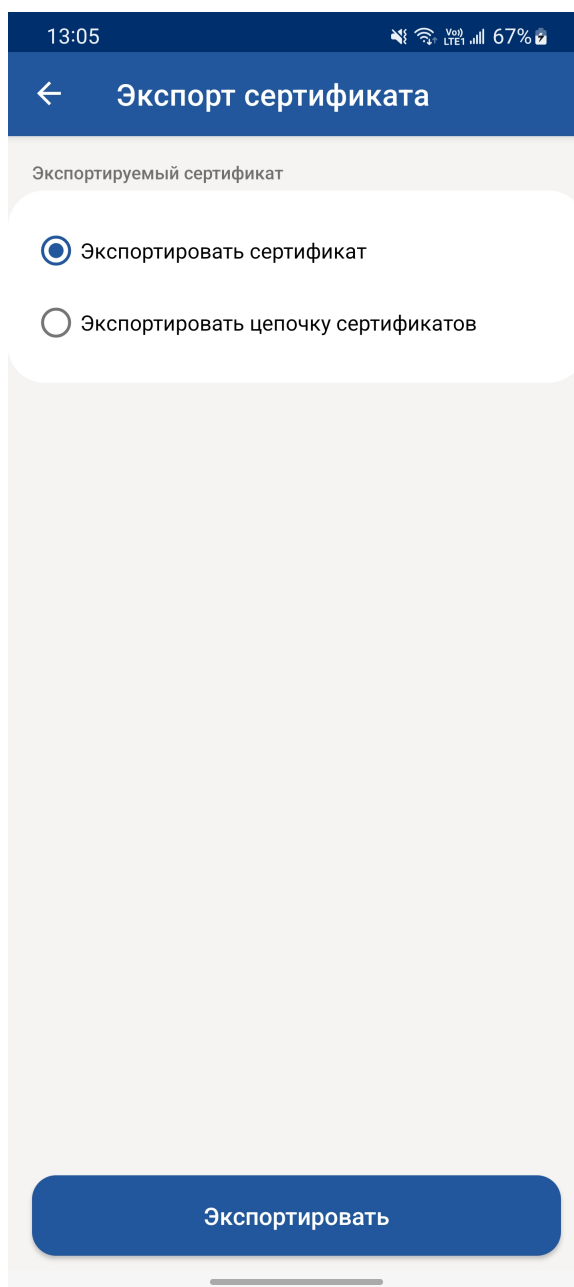

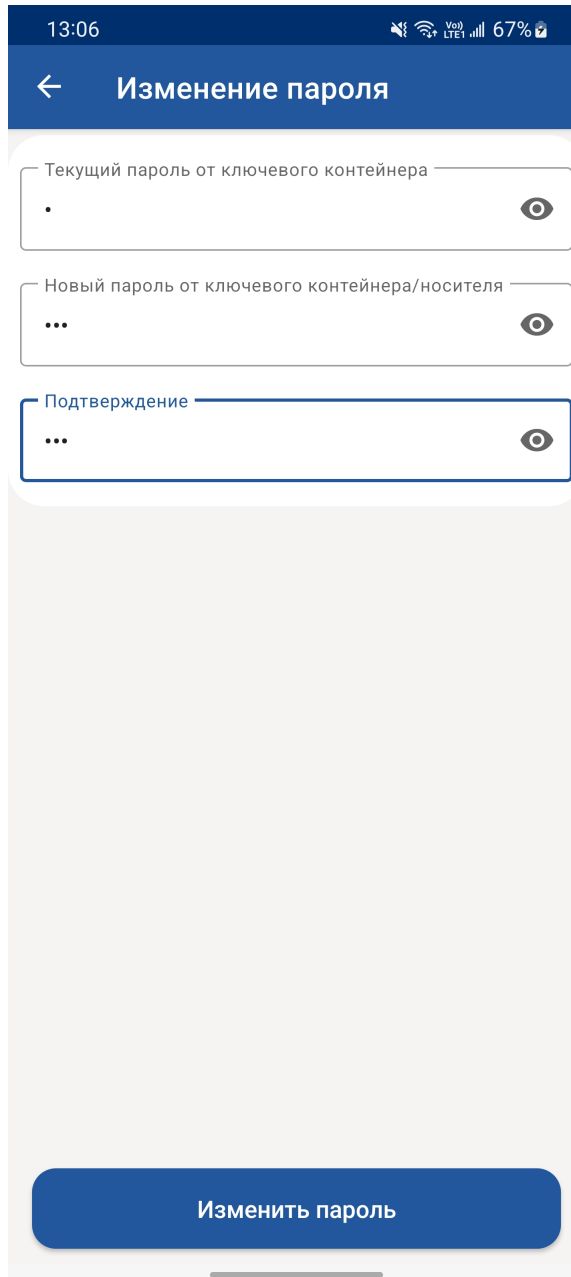


Рисунок 15. Экспорт сертификата из ключевого контейнера

2.4.10 Изменение пароля ключевого контейнера

Для изменения пароля ключевого контейнера на вкладке **Ключевые контейнеры** нажмите на кнопку  у необходимого контейнера, в открывшемся меню нажмите кнопку **Изменить пароль**.

Откроется окно «Изменение пароля» (см. [рис. 16](#)). В соответствующие поля введите текущий пароль от контейнера, новый пароль и подтвердите его повторным вводом. Нажмите кнопку **Изменить пароль**.



13:06

← **Изменение пароля**

Текущий пароль от ключевого контейнера

•

Новый пароль от ключевого контейнера/носителя

...

Подтверждение

...

Изменить пароль

Рисунок 16. Изменение пароля ключевого контейнера

2.5 Операции с сертификатами

Вкладка **Сертификаты** содержит информацию о сертификатах, упорядоченных по 3 хранилищам: Доверенные корневые ЦС, Промежуточные ЦС и Другие пользователи. Чтобы обновить перечень сертификатов, потяните экран сверху вниз.

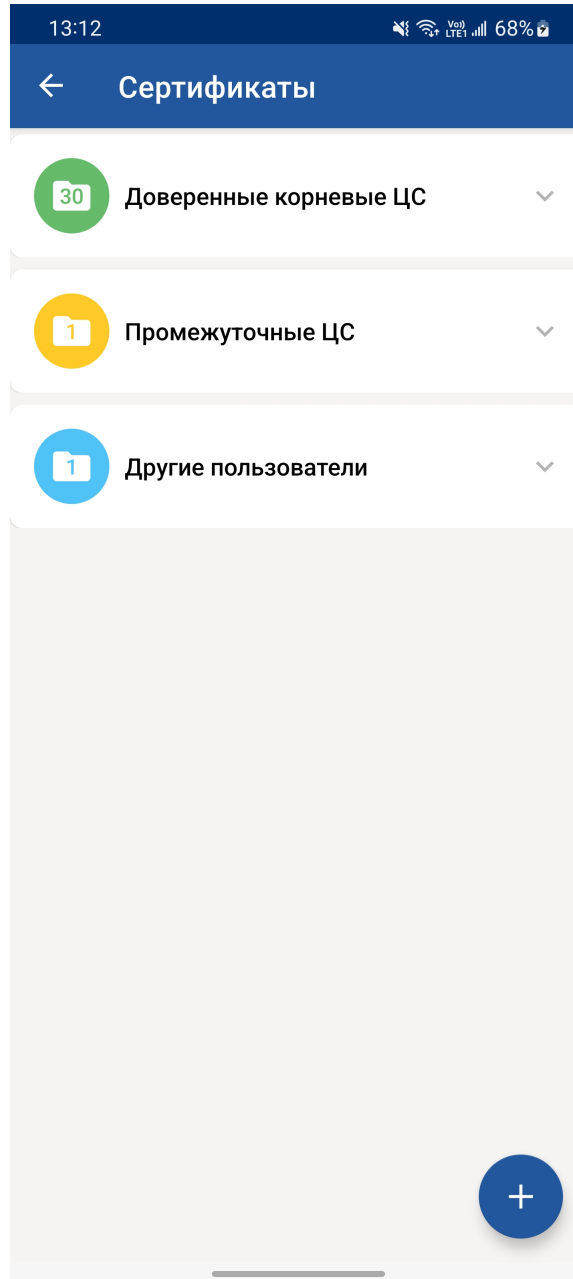


Рисунок 17. Вкладка **Сертификаты**

2.5.1 Просмотр информации о сертификате

Для просмотра информации о сертификате нажмите на сертификат.

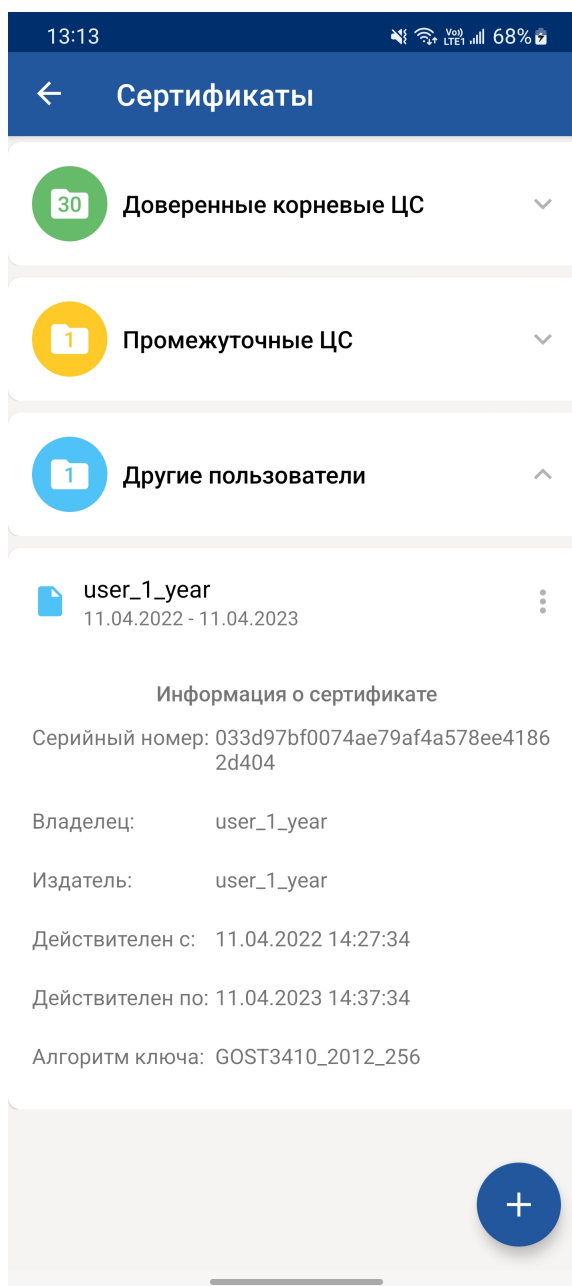



Рисунок 18. Свойства сертификата

2.5.2 Установка сертификата в хранилище

Чтобы установить сертификат с устройства в хранилище, на вкладке **Сертификаты** нажмите кнопку . Откроется окно «Установка сертификата» (см. [рис. 19](#)). Установите переключатель напротив необходимого хранилища, в которое будет помещен сертификат. Нажмите кнопку **Расположение файла сертификата** и выберите в проводнике файл с необходимым сертификатом. Нажмите кнопку **Установить сертификат** для установки сертификата в выбранное хранилище.

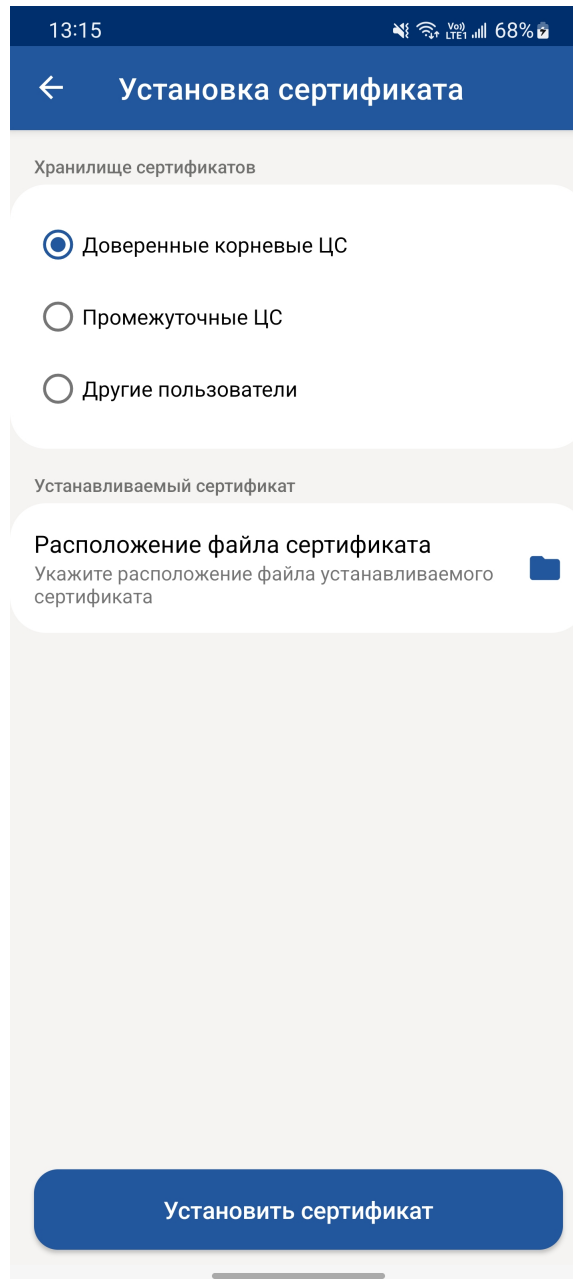



Рисунок 19. Установка сертификата в хранилище

2.5.3 Управление сертификатом

На вкладке **Сертификаты** у необходимого сертификата нажмите на кнопку . В открывшемся меню (см. [рис. 20](#)) доступны следующие действия с сертификатом:

- Поделиться сертификатом;
- Скачать сертификат;
- [Построение цепочки сертификатов](#);
- [Удаление сертификата](#).

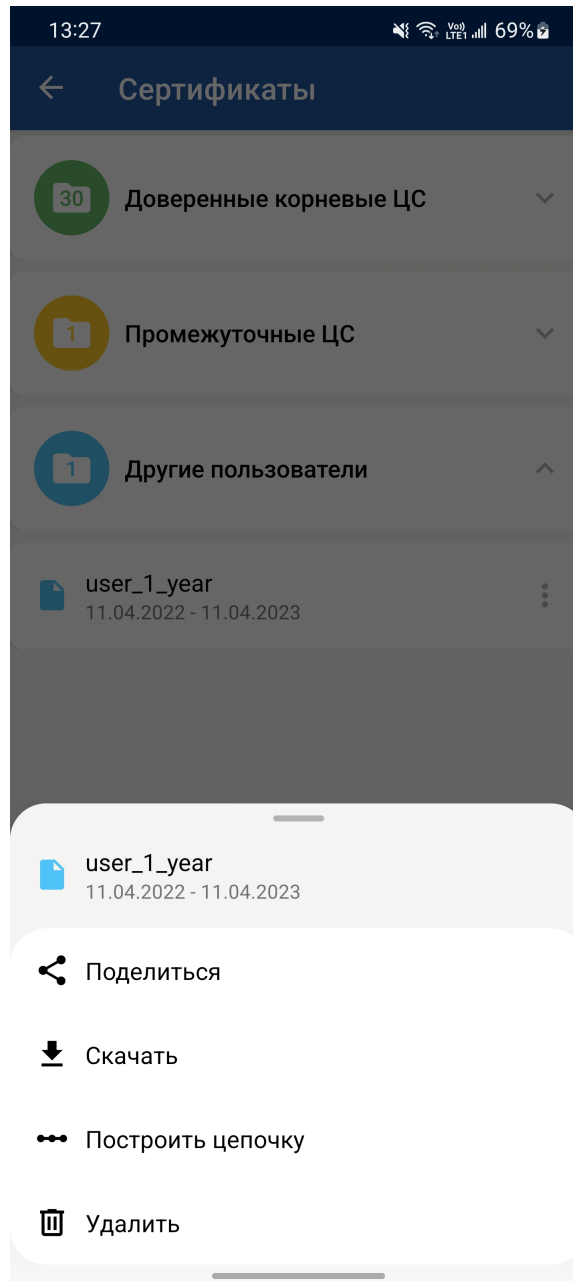




Рисунок 20. Управление сертификатом

2.5.4 Построение цепочки сертификатов

Для построения цепочки сертификатов на вкладке **Сертификаты** нажмите на кнопку  у необходимого сертификата, в открывшемся меню нажмите кнопку **Построить цепочку**. Откроется окно **Цепочка сертификатов** с построенной цепочкой (см. [рис. 13](#)).

2.5.5 Удаление сертификата

Для удаления сертификата на вкладке **Сертификаты** смахните справа налево необходимый сертификат или нажмите на кнопку  у необходимого сертификата, в открывшемся меню нажмите кнопку **Удалить**. После успешного удаления сертификата появится окно с результатом, содержащее кнопку **Отмена**, при нажатии на которую удаленный сертификат восстановится (см. [рис. 21](#)).

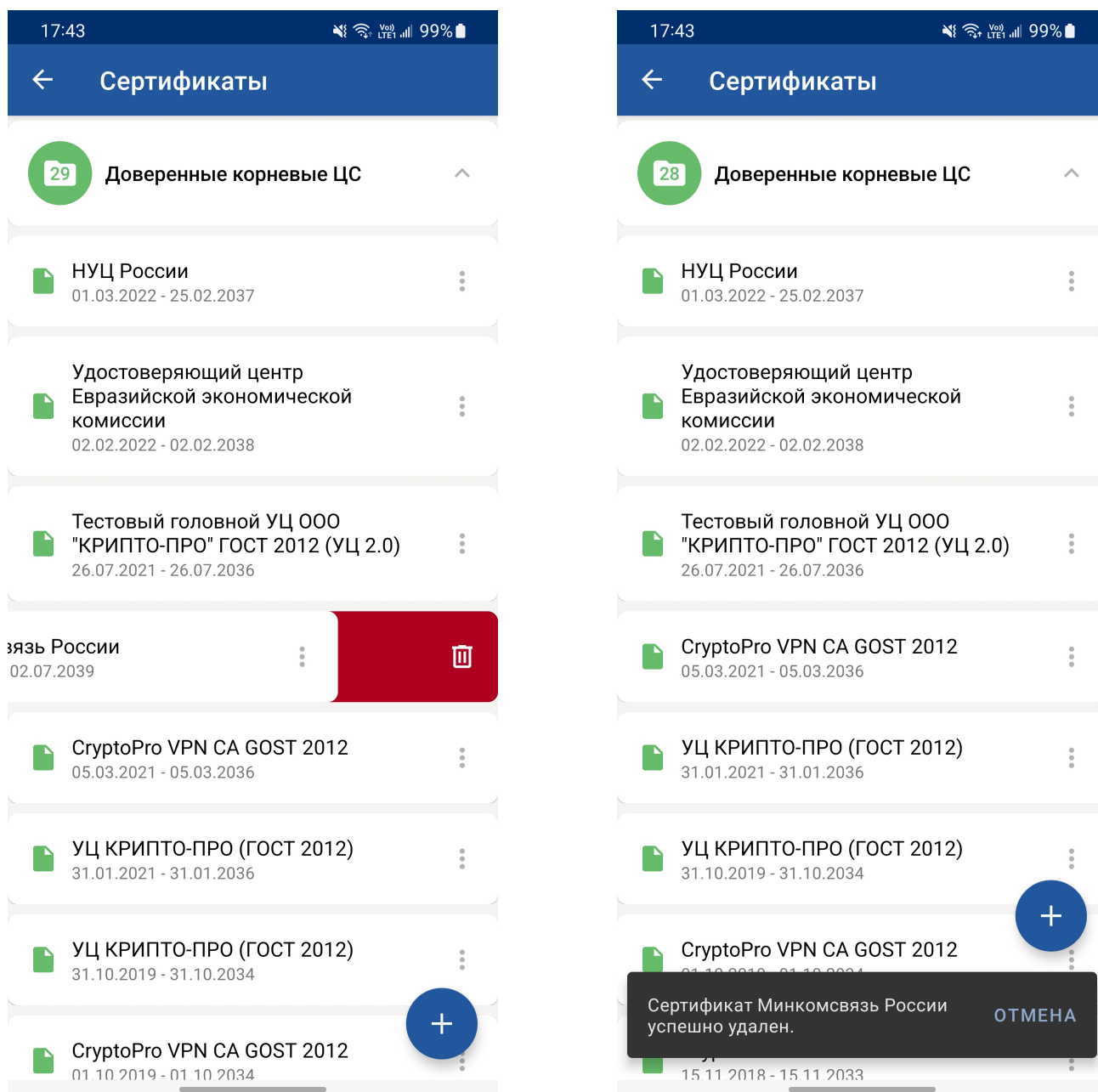


Рисунок 21. Удаление сертификата

2.6 Настройки

Вкладка **Настройки** позволяет управлять ключевыми носителями и установить необходимый уровень логирования событий криптопровайдера.

Для изменения отделяемого ключевого носителя или уровня журналирования установите переключатель напротив необходимого значения. После смены ключевого носителя требуется перезапуск приложения.

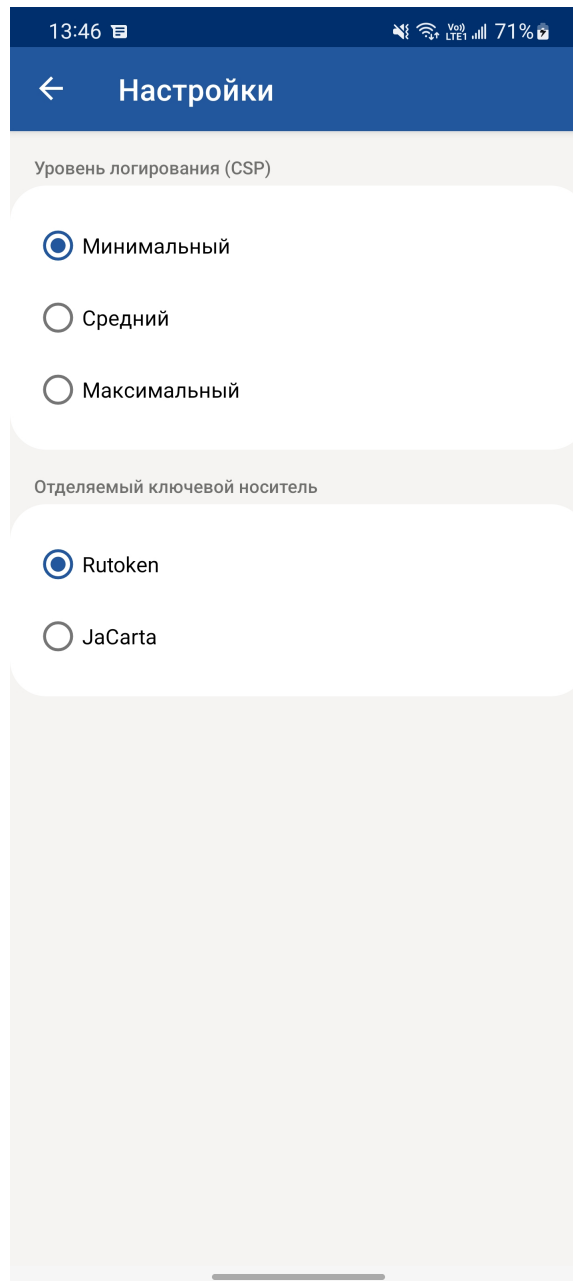


Рисунок 22. Вкладка **Настройки**