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 23

2021 г

Содержание

1 Инсталляция СКЗИ КриптоПро CSP

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

2 Интерфейс СКЗИ КриптоПро CSP

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

2.1 Доступ к контрольной панели СКЗИ

Панель настройки КриптоПро 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 КриптоПро CSP содержит вкладки **Лицензия** и **Целостность**.

Вкладка **Лицензия** предназначена для просмотра информации о версии установленного ПО СКЗИ КриптоПро 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**, **Ключевые носители** и **Настройки**. Чтобы открыть боковую панель, нажмите кнопку  или проведите вправо от левого края экрана.

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 **Ключевые носители** предназначена для управления доступными на устройстве ключевыми носителями.

Вкладка **Настройки** предназначена для управления журналированием в СКЗИ.

2.2 Ввод серийного номера лицензии

При установке программного обеспечения КриптоПро 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 КриптоПро CSP 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 нажмите кнопку  на вкладке **Лицензия**. В открывшемся диалоговом окне введите номер лицензии и нажмите кнопку **OK** (см. рис. 1).

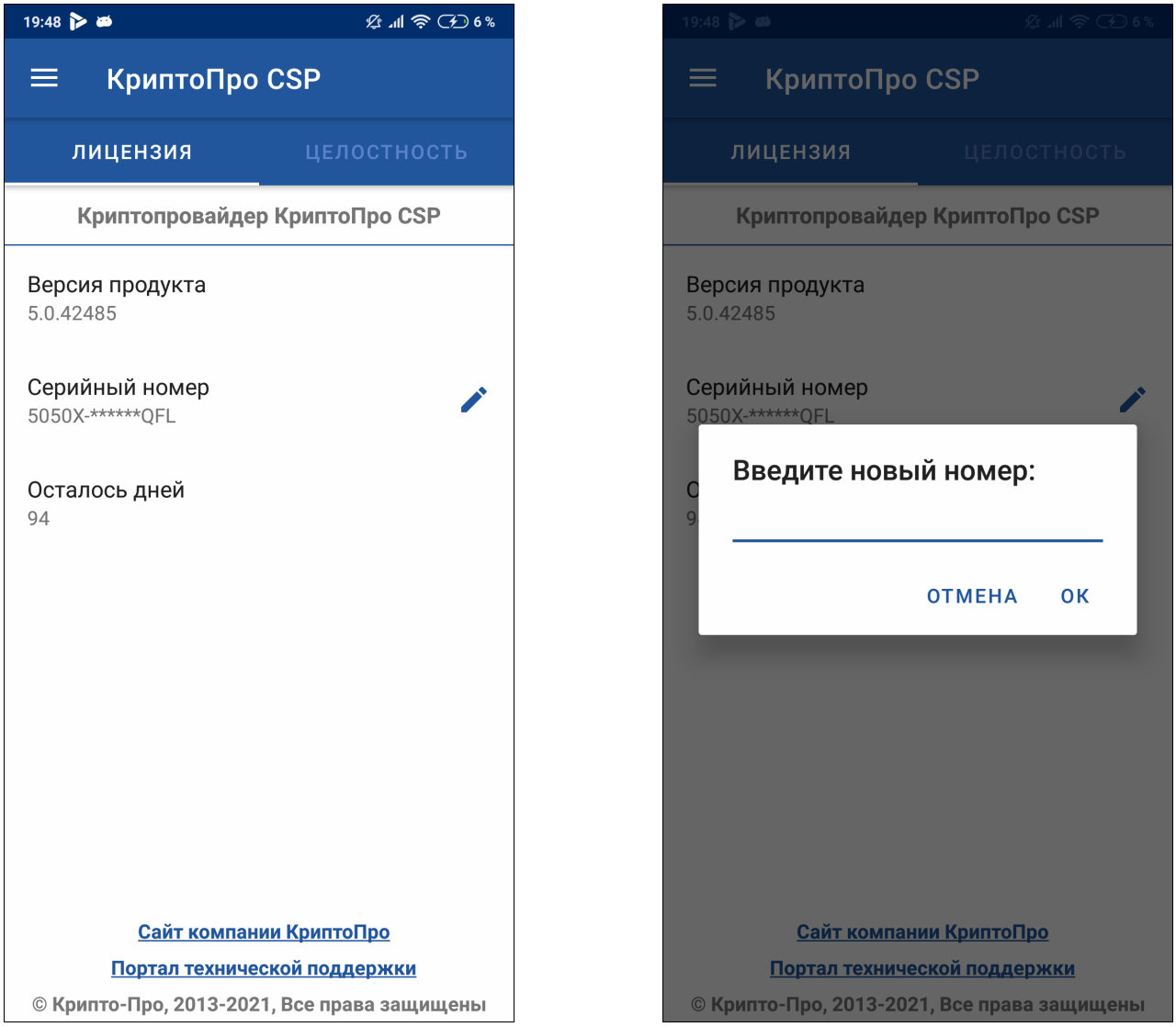

Рисунок 1. Ввод серийного номера лицензии

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

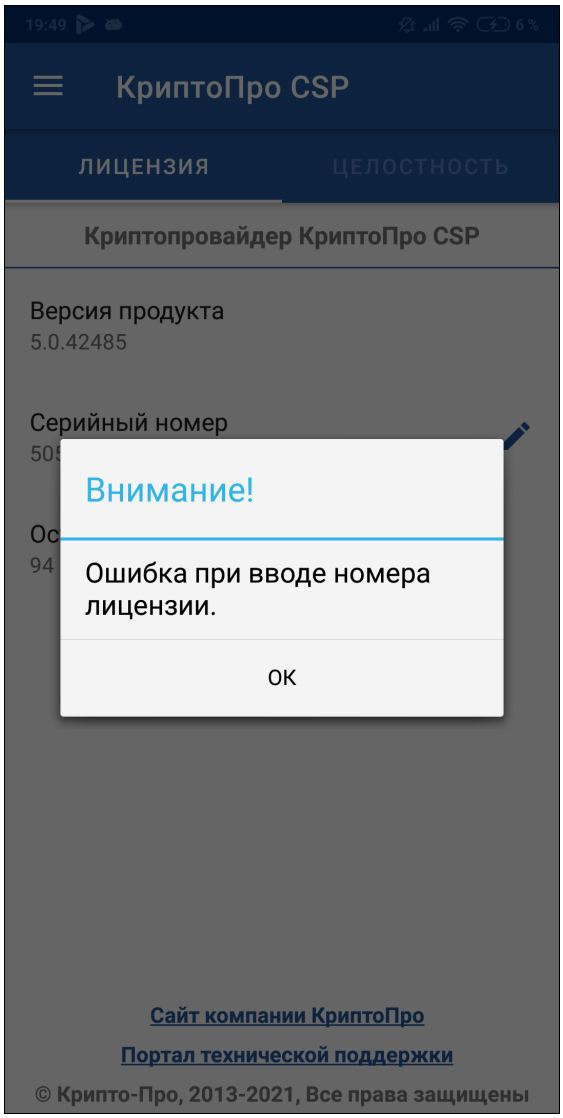

Рисунок 2. Ошибка при вводе некорректного номера лицензии

2.3 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 .

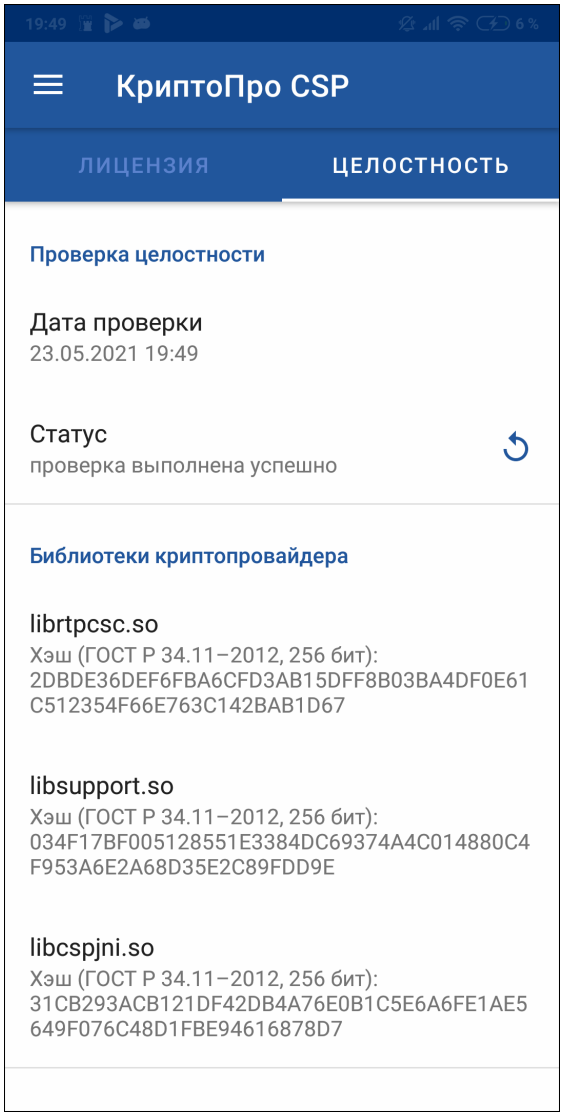

Рисунок 3. Вкладка **Целостность**

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. Для быстрого поиска необходимого контейнера воспользуйтесь кнопкой  .

2.4.1 Создание ключевого контейнера

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

Откроется окно «Создание ключевого 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 **Сертификат** и заполните сведения о сертификате (см. рис. 5). Нажмите кнопку для создания контейнера с указанными параметрами.

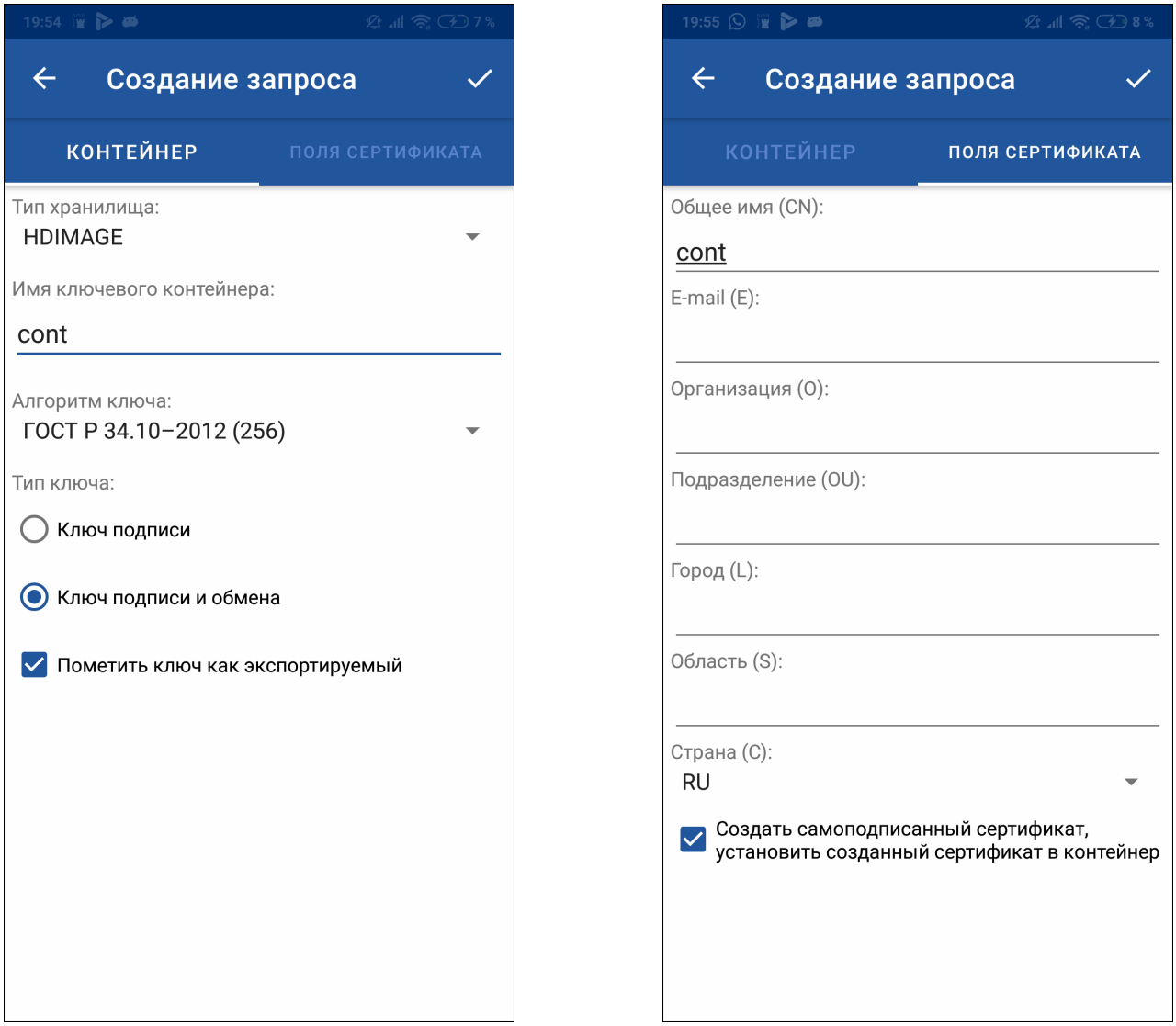

Рисунок 5. Создание ключевого контейнера

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 **OK**. Созданный контейнер появится в списке доступных контейнеров в окне **Ключевые контейнеры**.

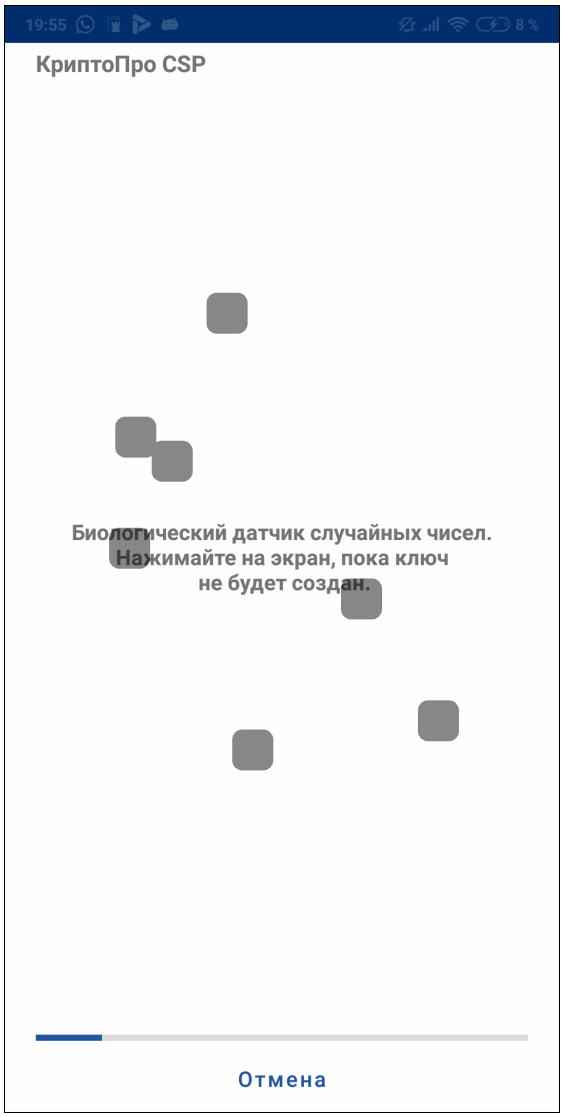

Рисунок 6. Окно биологического ДСЧ

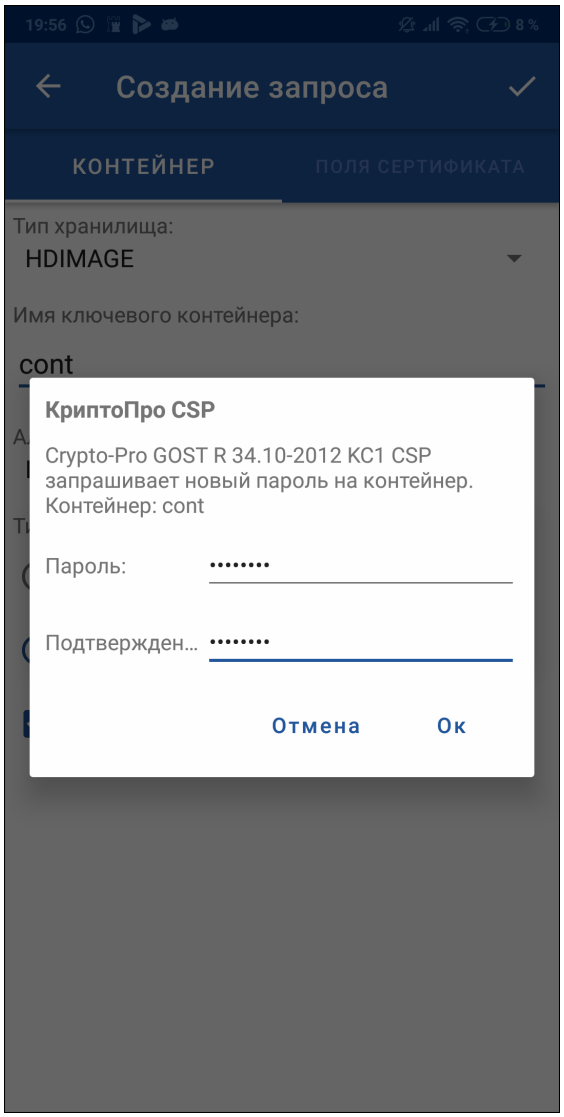

Рисунок 7. Установка пин-кода на доступ к ключу

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). Выберите длительным нажатием в проводнике конечную папку с ключевым контейнером. Нажмите кнопку для подтверждения выбора.

2.4.3 Управление контейнером

На вкладке **Ключевые контейнеры** нажмите на имя контейнера. В открывшемся окне «Управление контейнером» (см. рис. 8) 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;

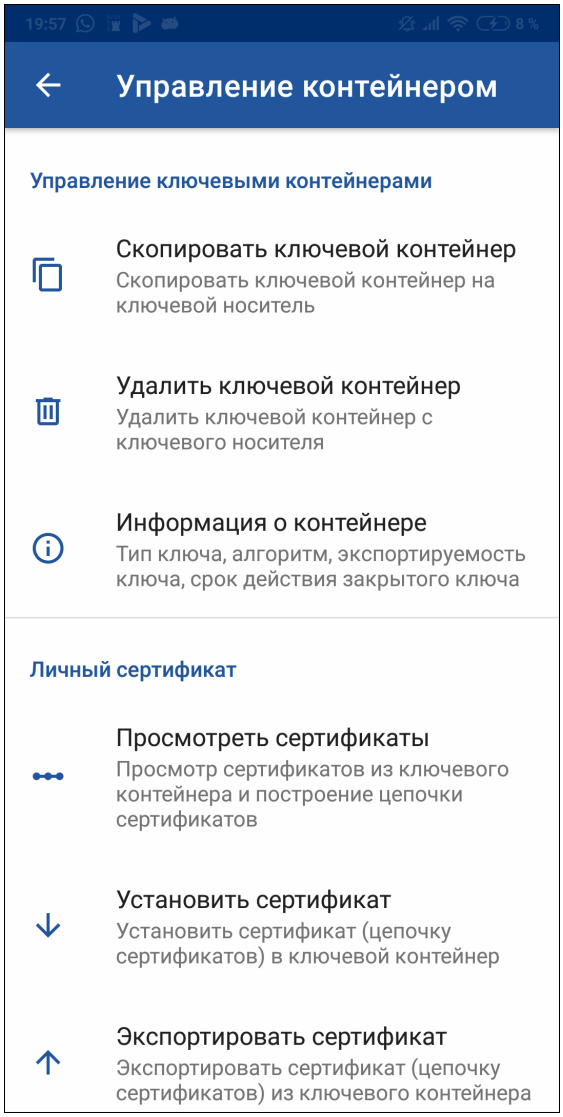

Рисунок 8. Управление контейнером

2.4.4 Копирование ключевого контейнера

Для копирования ключевого контейнера на вкладке **Ключевые контейнеры** нажмите на необходимый контейнер, в открывшемся окне «Управление контейнером» нажмите кнопку **Скопировать ключевой контейнер**. Откроется окно «Копирование контейнера» (см. рис. 9).

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

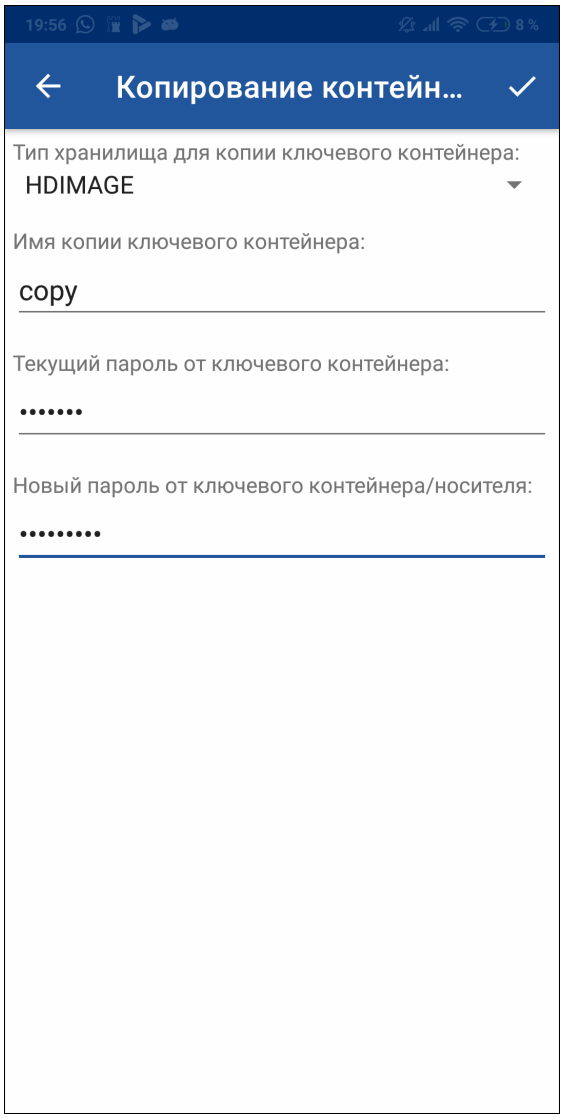

Рисунок 9. Копирование ключевого контейнера

2.4.5 Удаление ключевого контейнера

Для удаления ключевого контейнера на вкладке **Ключевые контейнеры** нажмите на необходимый контейнер, в открывшемся окне «Управление контейнером» нажмите кнопку **Удалить ключевой контейнер**. Откроется окно подтверждения удаления контейнера, нажмите кнопку **OK** (см. рис. 10).

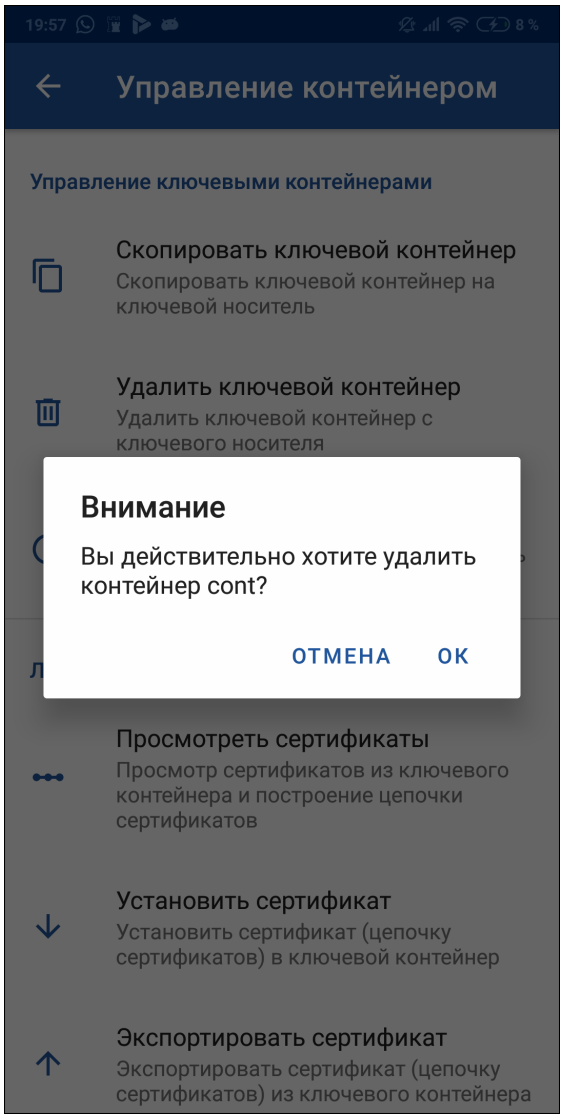

Рисунок 10. Удаление ключевого контейнера

2.4.6 Просмотр информации о ключевом контейнере

Для просмотра информации о контейнере (наличие сертификата контейнере, алгоритм, длина и срок действия ключа, признак экспортности ключа) на вкладке **Ключевые контейнеры** нажмите на необходимый контейнер, в открывшемся окне «Управление контейнером» нажмите кнопку **Информация о контейнере**. Если на доступ к контейнеру установлен пин-код, то он будет запрошен. Введите пин-код и нажмите кнопку **OK**.

Откроется окно «Информация о контейнере» (см. рис. 11).

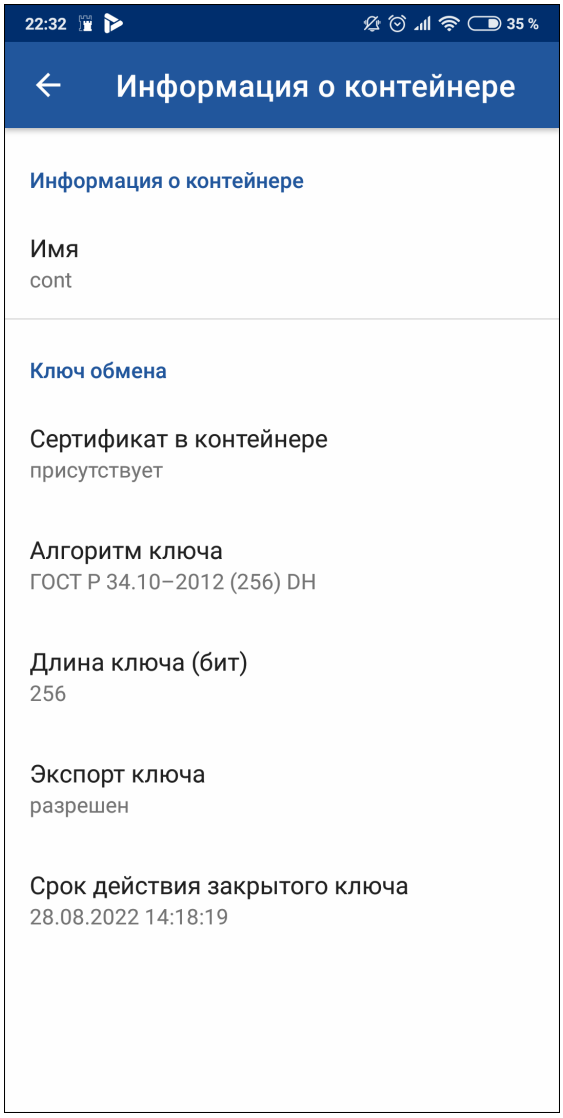

Рисунок 11. Просмотр информации о ключевом контейнере

2.4.7 Просмотр сертификата из ключевого контейнера

Для просмотра информации о сертификате, установленном в ключевом контейнере, на вкладке **Ключевые контейнеры** нажмите на необходимый контейнер, в открывшемся окне «Управление контейнером» нажмите кнопку **Просмотреть сертификат**.

Откроется окно «Просмотр сертификатов» (см. рис. 12). Нажмите кнопку **Свойства**, чтобы увидеть расширенный свойства сертификата (сроки действия, алгоритм ключа, описание полей).

Чтобы построить цепочку сертификатов, нажмите кнопку  . Откроется окно **Цепочка сертификатов** с информацией о сертификате и построенной цепочке.

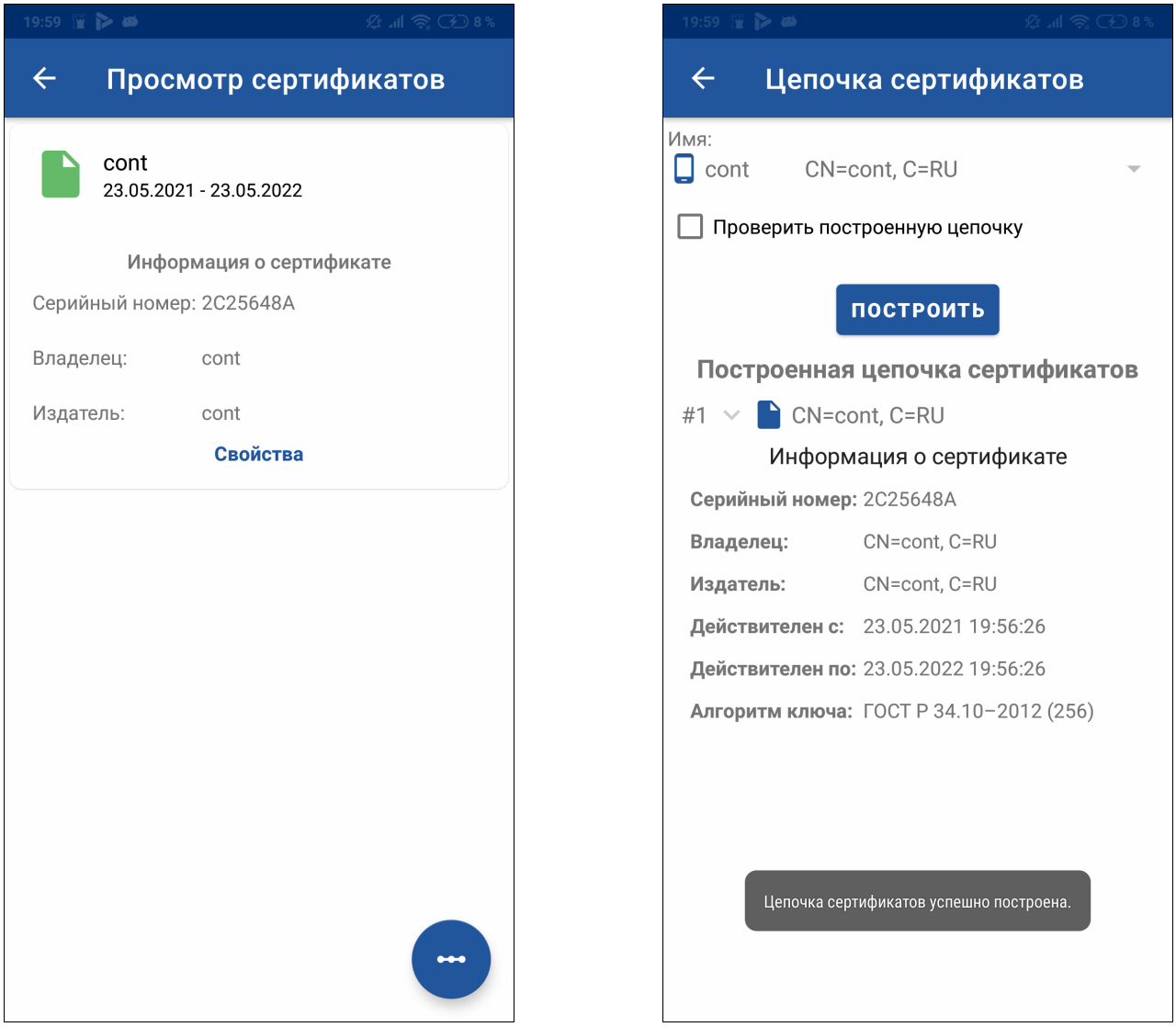

Рисунок 12. Просмотр сертификата (цепочки сертификатов) из ключевого контейнера

2.4.8 Установка сертификата в ключевой контейнер

Чтобы установить сертификат или цепочку сертификатов в контейнер, на вкладке **Ключевые контейнеры** нажмите на необходимый контейнер, в открывшемся окне «Управление контейнером» нажмите кнопку **Установить сертификат**.

Откроется окно «Установка сертификата» (см. рис. 13). Нажмите кнопку **Расположение файла сертификата** и выберите в проводнике файл с необходимым сертификатом (.cert, .crt) или цепочкой (.p7b). Нажмите кнопку  для подтверждения выбора, а затем  для установки выбранного сертификата/цепочки в контейнер.

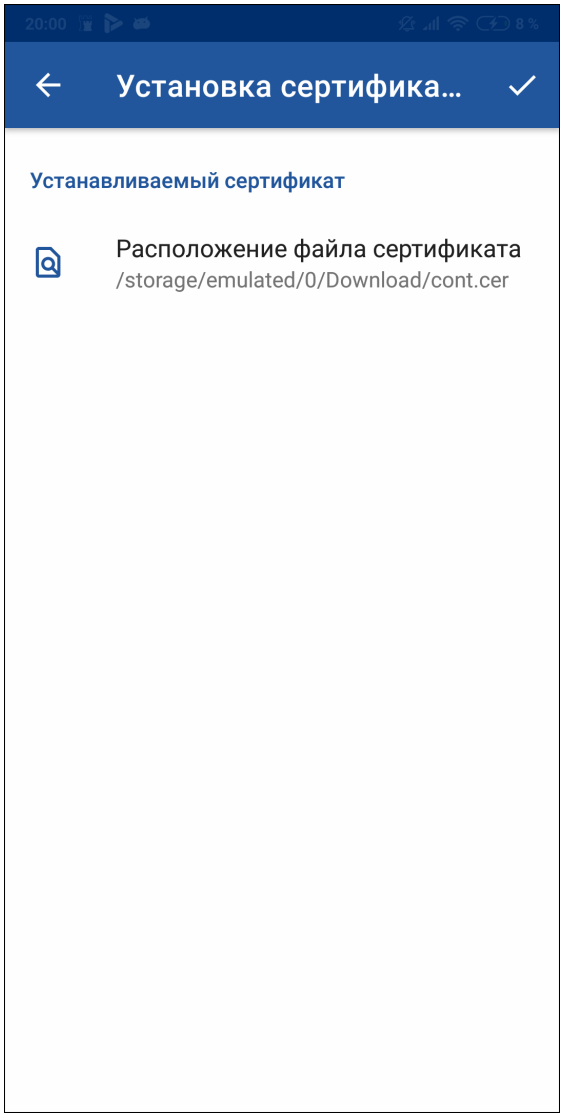

Рисунок 13. Установка сертификата в ключевой контейнер

2.4.9 Экспорт сертификата из ключевого контейнера

Чтобы экспортировать сертификат или цепочку сертификатов из ключевого контейнера, на вкладке **Ключевые контейнеры** нажмите на необходимый контейнер, в открывшемся окне «Управление контейнером» нажмите кнопку **Экспортировать сертификат**.

Откроется окно «Экспорт сертификата» (см. рис. 14). Нажмите кнопку **Расположение файла сертификата** и выберите длительным нажатием в проводнике конечную папку, в которую необходимо экспортировать сертификат или цепочку. Нажмите кнопку  для подтверждения выбора. Установите переключатель в соответствующее поле для выбора объекта экпорта — сертификат или цепочка сертификатов. Нажмите кнопку  для экспорта сертификата или цепочки в указанную папку.

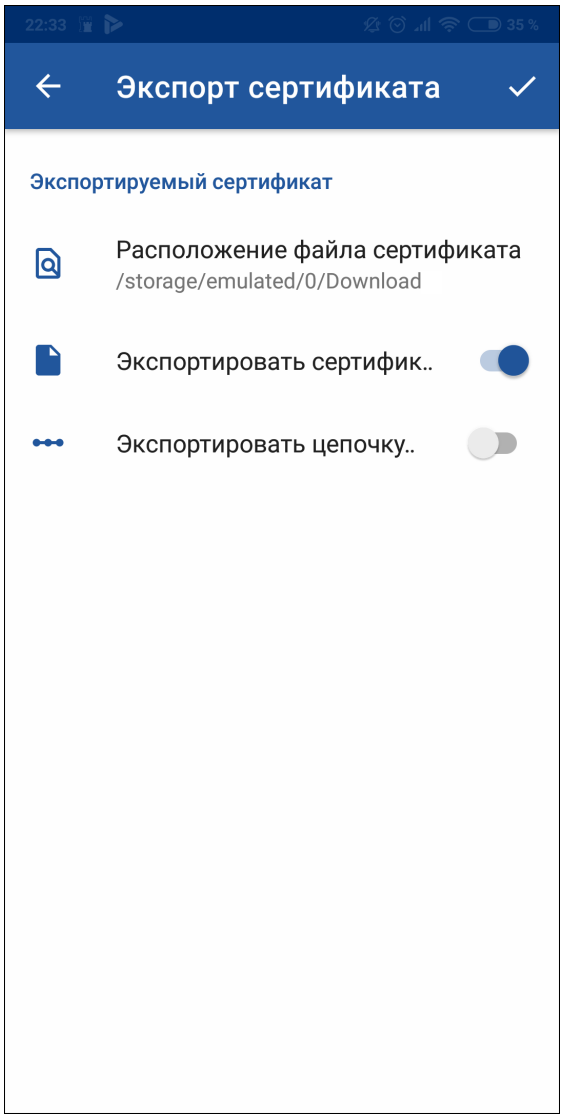

Рисунок 14. Экспорт сертификата из ключевого контейнера

2.4.10 Изменение пароля ключевого контейнера

Для изменения пароля ключевого контейнера на вкладке **Ключевые контейнеры** нажмите на необходимый контейнер, в открывшемся окне «Управление контейнером» нажмите кнопку **Изменить пароль**.

Откроется окно «Изменение пароля» (см. рис. 15). Введите текущий и новый пароли контейнера в соответствующие поля и нажмите кнопку  .

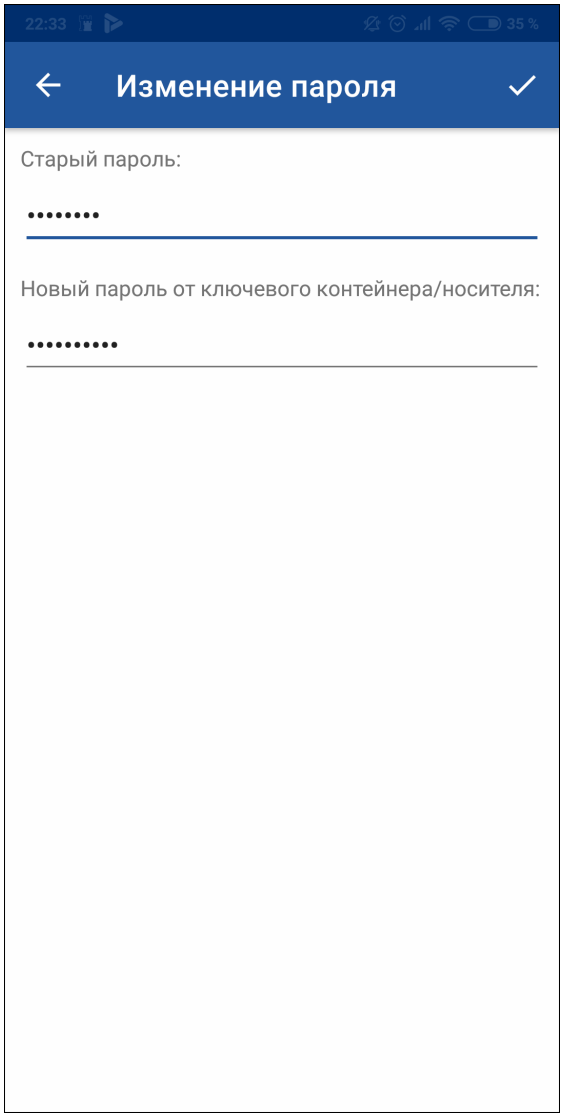

Рисунок 15. Изменение пароля ключевого контейнера

2.5 Операции с сертификатами

Вкладка **Сертификаты** содержит информацию о сертификатах, упорядоченных по 3 хранилищам: Доверенные корневые ЦС, Промежуточные ЦС и Другие пользователи.

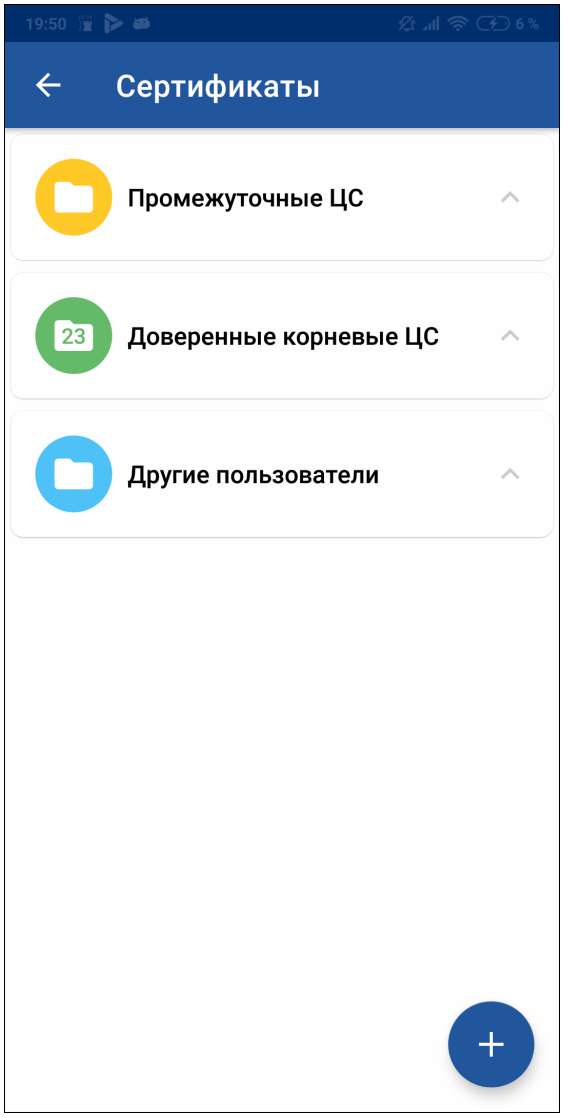

Рисунок 16. Вкладка **Сертификаты**

2.5.1 Просмотр информации о сертификате

Для просмотра краткой информации о сертификате нажмите на сертификат. Чтобы увидеть все свойства сертификата, нажмите на кнопку **Свойства** (см. рис. 17).

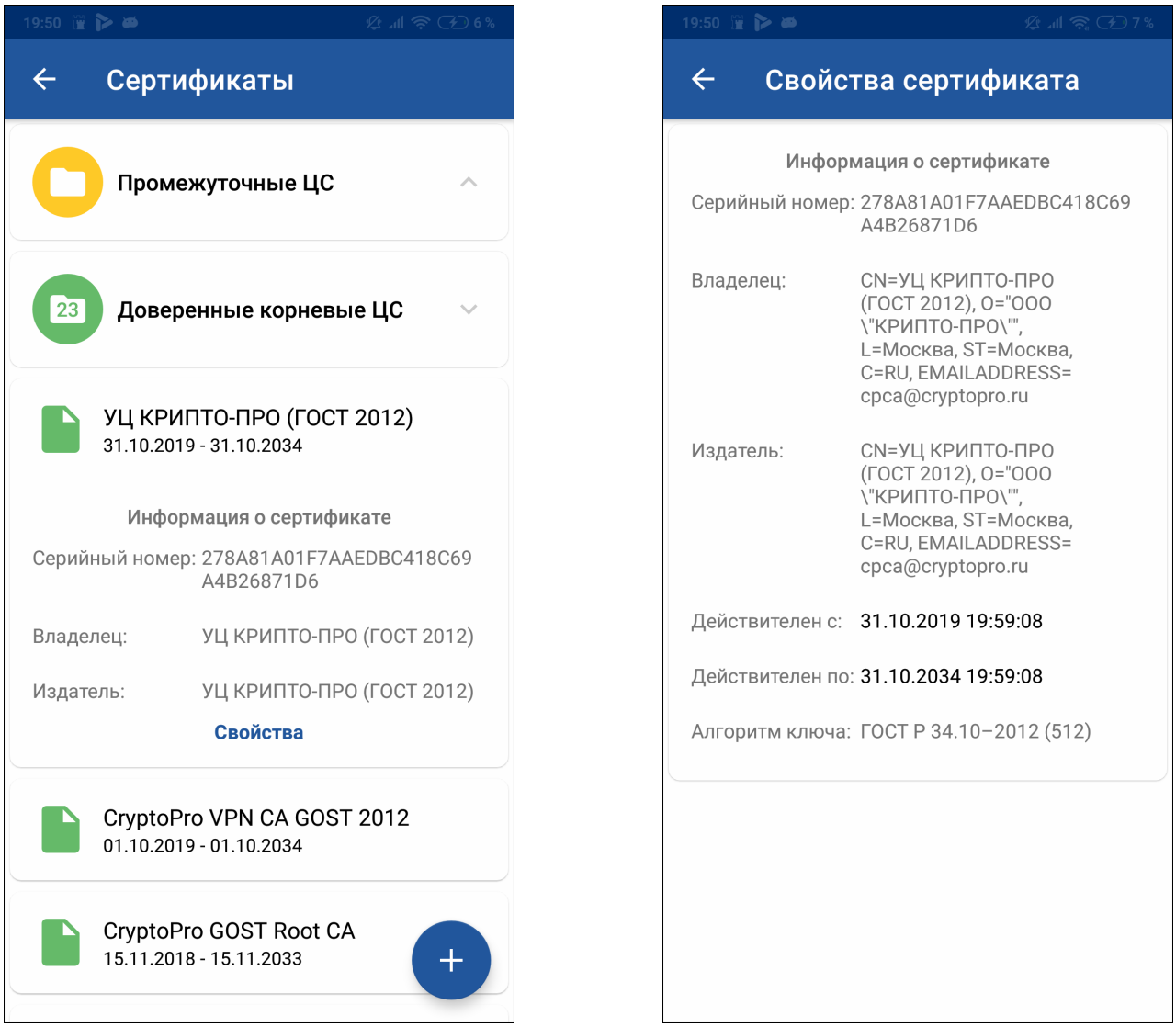

Рисунок 17. Свойства сертификата

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. 18). 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 ✓ для установки сертификата в выбранное хранилище.

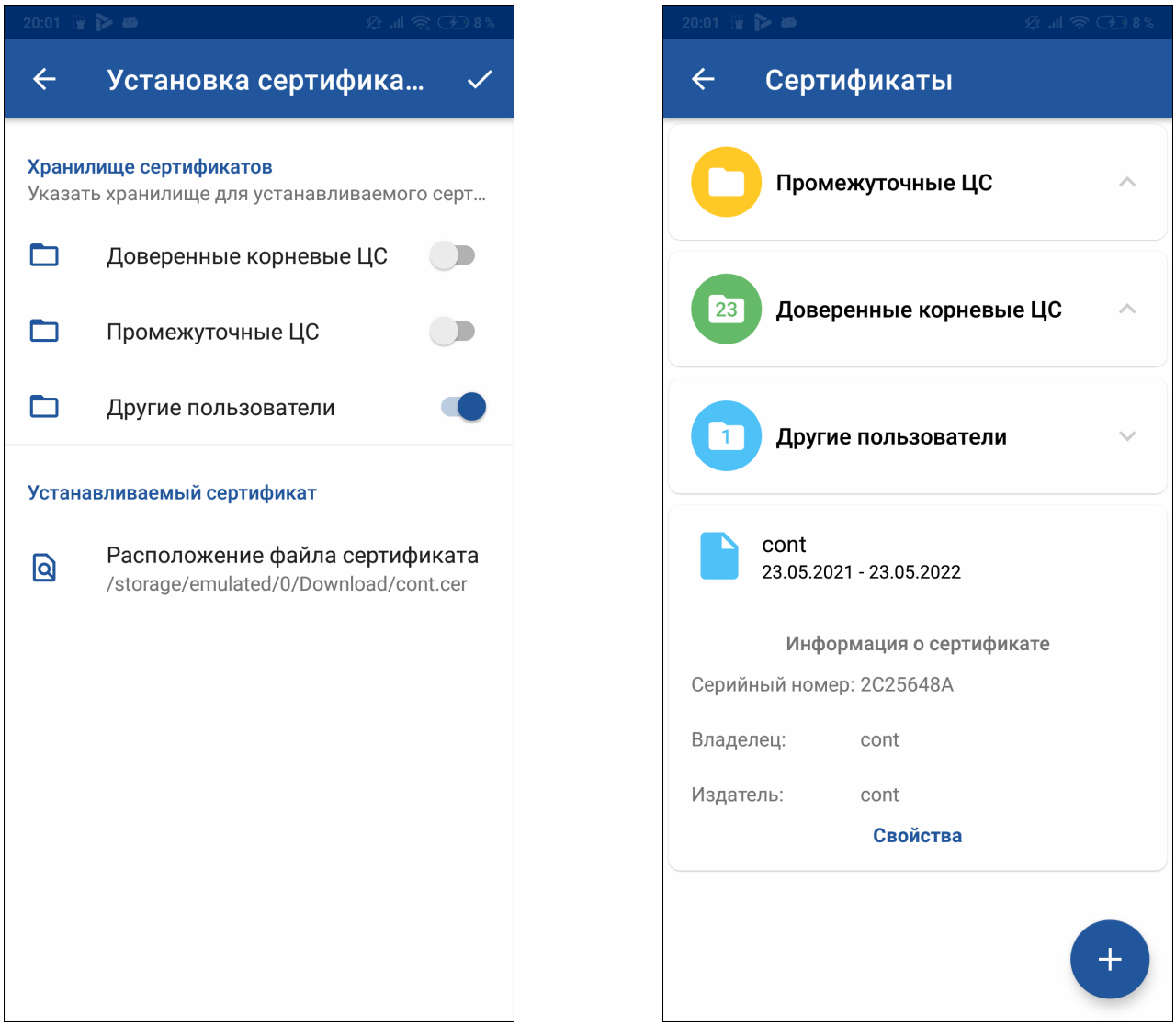

Рисунок 18. Установка сертификата в хранилище

2.6 Ключевые носители

Управление ключевыми носителями осуществляется с помощью вкладки **Ключевые носители**.

Чтобы выбрать отделяемый ключевой носитель, нажмите кнопку **Текущий отделяемый ключевой носитель** и выберите необходимый носитель в окне. Для каждого семейства ключевых носителей возможно выбрать несколько типов носителей, с которыми будет осуществляться работа, установив галочку напротив необходимых.

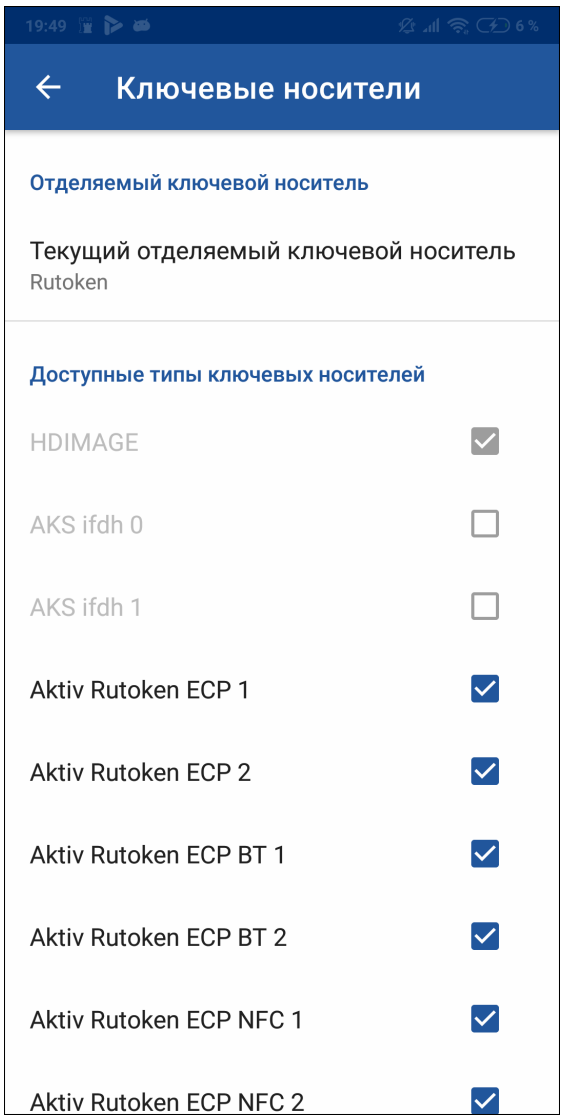

Рисунок 19. Вкладка **Ключевые носители**

2.7 Управление журналированием

Вкладка **Настройки** СКЗИ позволяет установить необходимый уровень логирования событий криптопровайдера.

Для изменения уровня журналирования установите переключатель напротив необходимого значения.

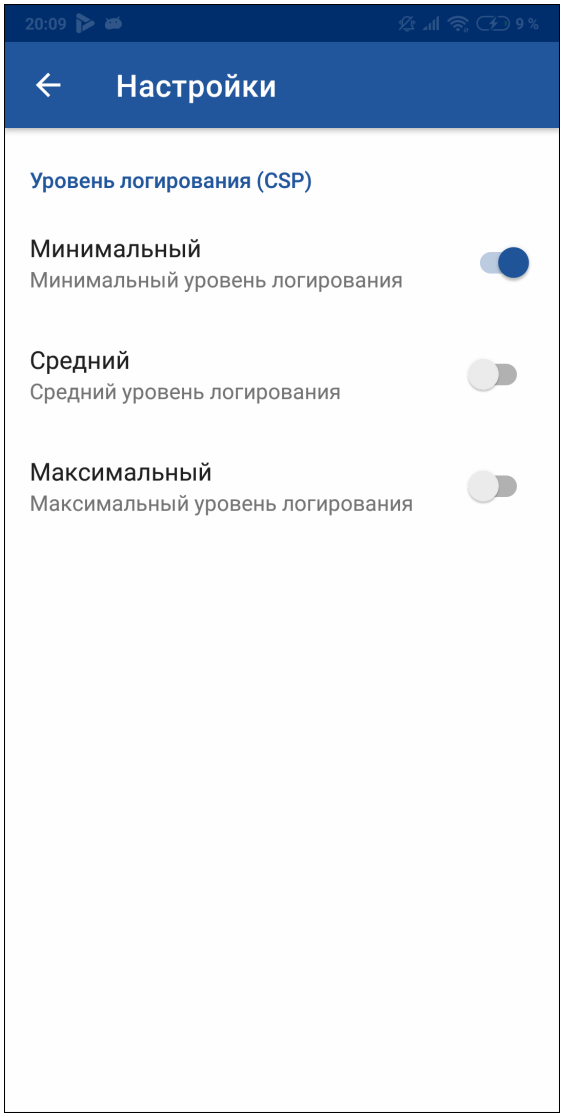

Рисунок 20. Вкладка **Настройки**