Цифровые технологии

КриптоАРМ ГОСТ для iOS · Архив

Документация продукта

Релиз Архивное руководство

Исходная документация на CryptoARM.ru

Редакция от 25.11.2026

Правообладатель и разработчик
ООО «Цифровые технологии»

Содержание

Архив 4

Исходные оглавления

- Содержание 5
- Содержание раздела 7
- Мастер подписи и шифрования 8

Общие сведения

- Установка приложения КриптоАРМ ГОСТ 9
- Графический пользовательский интерфейс приложения 10
- Контакты 16
- Управление сертификатами 20
- Операции над сертификатами 22
- Импорт сертификата из файла 26
- Создание запроса на сертификат 30
- Получение сертификата DSS 35
- Получение сертификата из УЦ 40
- Управление контейнерами 49
- Списки отзыва сертификатов (COC) 53

Работа с программой

- Управление списком файлов для выполнения операций 57
- Параметры операций 60
- Создание электронной подписи 67
- Результаты операций 70
- Проверка электронной подписи 72
- Добавление подписи 75
- Снятие электронной подписи 79
- Подпись сертификатом DSS 83
- Шифрование файлов 86
- Расшифрование файлов 88
- Подпись и шифрование 91
- Шифрование и архивирование 93
- Подпись, шифрование и архивирование 95

Расшифрование и разархивирование файлов 97
Расшифрование и снятие подписи 99
Расшифрование, разархивирование и снятие подписи 101
Документы 103
Лицензии 105
Журнал операций 107
Подключение Рутокен 110

Открыть статью на сайте

КриптоАРМ ГОСТ для iOS

Архивное руководство.

- Содержание
- Содержание раздела
- Мастер подписи и шифрования

Открыть статью на сайте

Содержание

Архив. КриптоАРМ ГОСТ для iOS.

Общие сведения

- Установка приложения КриптоАРМ ГОСТ
- Графический пользовательский интерфейс приложения
- Контакты

Сертификаты

- Управление сертификатами
- Операции над сертификатами
- Импорт сертификата из файла
- Создание запроса на сертификат
- Получение сертификата DSS
- Получение сертификата из УЦ
- Управление контейнерами
- Списки отзыва сертификатов (COC)

Работа с программой

- Управление списком файлов для выполнения операций
- Параметры операций
- Создание электронной подписи
- Результаты операций
- Проверка электронной подписи
- Добавление подписи
- Снятие электронной подписи
- Подпись сертификатом DSS
- Шифрование файлов
- Расшифрование файлов

Прямые групповые операции (подпись, архивирование, шифрование)

- Подпись и шифрование
- Шифрование и архивирование
- Подпись, шифрование и архивирование

Обратные групповые операции (расшифрование, разархивирование, снятие подписи)

- Расшифрование и разархивирование файлов
- Расшифрование и снятие подписи
- Расшифрование, разархивирование и снятие подписи

- Документы
- Лицензии
- Журнал операций
- Подключение Рутокен

Открыть статью на сайте

Содержание раздела

Архив. КриптоАРМ ГОСТ для iOS.

Общие сведения

- Установка приложения КриптоАРМ ГОСТ
- Графический пользовательский интерфейс приложения
- Контакты

Сертификаты

- Управление сертификатами
- Операции над сертификатами
- Импорт сертификата из файла
- Создание запроса на сертификат
- Получение сертификата DSS
- Получение сертификата из УЦ
- Управление контейнерами
- Списки отзыва сертификатов (COC)

Открыть статью на сайте

Мастер подписи и шифрования

Архив. КриптоАРМ ГОСТ для iOS.

Работа с программой

- Управление списком файлов для выполнения операций
- Параметры операций
- Создание электронной подписи
- Результаты операций
- Проверка электронной подписи
- Добавление подписи
- Снятие электронной подписи
- Подпись сертификатом DSS
- Шифрование файлов
- Расшифрование файлов

Прямые групповые операции (подпись, архивирование, шифрование)

- Подпись и шифрование
- Шифрование и архивирование
- Подпись, шифрование и архивирование

Обратные групповые операции (расшифрование, разархивирование, снятие подписи)

- Расшифрование и разархивирование файлов
- Расшифрование и снятие подписи
- Расшифрование, разархивирование и снятие подписи

- Документы
- Лицензии
- Журнал операций
- Подключение Рутокен

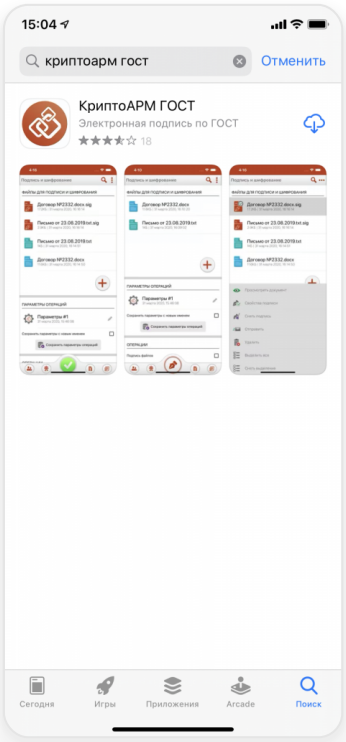
Открыть статью на сайте

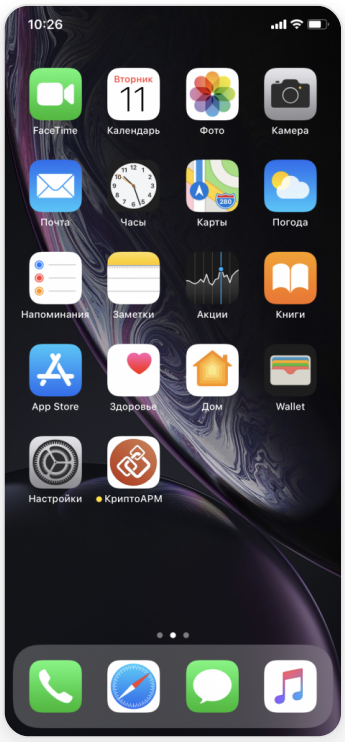
Установка приложения КриптоАРМ ГОСТ

Архив. КриптоАРМ ГОСТ для iOS.

Инсталляция, деинсталляция и обновление средства криптографической защиты информации КриптоПро CSP версии 5.0 R2 Исполнение 1-КриптоАРМ (далее — КриптоАРМ ГОСТ) происходит через магазин приложений «App Store» .

Для этого необходимо найти приложение в магазине и установить.





Открыть статью на сайте

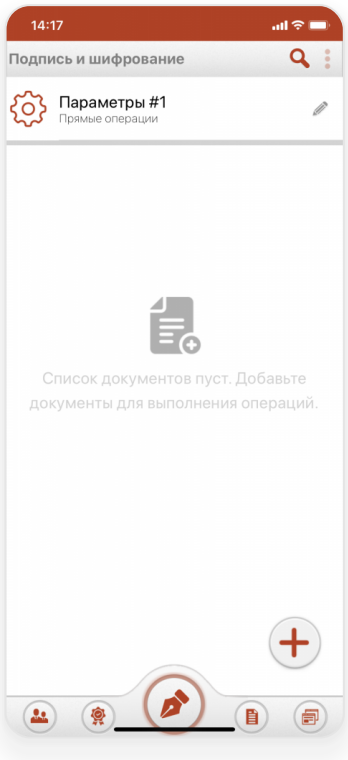
Графический пользовательский интерфейс приложения

Архив. КриптоАРМ ГОСТ для iOS.

Начало работы с КриптоАРМ ГОСТ

Работа с приложением КриптоАРМ ГОСТ начинается со страницы мастера **Подпись и шифрование.**

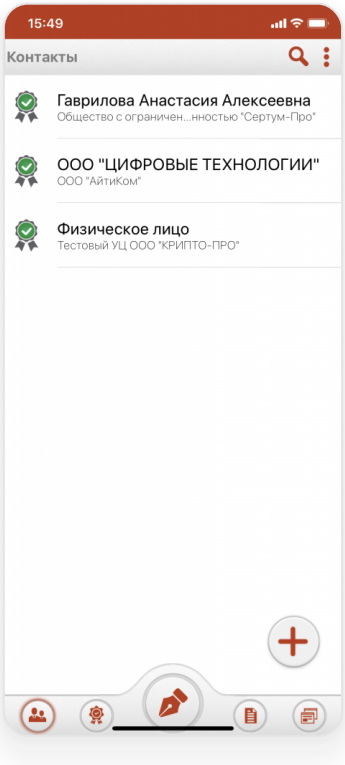
На рисунке отображена центральная рабочая часть окна, которая предназначена для добавления и управления списком файлов.



В верхней части располагается название раздела, функция поиска файлов и контекстное меню. Следующий блок – **Параметры операций** и в конце находится меню-панель с разделами и кнопкой **Выполнить**.

Контакты

Переход в список контактов происходит при выборе пункта меню Контакты .



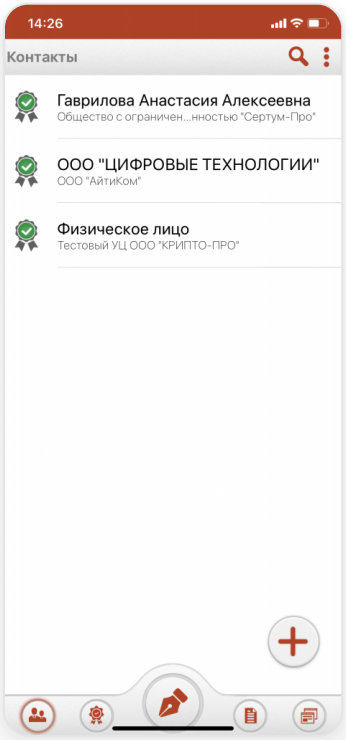
В разделе **Контакты** представлены сертификаты других пользователей, в адрес которых происходит шифрование документов.

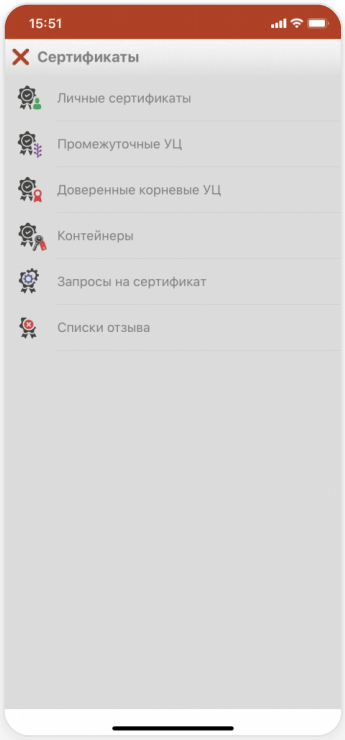
В верхней части располагается название раздела, функция поиска файлов и контекстное меню.

Личные сертификаты

Переход в список личных сертификатов происходит при выборе пункта меню **Сертификаты** .

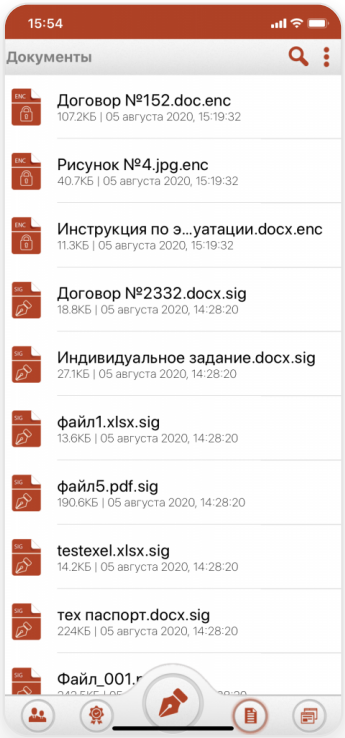
В верхней части располагается бургер-меню  с дополнительными разделами, название раздела, функция поиска файлов и контекстное меню.





Документы

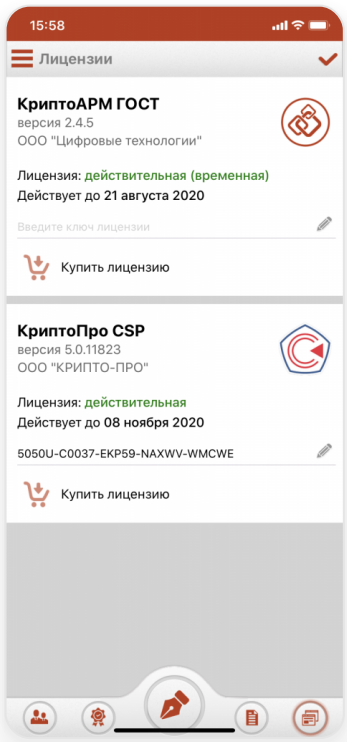
По нажатию на кнопку  открывается раздел **Документы.**

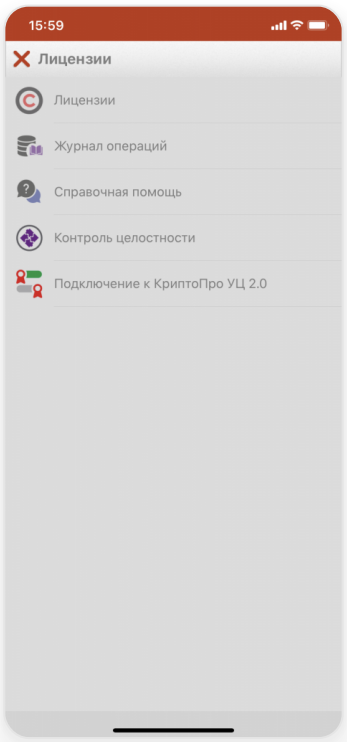


Лицензии

Переход в раздел **Лицензии** происходит при выборе пункта меню .

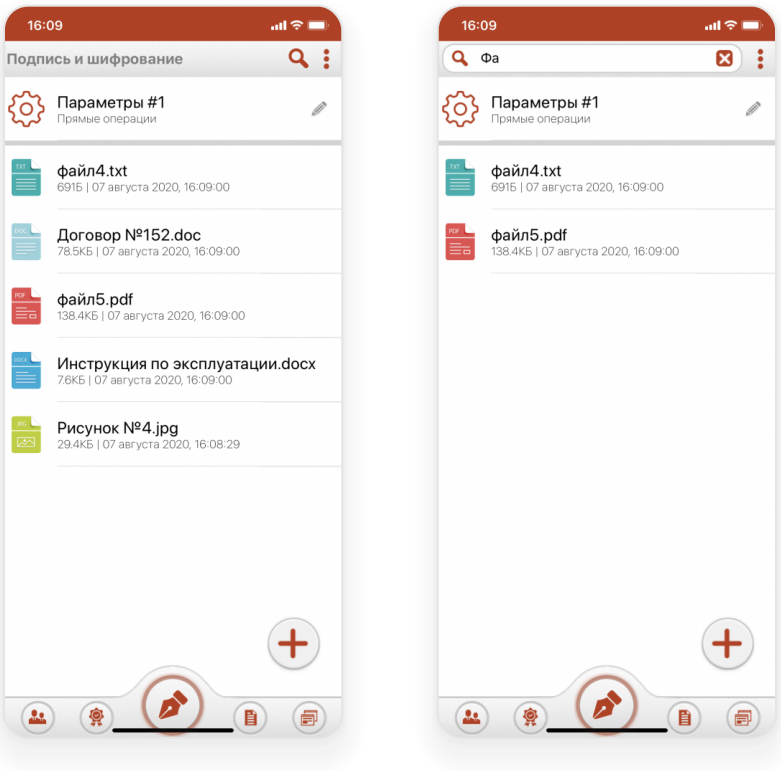
В верхней части располагается бургер-меню  с дополнительными разделами, название раздела, функция поиска файлов и контекстное меню.





Поиск в приложении

В элементах пользовательского интерфейса реализована функция поиска файлов. Для включения режима поиска нужно нажать на кнопку **Поиск**  и в строке поиска ввести ключевую фразу.



Поиск файлов реализован на основе совпадения ключевой фразы с названием файла. В результате вместо полного списка в окне остаются только файлы, удовлетворяющие критерию поиска.

Чтобы отменить фильтр поиска требуется удалить ключевую фразу или нажать на кнопку **Отмена** .

Примечание: В случае, неправильно указанного критерия поиска, список файлов может оказаться пустым, о чем будет свидетельствовать надпись «Ничего не найдено».

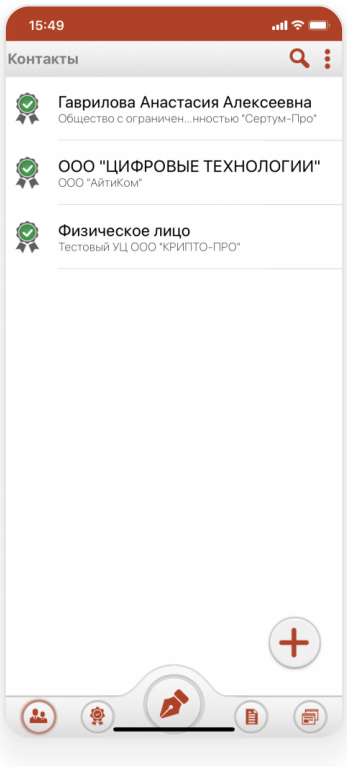
Открыть статью на сайте

Контакты

Архив. КриптоАРМ ГОСТ для iOS.

В разделе **Контакты** представлены сертификаты других пользователей, в адрес которых происходит шифрование документов.

Переход в список контактов происходит при выборе пункта меню **Контакты** .



Контакты можно импортировать, просматривать, экспортировать и удалять. Так же для списка контактов работает поиск.

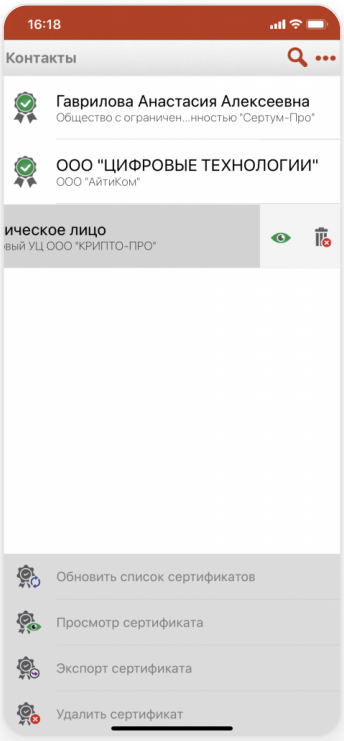
Импорт нового контакта

Импорт нового контакта выполняется кнопкой добавления .

Из хранилища нужно выбрать файл сертификата с расширением **.cer** или **.crt**. При успешном выполнении операции импорта контакт появляется в списке.

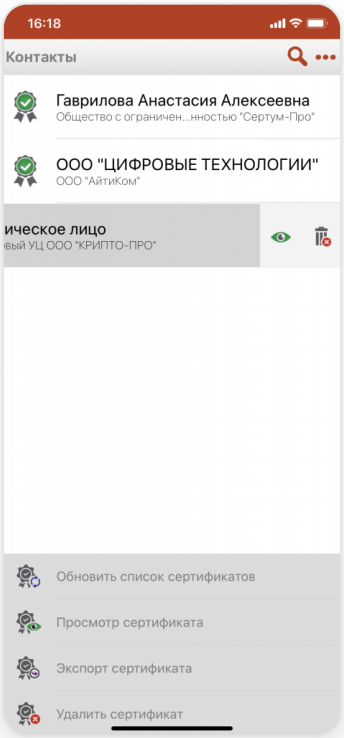
Просмотр свойств контакта

Для просмотра свойств контакта необходимо выбрать пункт **Просмотр сертификата** при свайпе влево или через контекстное меню операций .

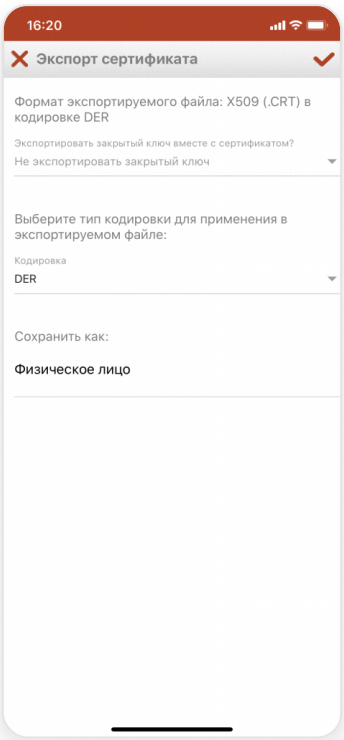


Экспорт контакта в файл

Для экспорта контакта в меню операций необходимо выбрать пункт **Экспорт сертификата**.

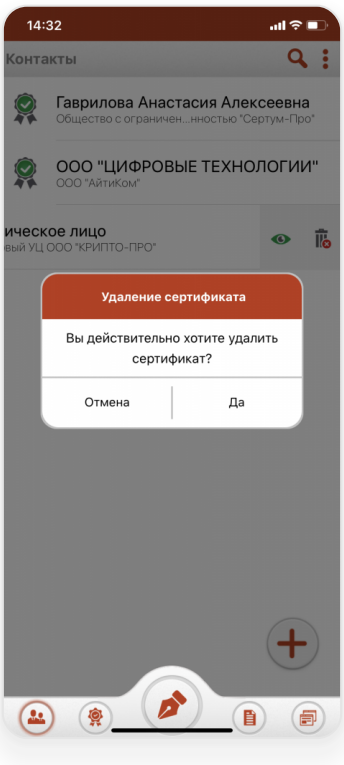


При экспорте появляется представление, в котором нужно выбрать кодировку (BASE-64 или DER) и задать имя сертификата (по умолчанию задается текущее имя сертификата). Имя сертификата указывается обязательно.



Удаление контакта

Для удаления контакта при свайпе влево или в меню операций необходимо выбрать пункт **Удалить сертификат**. При подтверждении операции контакт удалится из списка.



Открыть статью на сайте

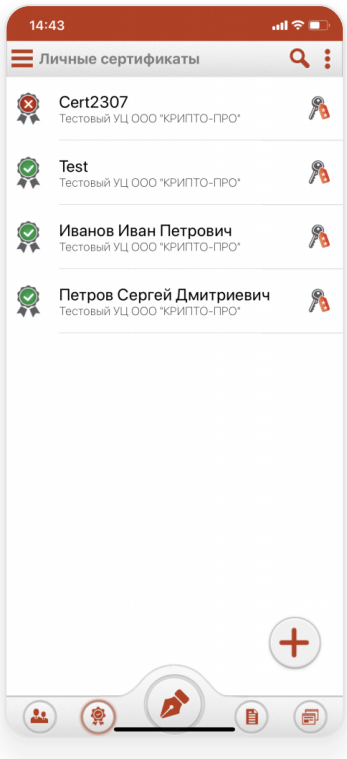
Управление сертификатами

Архив. КриптоАРМ ГОСТ для iOS.

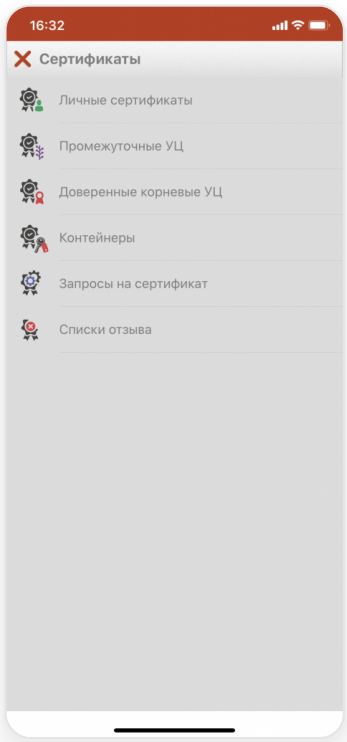
Для управления сертификатами в приложении добавлен отдельный пункт меню **Сертификаты** .

При выборе данного пункта открывается список личных сертификатов. При отображении сертификатов, они проверяются на корректность (математическая корректность и построение цепочки доверия). Если к сертификату привязан закрытый ключ, то напротив будет отображаться знак ключа .

Облачные сертификаты выделены знаком облака .
Возможно появление одного из двух статусов проверки сертификата: сертификат действительный и сертификат не действительный .



По нажатию на бургер-меню открывается меню разделов.



При этом кнопка меню заменяется на кнопку , по нажатию на которую происходит возврат назад к списку личных сертификатов. Меню содержит пункты:

- **Личные сертификаты** – для управления личными сертификатами, у которых есть привязка к закрытому ключу.
- **Промежуточные УЦ** – раздел с промежуточными сертификатами, необходимыми для корректного построения цепочек сертификации.
- **Доверенные корневые УЦ** – раздел с доверенными корневыми сертификатами, то есть сертификатами корневых удостоверяющих центров. В данном разделе также отображаются сертификаты сервисов УЦ (например, КриптоПро УЦ 2.0) со статусами созданных подключений. При получении сертификатов сервисов УЦ они автоматически устанавливаются в данный раздел.
- **Контейнеры** – раздел с ключевыми контейнерами. В данном разделе отображаются ключевые контейнеры локального хранилища CSP, подключенных устройств с возможностью установки сертификатов из контейнера.
- **Запросы на сертификат** – содержит созданные в приложении запросы на сертификат.
- **Списки отзыва** – раздел со списками отзыва на сертификаты. Необходимы для выполнения локальной проверки сертификатов на действительность.

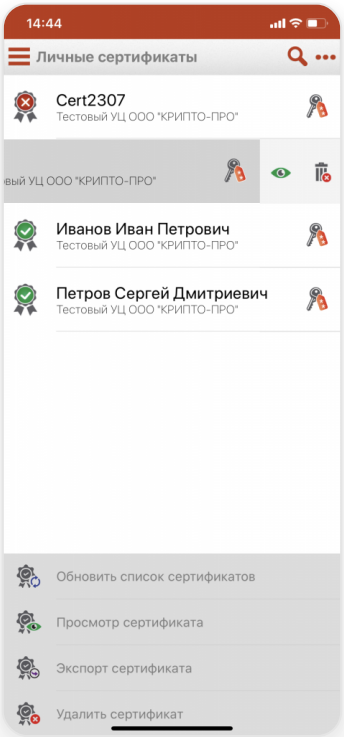
Открыть статью на сайте

Операции над сертификатами

Архив. КриптоАРМ ГОСТ для iOS.

Просмотр сертификата

Для просмотра сертификата при свайпе влево или в контекстном меню необходимо выбрать операцию **Просмотр сертификата**.

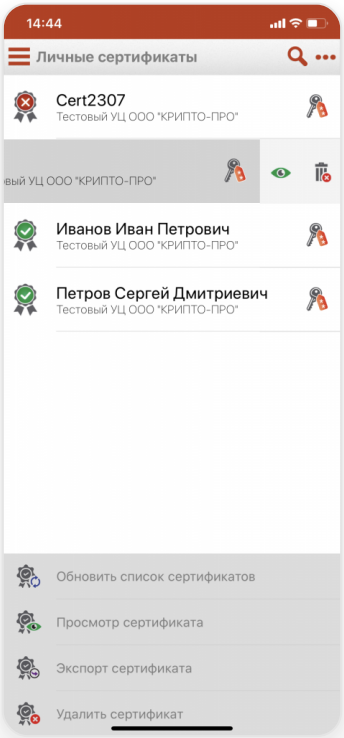


Открывается форма просмотра сертификата, содержащая пункты:

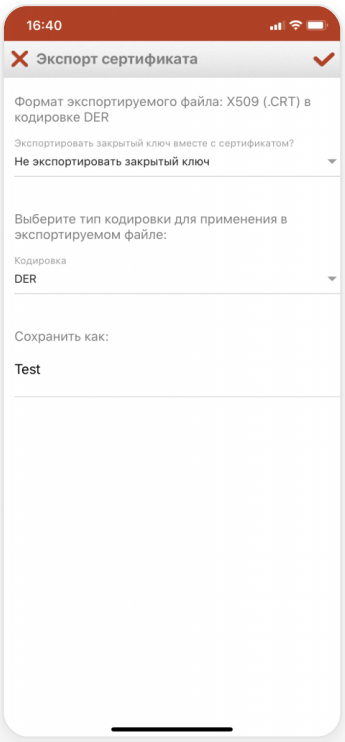
- **Сертификат** - содержит сведения о владельце сертификата, издателе и самом сертификате;
- **Цепочка доверия** - отображает общий статус построения цепочки доверия и приводится «дерево» сертификации.

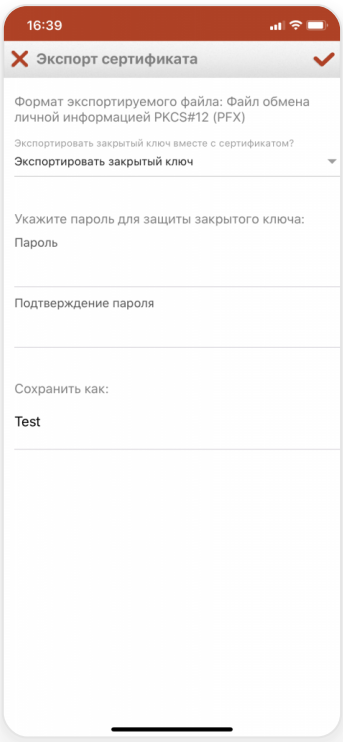
Экспорт сертификата

Для экспорта сертификата в контекстном меню необходимо выбрать операцию **Экспорт сертификата**.



Открывается форма выбора настроек формата файла экспортируемого сертификата. При экспорте сертификата можно экспортировать и не экспортировать закрытый ключ вместе с сертификатом.

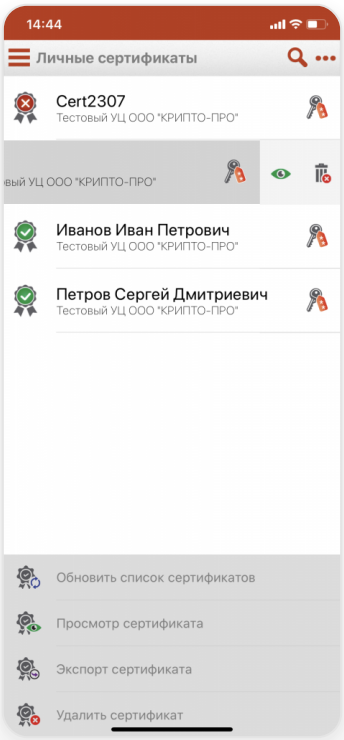




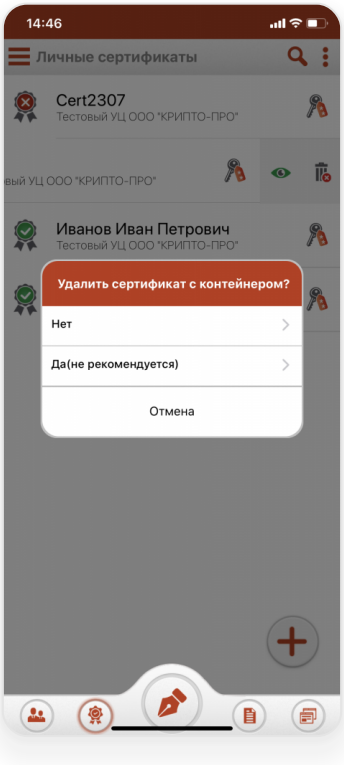
При выборе **Экспортировать закрытый ключ** необходимо указать пароль для защиты закрытого ключа. В случае выбора **Не экспортировать закрытый ключ** нужно только выбрать кодировку файла (BASE-64 или DER) сертификата.

Удаление сертификата

Для удаления сертификата при свайпе влево или в контекстном меню необходимо выбрать операцию **Удалить сертификат**.



В появившемся диалоговом окне нажать:



- **Нет** - для удаления сертификата без ключевого контейнера;
- **Да (не рекомендуется)** - для удаления сертификата вместе с ключевым контейнером;
- **Отмена** - для отмены удаления сертификата.

	Не рекомендуется удалять контейнер закрытого ключа, так как он не подлежит восстановлению.

Открыть статью на сайте

Импорт сертификата из файла

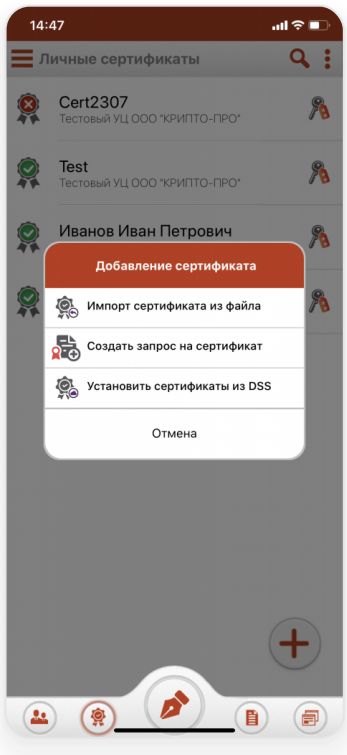
Архив. КриптоАРМ ГОСТ для iOS.

Импорт сертификатов может понадобиться для выполнения следующих задач:

- Установка личного сертификата с привязкой к ключевому контейнеру для выполнения операций подписи и расшифрования;
- Установка сертификата, который был отправлен другим пользователем, компьютером или центром сертификации.

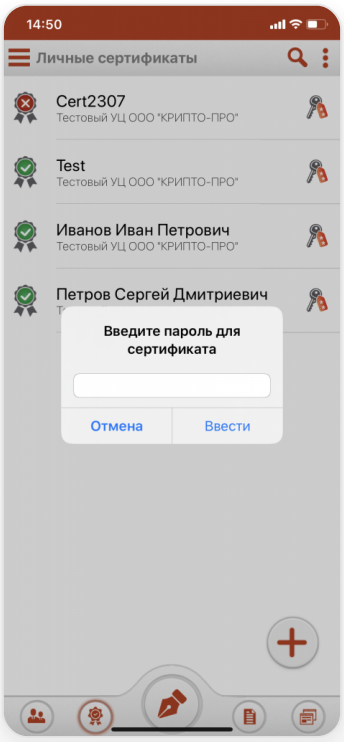
Импорт личного сертификата с привязкой к закрытому ключу

Импорт нового сертификата в хранилище выполняется кнопкой добавления сертификата . В открывшемся окне нужно выбрать операцию **Импортировать сертификат из файла**.

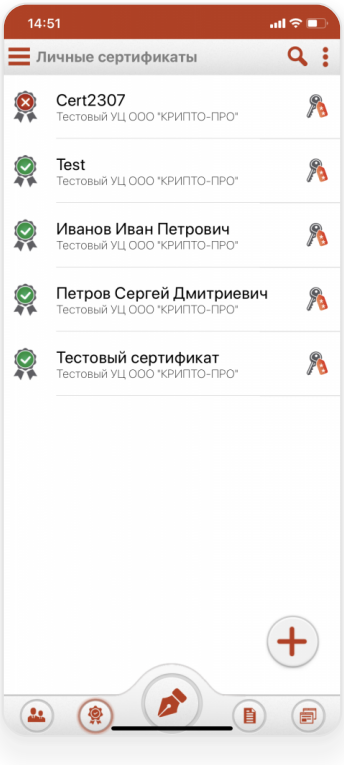


Если в приложении ранее был создан ключевой контейнер, и обработан запрос на сертификат в Удостоверяющем центре (УЦ), то в качестве файла сертификата нужно выбрать сертификат, полученный из УЦ. Сертификат будет отображаться в категории **Личные сертификаты**. Данным сертификатом можно подписывать и расшифровывать документы.

Если у пользователя есть сертификат с закрытым ключом в формате PKCS #12 (.pfx), то в качестве файла сертификата нужно выбрать данный сертификат. На запрос ввода пароля ввести пароль к ключевому контейнеру.



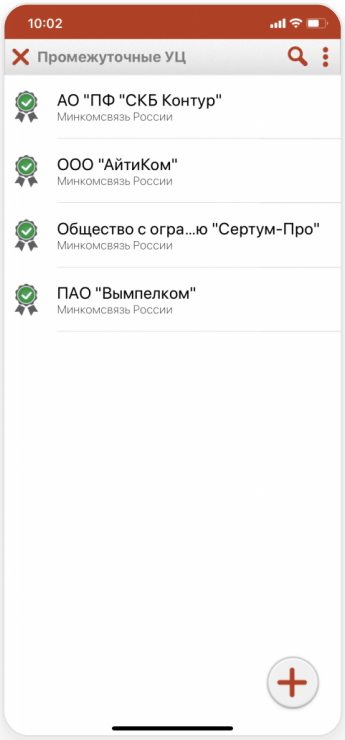
Далее задать новый пароль. Сертификат устанавливается в хранилище Личных сертификатов. У данного сертификата есть контейнер с закрытым ключом. Данным сертификатом можно подписывать и расшифровывать документы.



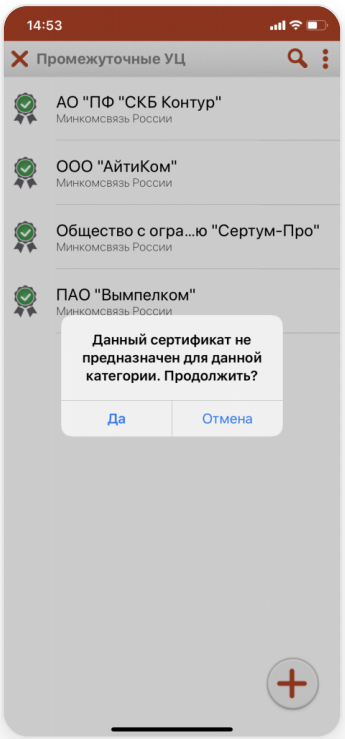
Если при импорте не будет найден закрытый ключ, соответствующий сертификату, то возникнет сообщение об ошибке «Ошибка при добавлении сертификата».

Импорт сертификата без привязки к закрытому ключу

Импорт нового сертификата в хранилище выполняется кнопкой добавления сертификата . Далее необходимо найти файл в хранилище и выбрать для добавления. При успешном выполнении операции импорта сертификат автоматически помещается в выбранное хранилище.



Если при импорте приложение определило, что для данного сертификата лучше подойдет другое хранилище, то возникнет сообщение об ошибке, с возможностью принудительной установки в выбранное хранилище.



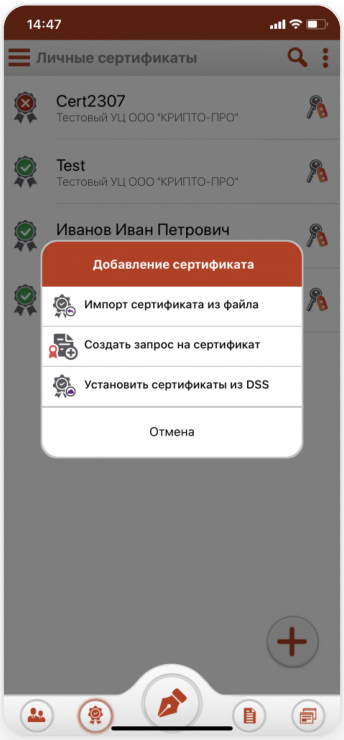
Открыть статью на сайте

Создание запроса на сертификат

Архив. КриптоАРМ ГОСТ для iOS.

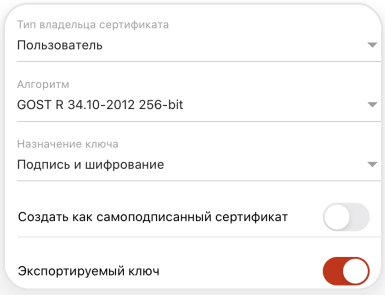
Создать запрос на сертификат можно, нажав кнопку **Добавить** .

- в разделе Личные сертификаты;
- в разделе Запросы.



Далее открывается форма создания запроса на сертификат, которая содержит поля для сбора необходимых сведений.

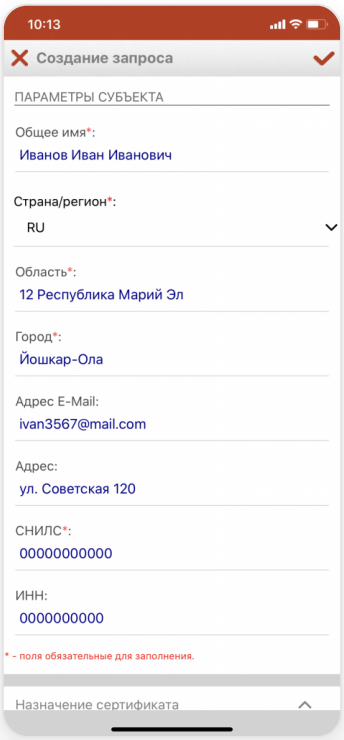
В зависимости от назначения сертификата выбирается **Тип владельца сертификата**, **Алгоритм** и **Назначение ключа**.



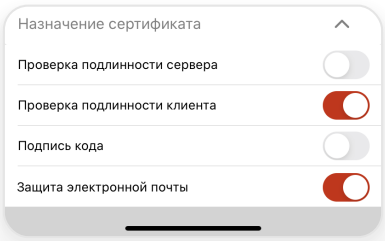
При включении опции **Создать как самоподписанный сертификат** происходит создание самоподписанного сертификата и его автоматическая установка в Личное хранилище пользователя и в хранилище Доверенных корневых сертификатов. Запросы на самоподписанные сертификаты не создаются.

При включении опции **Экспортируемый ключ** можно проводить экспорт сертификата вместе с закрытым ключом.

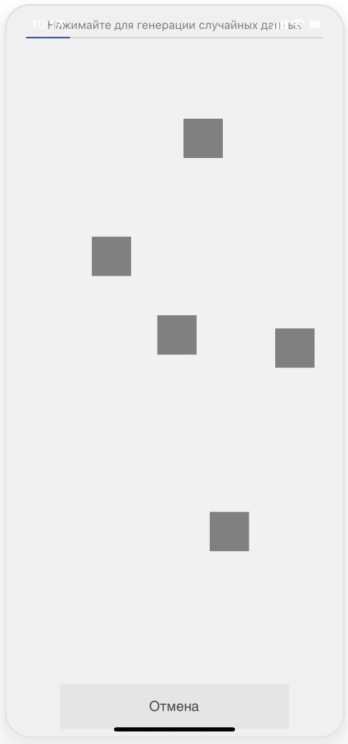
В разделе ниже **Параметры субъекта** указывается идентификационная информация о владельце сертификата согласно выбранному типу владельца сертификата.



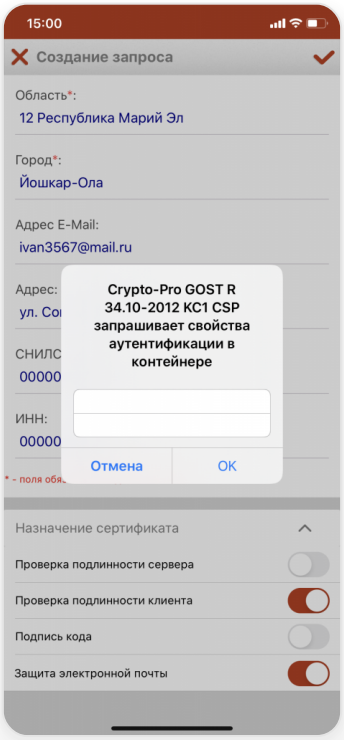
Назначение сертификата (EKU).



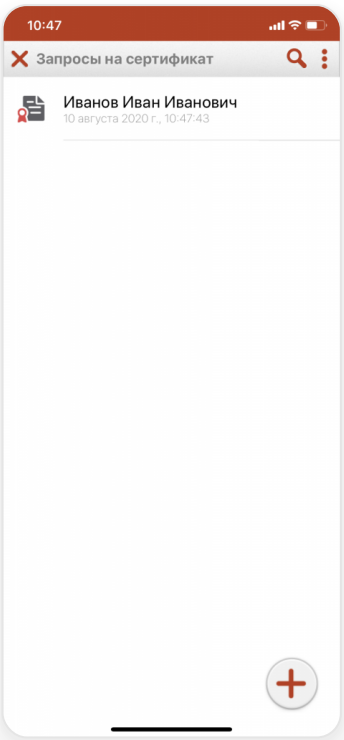
По кнопке **Галочка**  (в правом верхнем углу) будет открыта форма генерации ключевого контейнера.



Далее на запрос системы, установите пароль на данный контейнер и подтвердите его.



После завершения операции возникнет окно с информацией о ее результатах и, сформированный запрос, отобразится в разделе **Запросы на сертификат** в разделе **Сертификаты**.



Для запроса доступны следующие операции:

- **Просмотр** – для просмотра свойств запроса;
- **Экспортировать** – для сохранения сертификата в файл;
- **Удалить** – для удаления запроса из списка.

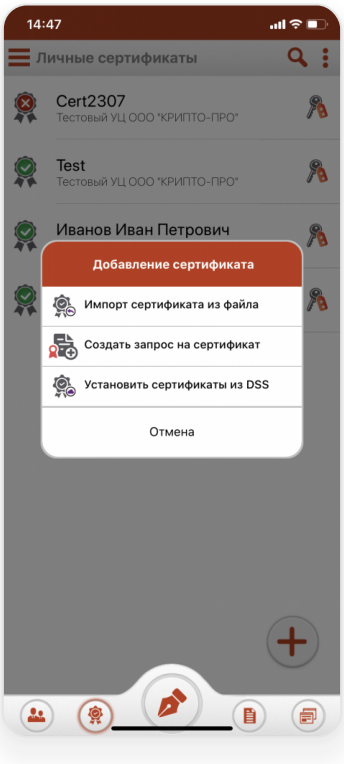
Созданный запрос на сертификат следует направить на рассмотрение в Удостоверяющий центр (УЦ). Далее полученный из УЦ сертификат импортировать в приложение для работы с данным сертификатом.

Открыть статью на сайте

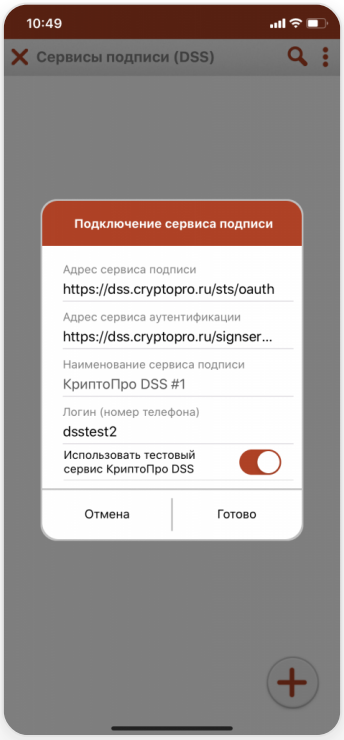
Получение сертификата DSS

Архив. КриптоАРМ ГОСТ для iOS.

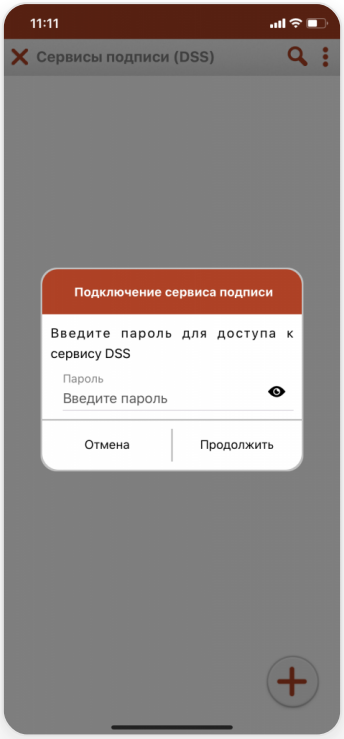
Для выполнения импорта сертификата из DSS в хранилище можно воспользоваться кнопкой добавления сертификата . В открывшемся окне нужно выбрать операцию **Установить сертификаты из DSS**.



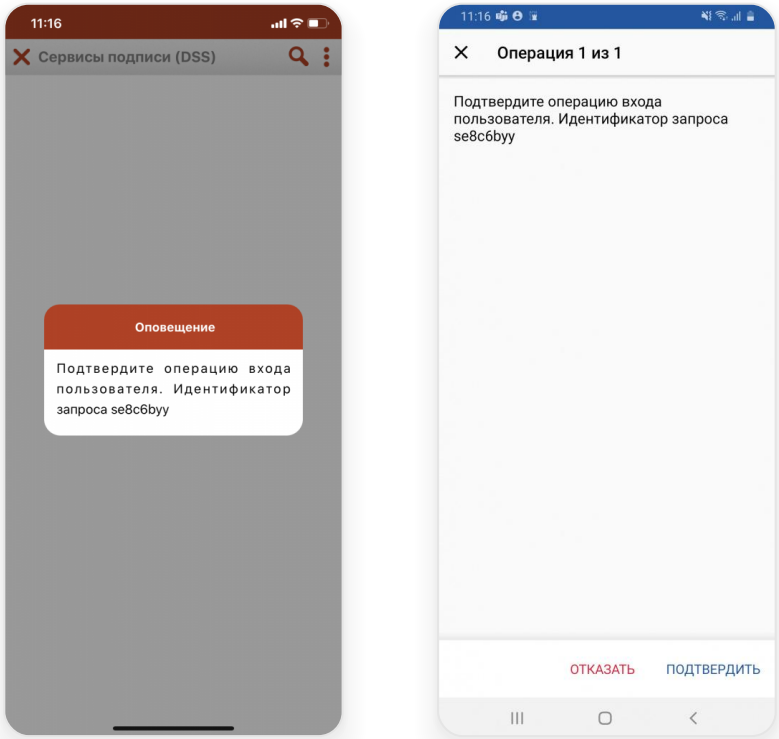
Далее откроется раздел для работы со списком подключений к DSS. Для добавления нового подключения необходимо нажать на кнопку добавления . После нажатия открывается окно для ввода адресов серверов авторизации и DSS, логина для аутентификации. В качестве примера использованы адреса тестового сервиса КриптоПро DSS.



Если у пользователя в личном кабинете стоит аутентификация по паролю, то в следующем появившемся окне необходимо ввести пароль.

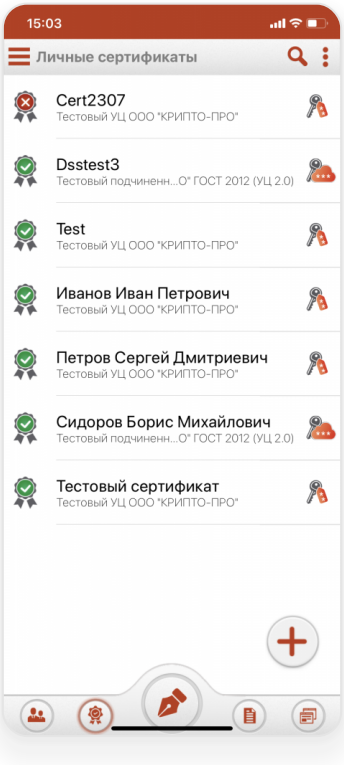


Если у пользователя в личном кабинете DSS в настройках стоит подтверждение аутентификации по SMS, электронной почте или с помощью мобильного приложения, то при нажатии **Готово** появляется сообщение, что операцию нужно подтвердить. Если нет, то данный шаг пропускается.

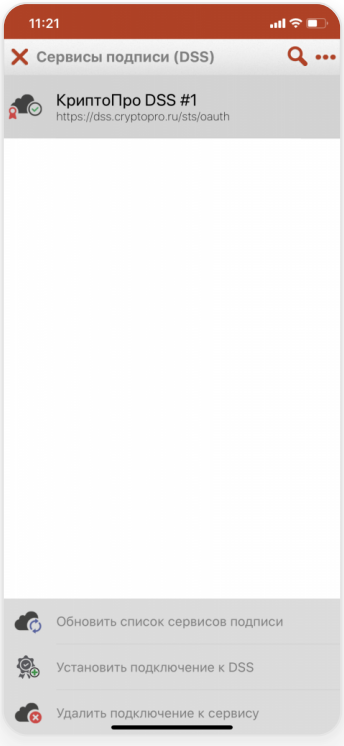


При успешной аутентификации на следующем шаге сертификаты DSS автоматически помещаются в хранилище Личных сертификатов.

Сертификаты DSS отличаются от сертификатов, хранящихся локально, индикатором «облако» .



Также списком сервисов DSS можно управлять. Для этого необходимо выделить подключение и нажать на контекстное меню.



Подключение к DSS можно:

- **Обновить** – обновление списка.

- **Установить** – переподключиться к сервису DSS (например, в результате каких-либо изменений в личном кабинете пользователя).
- **Удалить** – удалить подключение к сервису, сертификаты при этом не удаляются.

Открыть статью на сайте

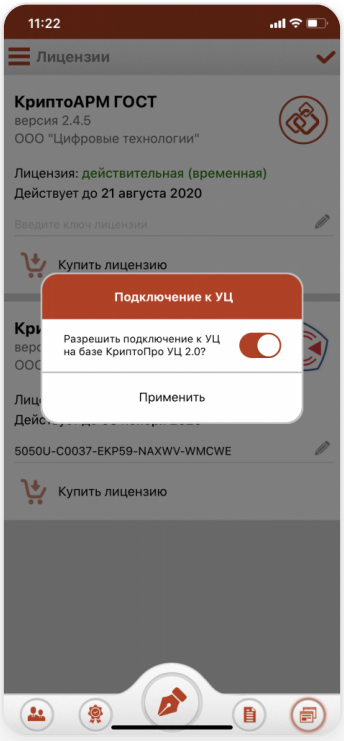
Получение сертификата из УЦ

Архив. КриптоАРМ ГОСТ для iOS.

Сервис Удостоверяющие Центры необходим для обработки запросов на сертификат и выпуска сертификатов для пользователей. При выборе сервиса **Удостоверяющие центры** открывается список подключений к сервисам УЦ.

До выполнения операций с сервисами необходимо удостовериться в наличии подключения к сети Интернет и загрузить промежуточный и корневой сертификаты удостоверяющего центра, к которому будет осуществляться подключение.

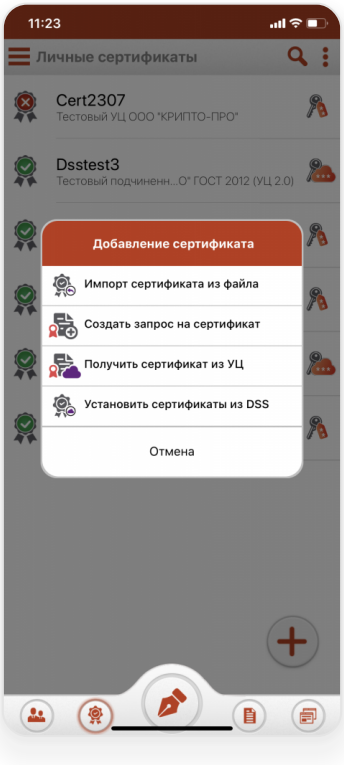
Для подключения к УЦ и последующего получения сертификата необходимо в разделе **Лицензии** в бургер-меню выбрать **Подключение к КриптоПро УЦ 2.0**. После выбора пункта меню появится модальное окно, в котором нужно разрешить подключение к УЦ на базе КриптоПро УЦ 2.0 и нажать **Применить**.



Для создания запроса на сертификат и выпуска сертификата пользователя нужно добавить сервис подключения к КриптоПро УЦ 2.0. А затем, используя данное подключение, создать запрос на сертификат.

Добавление нового сервиса

Создать подключение можно, выбрав **Получить сертификат из УЦ** в модальном окне при добавлении сертификата в списке Личных сертификатов.



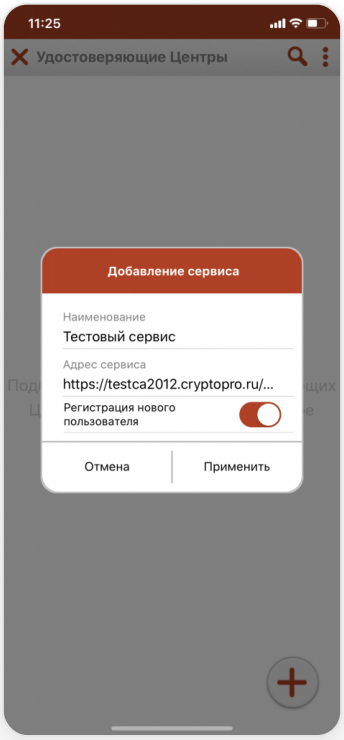
Открывается компонент для работы с подключениями к удостоверяющим центрам.

При нажатии на кнопку **Добавить** открывается форма ввода параметров подключения: Наименование и Адрес сервиса.

Адрес сервиса задается вместе с указанием GUID'а папки УЦ в следующем виде:

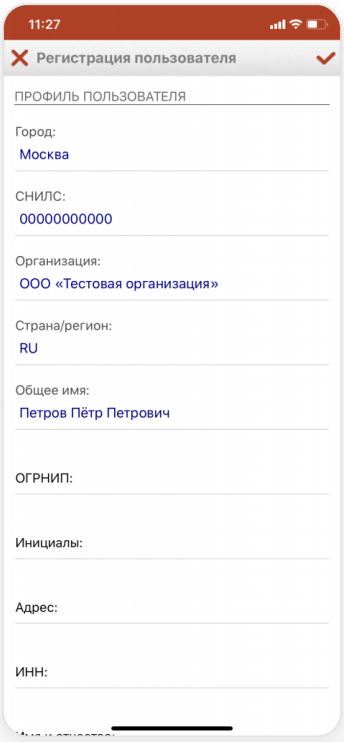
https://{адрес веб-сервера УЦ}/ui/api/{GUID folder}.

Если пользователь ранее не был зарегистрирован в УЦ, то для добавления подключения нужно активировать переключатель **Регистрация нового пользователя**.

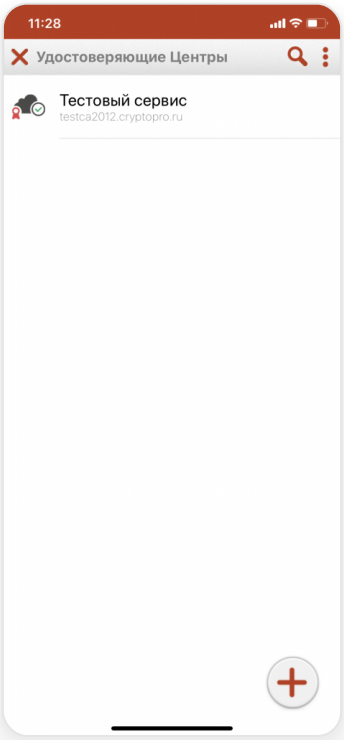


В качестве примера, введены данные для подключения к тестовому удостоверяющему центру.

После ввода данных для авторизации и нажатия на кнопку **Применить** открывается форма регистрации. Новое подключение не создастся без заполнения всех обязательных полей.

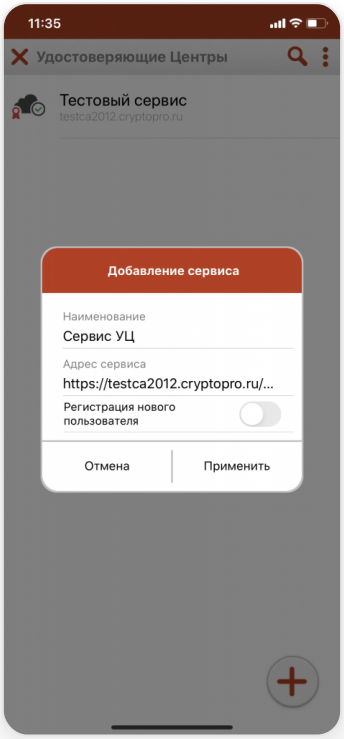


Если все данные введены корректно и подключение уникальное, то должно появиться новое подключение к УЦ.

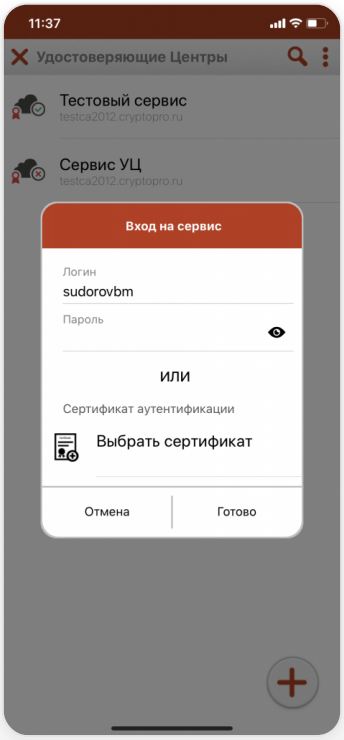


Вход на сервис

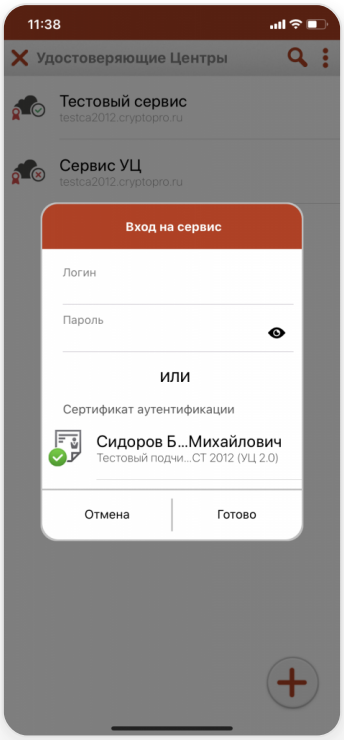
Если пользователь уже зарегистрирован в удостоверяющем центре, то возможно осуществить вход на сервис с логином/паролем или с сертификатом. Для этого в форме подключения необходимо не включать режим регистрации нового пользователя.



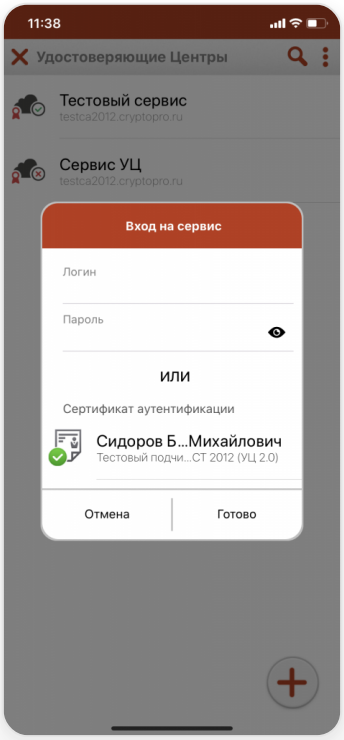
Далее появляется диалоговое окно входа на сервис.



В диалоге входа на сервис можно ввести логин/пароль или выполнить выбор сертификата для создания двухстороннего TLS соединения (выполняется аутентификация по сертификату).

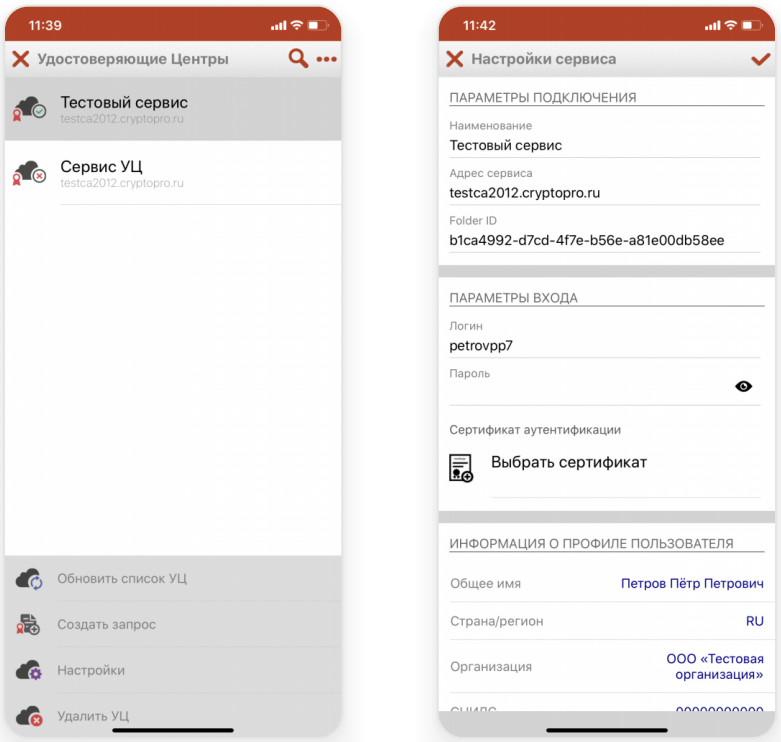


Для выбора сертификата открывается представление личного хранилища сертификатов. Для смены выбранного сертификата аутентификации достаточно повторно щелкнуть на него. Если указаны и логин/пароль и сертификат, приоритет будет у соединения по сертификату. Если соединение по сертификату не будет корректно установлено, то можно перейти на работу по логину/паролю.



Операции для сервисов УЦ

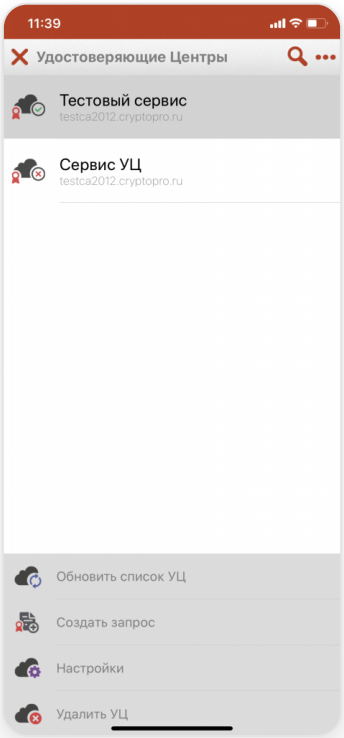
При выборе подключения и нажатии на кнопку контекстного меню появляется меню с доступными операциями:



- **Обновить список УЦ** – при обновлении проверяется статус текущих подключений к УЦ.
- **Создать запрос** - открывается форма создания запроса на сертификат, с привязкой к данному подключению сервиса УЦ.
- **Настройки** - открывается страница с отображением необходимых настроек подключения, где помимо названия сервиса и адреса присутствуют идентификаторы из профиля пользователя при регистрации, выбранный сертификат аутентификации. Поле **Наименование** является редактируемым. После редактирования сохранение осуществляется по кнопке Сохранить . Информация о профиле пользователя - та информация, которая заполняется пользователем при регистрации, либо ее можно извлечь на основании запроса для существующего пользователя УЦ.
- **Удалить** - удаление данного подключения вместе с профилем пользователя. Созданные запросы в виде сохраненных файлов остаются, только теряется привязка к УЦ.

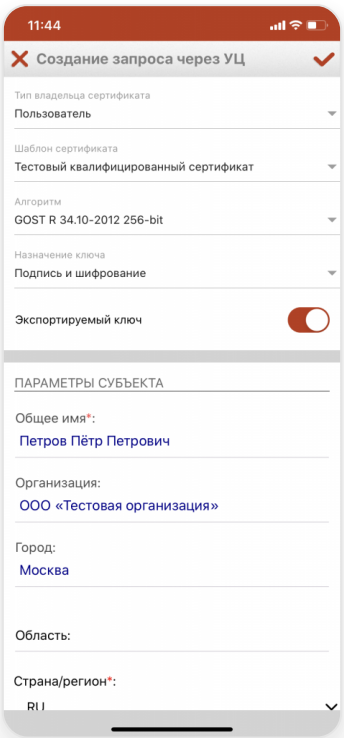
Создание запроса

Для создания запроса на получение сертификата из УЦ online необходимо выделить подключение к УЦ и в контекстном меню выбрать пункт **Создать запрос**.



Открывается форма создания запроса на сертификат. В данном представлении нужно выбрать Тип владельца сертификата, Шаблон сертификата, Алгоритм и Назначение сертификата.

Примечание: Для шаблона сертификата необходимо выбрать **Тестовый квалифицированный сертификат** (вариант №3). Форму запроса можно дополнить необходимыми данными в зависимости от выбранного типа владельца сертификата.

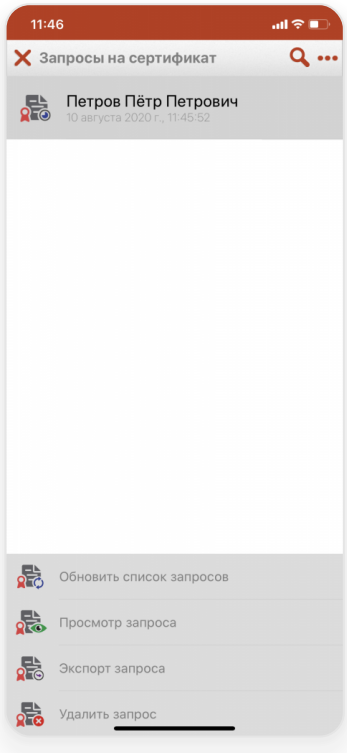


Далее нажать на  и сгенерировать ключевой контейнер, задать пароль. При успешном создании запроса, он будет находиться в разделе Запросы на сертификат.

Для отображения статуса запроса применяются следующие обозначения:

	Для данного запроса сертификат выпущен и установлен в хранилище КриптоПро.
	Запрос отклонен Удостоверяющим Центром.
	Запрос находится в обработке Удостоверяющим центром.
	Проблемы с соединением, не позволяющие актуализировать статус запроса.

Для того чтобы получить сертификат, необходимо **Обновить список запросов**. Если все данные верны, УЦ выпустит сертификат.

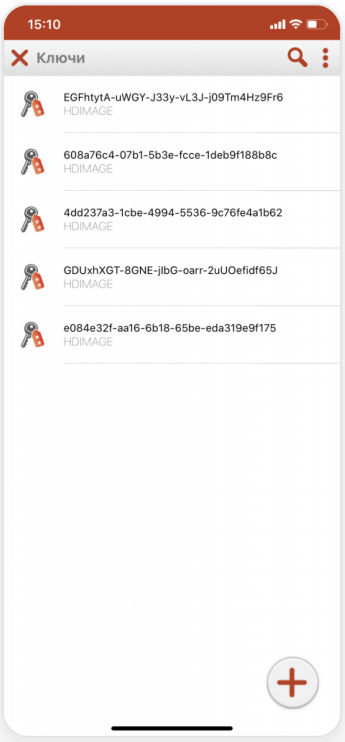


Открыть статью на сайте

Управление контейнерами

Архив. КриптоАРМ ГОСТ для iOS.

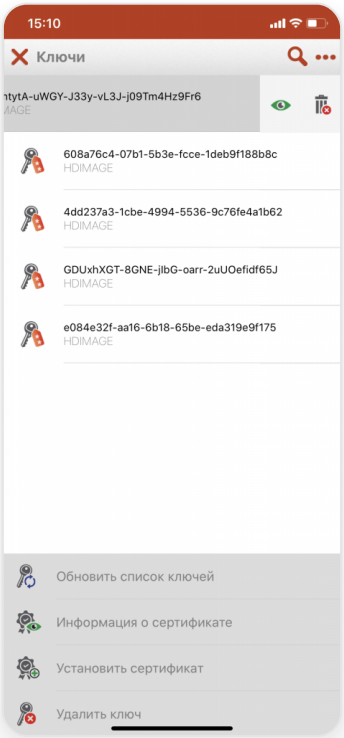
При открытии раздела **Контейнеры** отображается список контейнеров, которые установлены в локальное хранилище КриптоПро CSP. В представлении кроме кнопки возврата назад (закрытия) и поиска также имеется кнопка вызова меню операций .



Обновление списка ключей

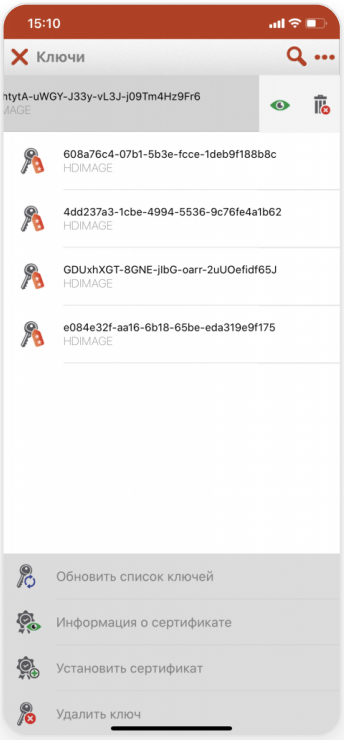
Для перечитывания контейнеров из локального хранилища необходимо выбрать пункт **Обновить список ключей** в меню операций. Обновление списка ключей необходимо при:

- подключении рутокена;
- добавлении нового сертификата.

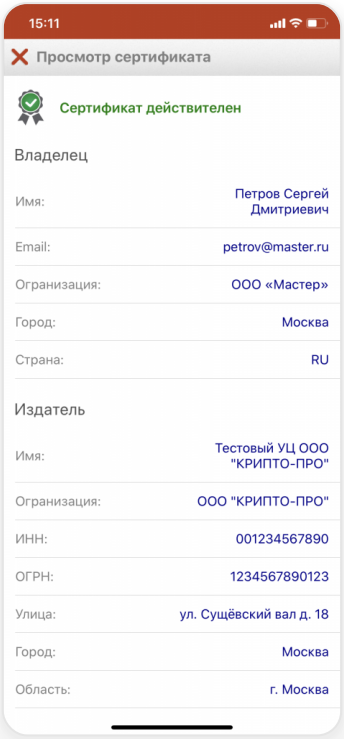


Просмотр информации о сертификате

Если в контейнере есть сертификат, то можно посмотреть информацию о нем, нажав **Информация о сертификате** в меню операций или при свайпе влево. Данный пункт отображается в меню только в том случае, если в контейнере имеется сертификат пользователя.

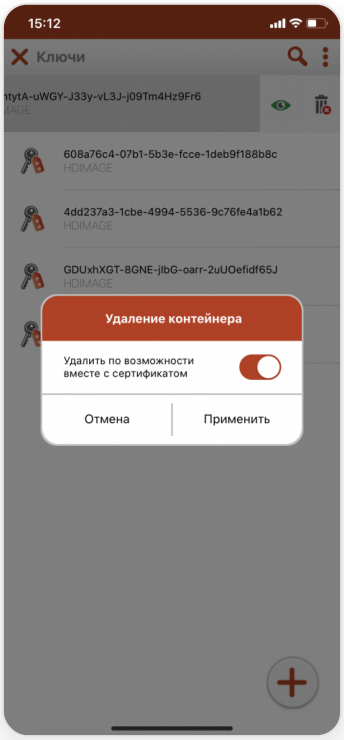


После нажатия на кнопку операции открывается форма **Просмотр сертификата**. В данной форме предоставлена информация о сертификате.



Удаление контейнера

При выборе операции **Удалить ключ** в меню операций или при свайпе влево, возникает диалоговое окно для выбора способа удаления контейнера, вместе с сертификатом, связанным с контейнером, или без сертификата. Если удалить контейнер без связанного с ним сертификата, то в хранилище сертификатов останется сертификат без ключевого контейнера. Таким сертификатом нельзя выполнять операции подписи и расшифрования.

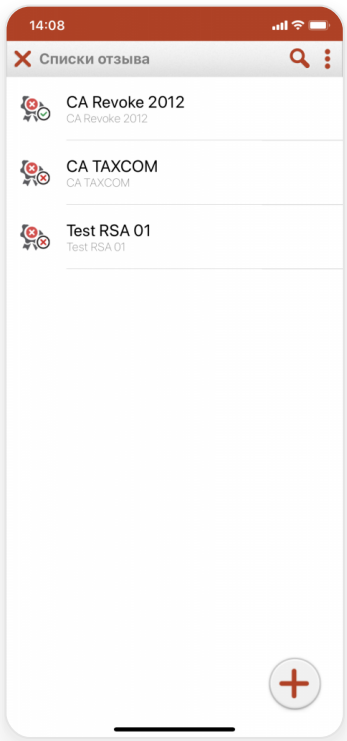


Открыть статью на сайте

Списки отзыва сертификатов (COC)

Архив. КриптоАРМ ГОСТ для iOS.

Для работы со списками отзыва сертификатов в пункт меню Сертификаты добавлен подпункт **Списки отзыва сертификатов**.



По кнопке можно установить список отзыва из хранилища. При успешном импорте файл отображается в разделе Список отзыва сертификатов.

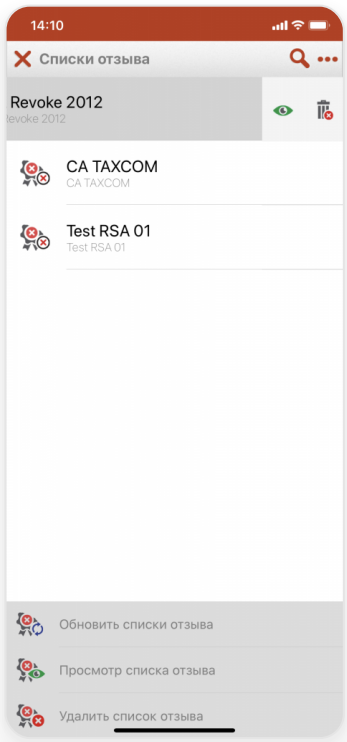
Для списков отзыва могут быть следующие обозначения:

список отзыва сертификатов с корректной подписью;

список отзыва сертификатов с некорректной подписью.

Обновление списка отзыва

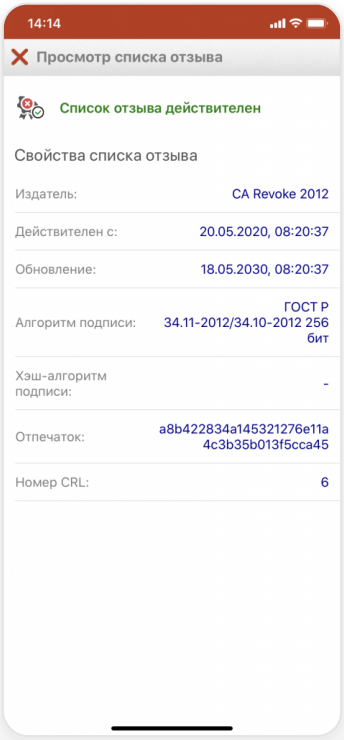
Для обновления списка отзыва в контекстном меню необходимо выбрать операцию Обновить списки отзыва. При вызове контекстного меню операция появляется всегда.



Данная операция позволяет снова проверить корректность списка отзыва, и, если произошли изменения, то они отражаются в изменении статусов иконок.

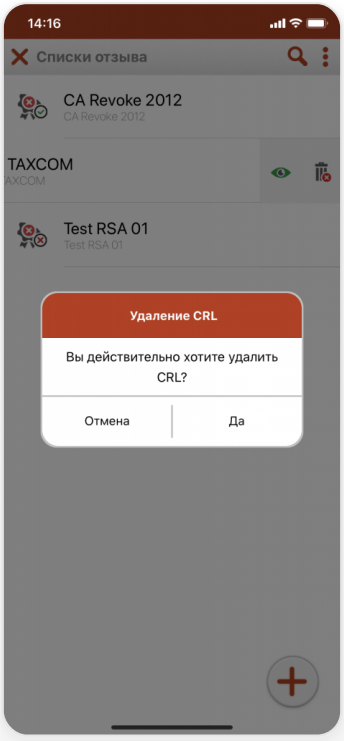
Просмотр списка отзыва

Для просмотра свойств списка отзыва сертификата при свайпе влево или в контекстном меню необходимо выбрать операцию **Просмотр отзыва**. При выделении множества элементов операция просмотра свойств списка отзыва скрывается. Свойства отображаются в отдельном компоненте.



Удаление списка отзыва

Для удаления списка отзыва сертификата при свайпе влево или в контекстном меню необходимо выбрать операцию **Удалить**. Удалять можно один элемент или сразу несколько. При удалении необходимо подтвердить действие в соответствующем диалоговом окне.

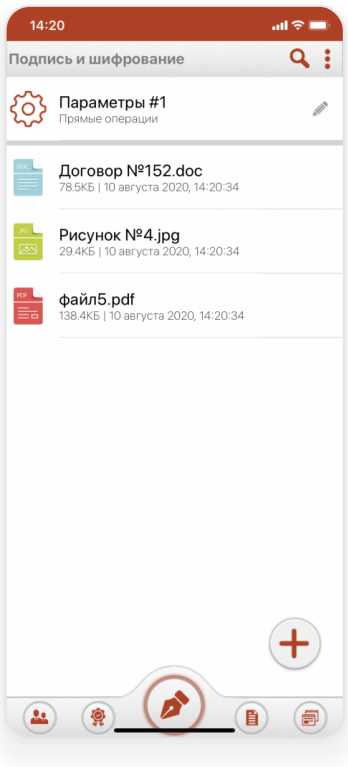


Открыть статью на сайте

Управление списком файлов для выполнения операций

Архив. КриптоАРМ ГОСТ для iOS.

Файлы в Мастер подписи и шифрования можно добавить двумя способами: через кнопку **Добавить**  или открыть файл из стороннего приложения (например, открыть файл через диск, почту, галерею).

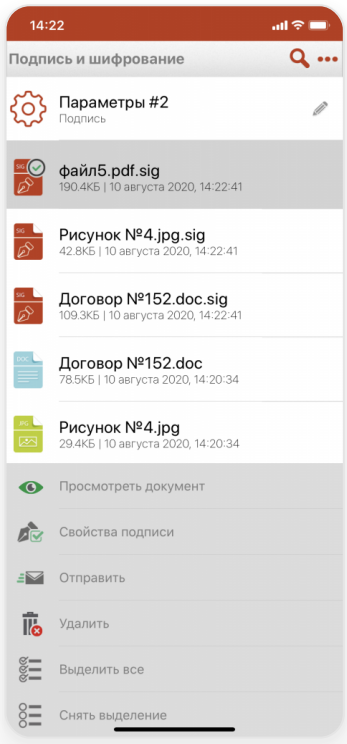


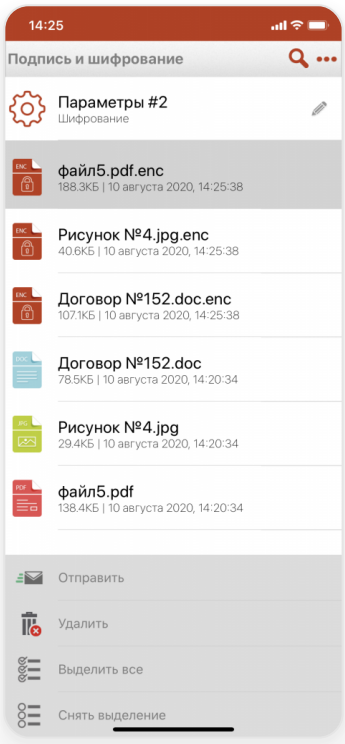
Для списка документов доступны поиск и управление файлами через контекстное меню, открывающееся при нажатии на кнопку . В меню предоставлены операции, описанные в таблице:

Операция	Действие
 Просмотреть документ	Выполняется передача документа на просмотр стороннему приложению через диалог выбора. Операция отображается только в том случае, если в списке выделен один документ.
 Отправить	

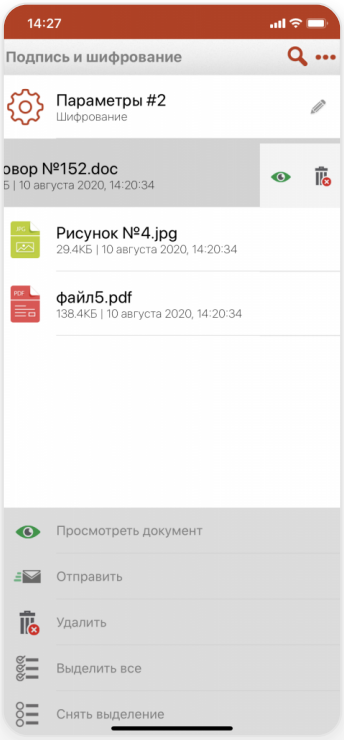
	Данная операция осуществляет передачу выбранного документа любому приложению из отображаемого списка для последующей обработки.
Удалить	Операция позволяет удалить выбранный документ из текущего списка.
Свойства подписи	Выполняется открытие представления с отображением информации о подписи. Эта операция в меню доступна только при выделении одного подписанного документа.
Выделить все	Происходит выделение всех элементов списка документов.
Снять выделение	При выборе операции выделение с файлов в списке сбрасывается. Меню операций закрывается. После сброса выделения в меню остается только операция Выделить все.

Пример вызова контекстного меню для одного подписанного и зашифрованного файла:





Для каждого файла списка доступны кнопки операции, появляющиеся при свайпе влево:

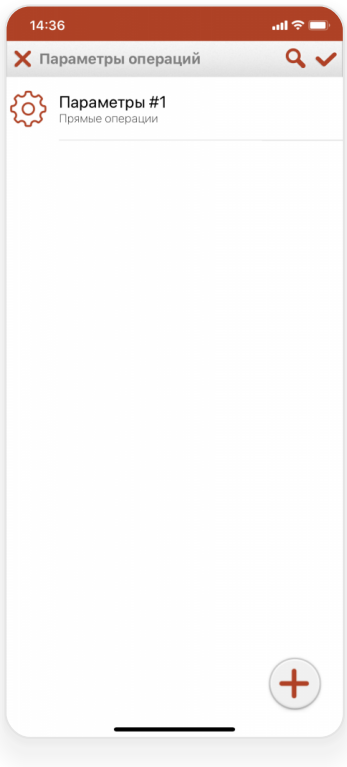

14:27
Подпись и шифрование
Параметры #2
Шифрование
овор №152.doc
Б | 10 августа 2020, 14:20:34
Рисунок №4.jpg
29.4КБ | 10 августа 2020, 14:20:34
файл5.pdf
138.4КБ | 10 августа 2020, 14:20:34
Просмотреть документ
Отправить
Удалить
Выделить все
Снять выделение

Открыть статью на сайте

Параметры операций

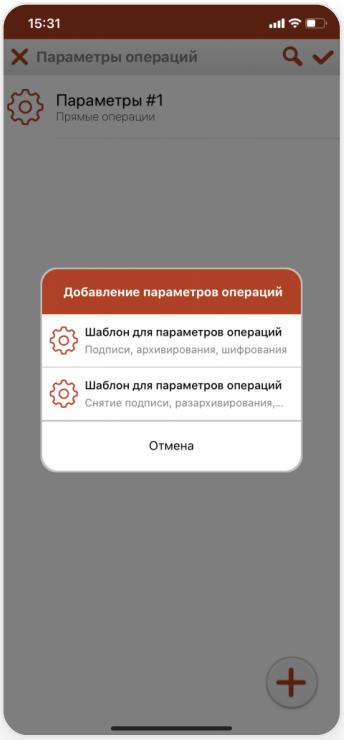
Архив. КриптоАРМ ГОСТ для iOS.

Установка параметров подписи и шифрования происходит в разделе **Параметры операций**. Для того, чтобы перейти в параметры операций, нужно в Мастере подписи и шифрования нажать на карандаш . Далее откроется раздел, в котором будут отображаться все созданные и сохраненные операции.

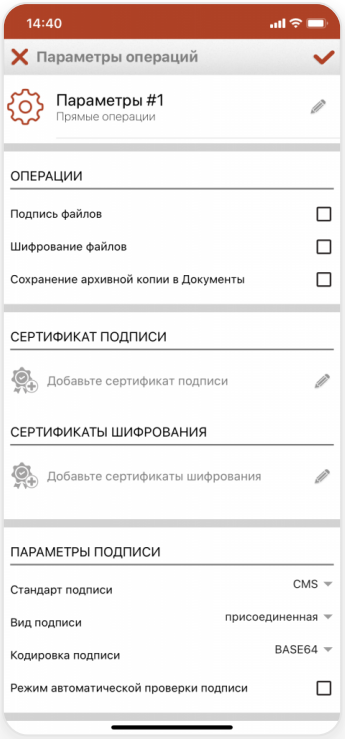


Добавление нового параметра операций производится по кнопке **Добавить** .

После нажатия кнопки появляется диалоговое окно с выбором шаблона для параметра операции. Для того чтобы подписать или зашифровать файлы, необходимо выбрать «Шаблон для параметров операций (подписи, архивирования, шифрования...)».



Далее после выбора шаблона откроется настройка Параметров операции.



В параметрах операций можно настроить:

- Наименование операции;

- Тип операции;
- Сертификат подписи;
- Сертификаты шифрования;
- Параметры подписи;
- Параметры шифрования.

Установка типа операции

В блоке Операции можно выбрать тип операции:

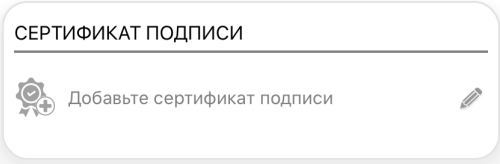
- Подпись файлов;
- Шифрование файлов;
- Сохранение архивной копии в Документы.



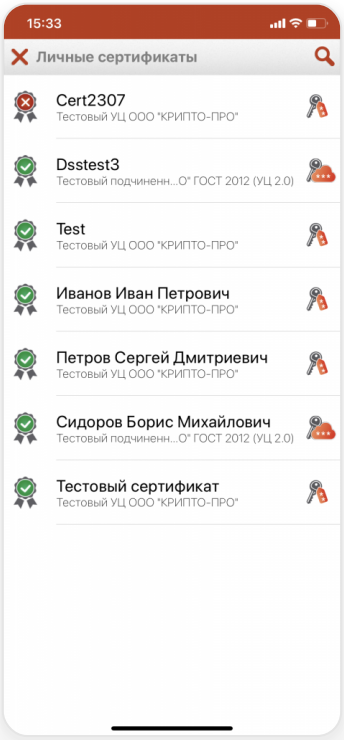
Примечание: Опция **Сохранение архивной копии в Документы** служит для сохранения копии полученного после операций файла в раздел Документы, который находится в пункте меню .

Установка сертификата подписи

В блоке **Сертификат подписи** необходимо выбрать сертификат с закрытым ключом из списка **Личных сертификатов**. Эта операция производится нажатием на иконку карандаша .



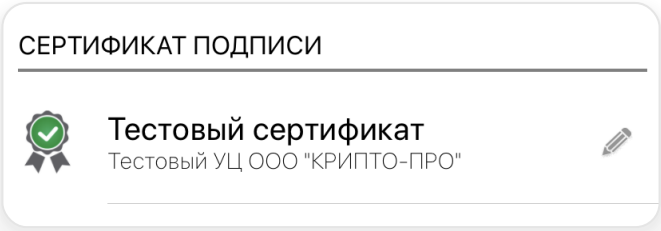
В появившемся окне отобразятся Личные сертификаты.



Выбор сертификата подписи осуществляется его выделением. Если был выбран неправильный сертификат, то его можно заменить повторным нажатием на иконку .

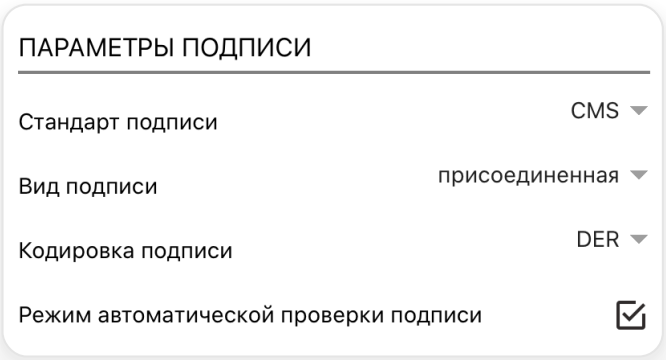
Примечание: Если в хранилище личных сертификатов нет сертификата с закрытым ключом, то его можно создать или импортировать в разделе Сертификаты.

После успешного выбора сертификат будет отображаться в разделе **Сертификат подписи**.



Установка параметров подписи

Параметры подписи задаются в разделе **Параметры подписи**.

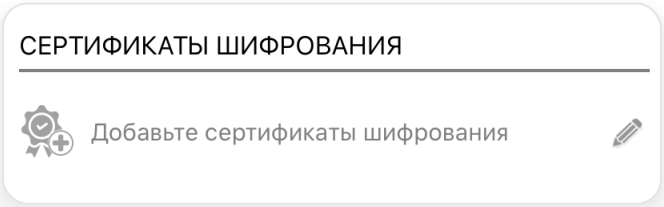


В параметрах можно настроить:

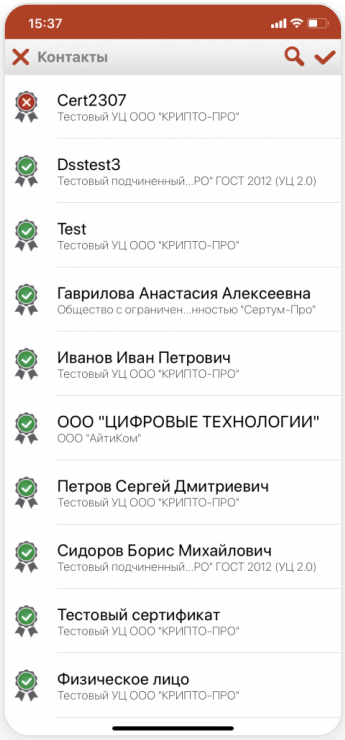
- Стандарт подписи - CMS для создания классической подписи.
- Вид подписи – присоединённая или отсоединённая.
- Кодировка подписи - сохранение подписи в одной из двух кодировок (BASE64 или DER).
- Режим автоматической проверки подписи – корректность подписи проверяется сразу же после добавления или создания подписанного файла.

Установка сертификатов шифрования

Для того, чтобы выполнить шифрование необходимо выбрать сертификаты получателей. Эта операция производится нажатием на иконку карандаша в разделе **Сертификаты шифрования**.



Выбор сертификатов шифрования осуществляется из списка Контакты, в составе которого отображаются и личные сертификаты. В списке Контакты возможен множественный выбор сертификатов, поэтому окончательный набор элементов фиксируется кнопкой .



Если был выбран неправильный сертификат, то его можно заменить повторным нажатием на иконку .

Если в хранилище отсутствуют сертификаты, то их можно создать или импортировать в разделах Сертификаты и Контакты.

После успешного выбора сертификаты отображаются в разделе Сертификаты шифрования.



Установка параметров шифрования

Параметры шифрования задаются в разделе Параметры шифрования.



В параметрах можно настроить:

- Кодировка шифрования - сохранение зашифрованного файла в одной из двух кодировок (BASE64 или DER).
- Архивировать файлы перед шифрованием - файлы архивируются (ZIP) перед выполнением операции шифрования. Шифруется созданный ZIP-архив.
- Проверять keyAgreement - при установленном флаге, при операции шифрования в сертификатах проверяется наличие в расширении keyUsage использование ключа keyAgreement (согласование ключей). Если в сертификате нет использования ключа «Согласование ключей», то при включенном флаге, операция шифрования в адрес такого сертификата производится не будет. При выключенном флаге шифрование будет выполняться в адрес сертификатов без использования ключа «Согласование ключей».

После настройки всех необходимых параметров для сохранения нужно нажать на галочку . Далее в списке Параметров операций выделить параметр и снова нажать на галочку. Все настроенные параметры операции будут сохранены в данном списке.

Открыть статью на сайте

Создание электронной подписи

Архив. КриптоАРМ ГОСТ для iOS.

Для того, чтобы подписать файлы необходимо:

1. В **Мастер подписи и шифрования** добавить файлы для подписания.

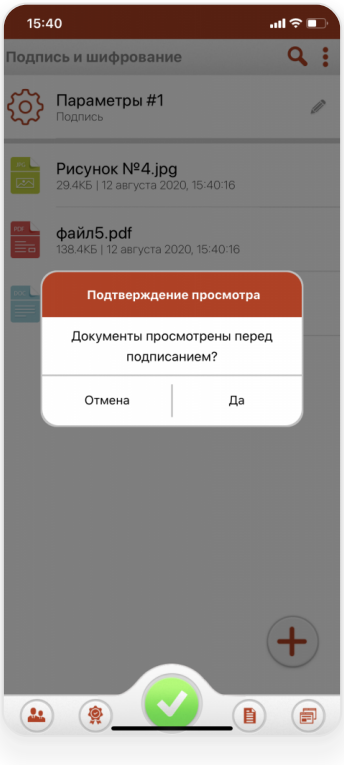
2. В **Параметрах операций** выбрать/создать шаблон, в котором нужно указать сертификат подписи и задать параметры подписи.

В приложении КриптоАРМ ГОСТ доступно создание подписи для одного или сразу нескольких файлов.

После выполнения всех условий:

- Добавлен хотя бы один файл;
- В настройках параметра операции выбран сертификат подписи и установлена опция «Подпись» (если необходимо только подписать файлы, опция «Шифрование» должна быть не активна); появляется кнопка **Выполнить** . Нажатие на кнопку **Выполнить** запускает процесс подписи.

Подписываемые файлы обязательно необходимо просмотреть перед операцией. Для дополнительной проверки далее появляется диалоговое окно с вопросом: «Документы просмотрены перед подписанием?».

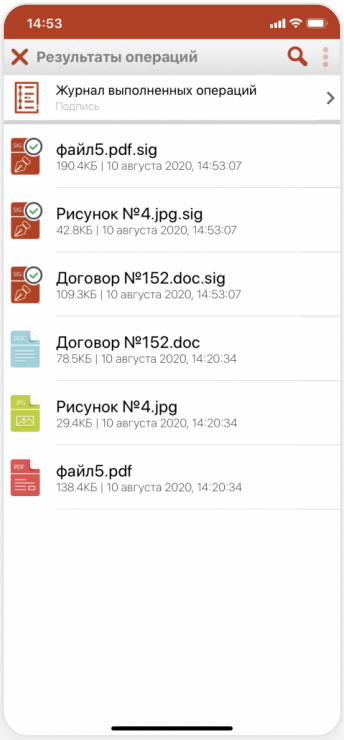


Если документы просмотрены, то необходимо нажать **Да** и начнется процесс подписи. В противном случае, рекомендуется нажать **Отмена** и просмотреть документы.

Выбранные файлы подписываются по очереди. Если сертификат защищен паролем, то при подписи появится диалоговое окно для подтверждения пароля.

По кнопке **Отмена** операция подписи не выполняется.

По окончании процесса исходные документы (оригиналы) и результаты операций (с расширением **.sig**) отображаются в отдельном мастере **Результаты операций**.

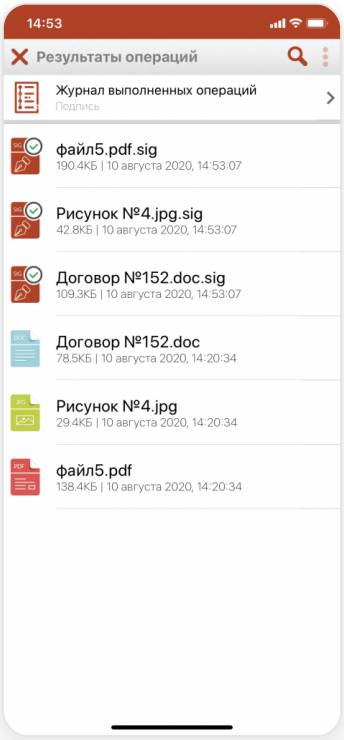

14:53
Результаты операций
Журнал выполненных операций
Подпись
файл5.pdf.sig
190.4КБ | 10 августа 2020, 14:53:07
Рисунок №4.jpg.sig
42.8КБ | 10 августа 2020, 14:53:07
Договор №152.doc.sig
109.3КБ | 10 августа 2020, 14:53:07
Договор №152.doc
78.5КБ | 10 августа 2020, 14:20:34
Рисунок №4.jpg
29.4КБ | 10 августа 2020, 14:20:34
файл5.pdf
138.4КБ | 10 августа 2020, 14:20:34

Открыть статью на сайте

Результаты операций

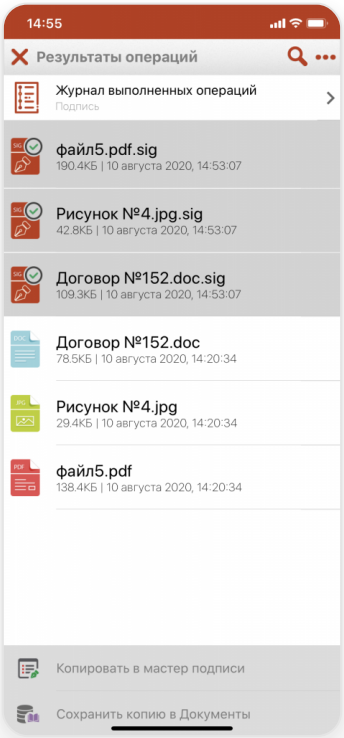
Архив. КриптоАРМ ГОСТ для iOS.

По окончании процесса исходные документы (оригиналы) и результаты операций отображаются в отдельном мастере **Результаты операций**.



У файлов меняется иконка, наименование, дата создания.

Документы из Результатов операции можно **Копировать в мастер подписи** для выполнения других операций или **Сохранить копию в Документы**. Для этого необходимо выделить файлы и нажать на контекстное меню. Далее откроется список как показано на рисунке ниже.



Опция **Сохранить копию в Документы** служит для сохранения копии файлов в раздел **Документы**, который находится в пункте меню .

После выполнения операций Мастер подписи и шифрования очищается от добавленных в него файлов. Результаты операций сохраняются до выполнения следующей операции или до закрытия приложения.

Также, в мастере Результаты операций можно просмотреть документ свайпом влево.

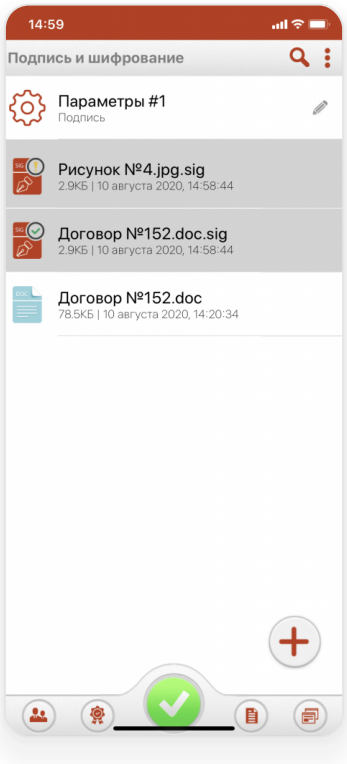
Открыть статью на сайте

Проверка электронной подписи

Архив. КриптоАРМ ГОСТ для iOS.

Для проверки подписи достаточно выделить файлы с расширением **.sig**, которые содержат электронную подпись. В результате иконка подписанного файла меняется на иконку с отображением статуса подписи.

Результатом проверки подписи является отображение информации о подписи документа в виде изменения иконки подписанного файла  на иконку, содержащую статус подписи.

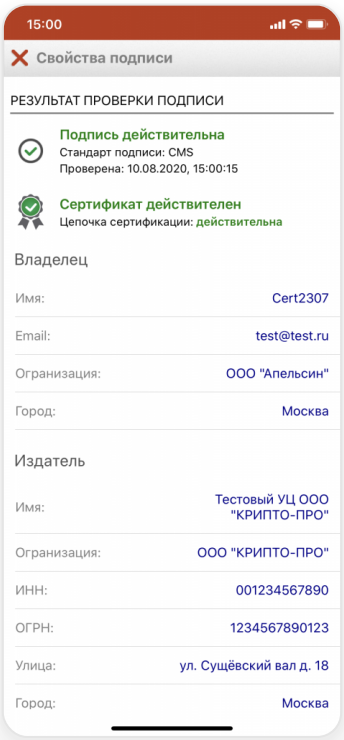


Все возможные статусы продемонстрированы ниже в таблице:

Статус подписи	Описание
	Подпись корректна.
	Подпись некорректна.
	Невозможно проверить подпись.

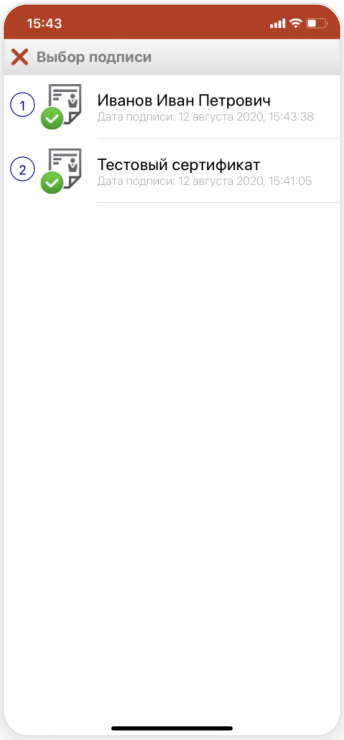
	Статус выставляется в том случае, например, когда проверка осуществляется через API внешнего сервиса и в текущий момент времени необходимый ответ не получен или не установлено соединение. Данный статус появляется, если подпись отсоединенная и в списке мастера отсутствует оригинальный документ, необходимый для проверки.

Если в списке выделен один подписанный файл, то при вызове контекстного меню, среди доступных операций имеется операция **Свойства подписи**, которая открывает результат проверки подписи в отдельном представлении. На рисунке показано представление для отображения свойств подписи документа:



Свойства подписи отображаются единым списком с полосой прокрутки.

Если документ подписан несколькими подписями (имеет соподписи), то для просмотра информации о подписи нужно выбрать подписчика.


15:43
Выбор подписи
1
Иванов Иван Петрович
Дата подписи: 12 августа 2020, 15:43:38
2
Тестовый сертификат
Дата подписи: 12 августа 2020, 15:41:05

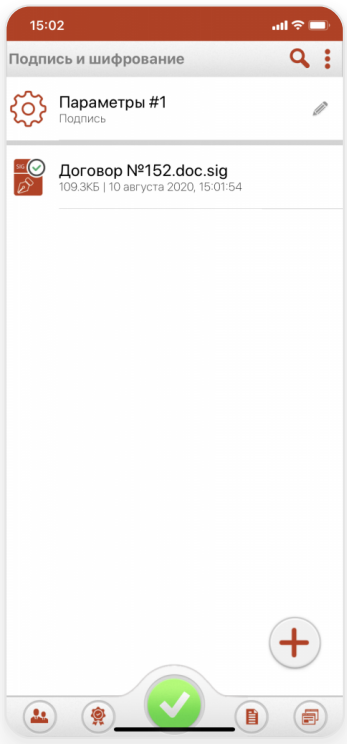
Открыть статью на сайте

Добавление подписи

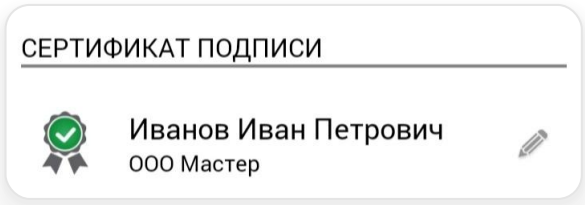
Архив. КриптоАРМ ГОСТ для iOS.

Приложение КриптоАРМ ГОСТ позволяет добавлять электронные подписи к уже подписанному файлу. Добавление подписи осуществляется также по нажатию на кнопку **Выполнить** . Для того, чтобы кнопка выполнения стала зеленой, необходимо выполнение следующих условий:

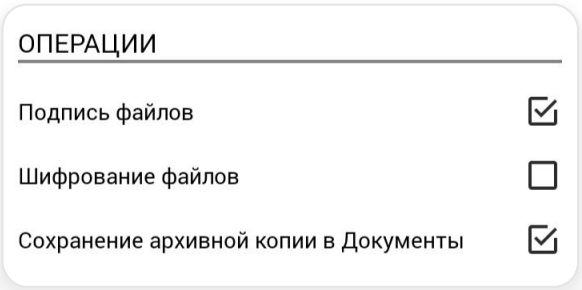
1. Добавлен хотя бы один подписанный файл;



2. Выбран сертификат подписи:

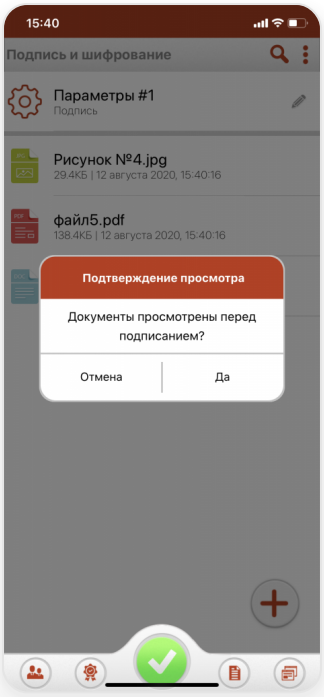


3. Установлен переключатель Подпись. Если необходимо только подписать файлы, переключатель Шифрование должен быть не активен.

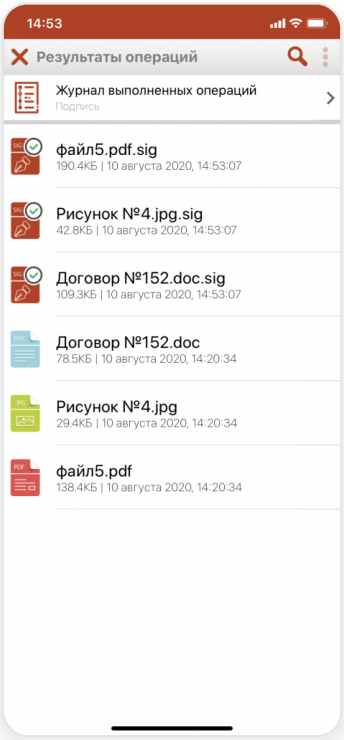


Примечание: Для всех добавленных подписей настройки подписи, такие как кодировка и вид подписи, используются по умолчанию, как для первой подписи.

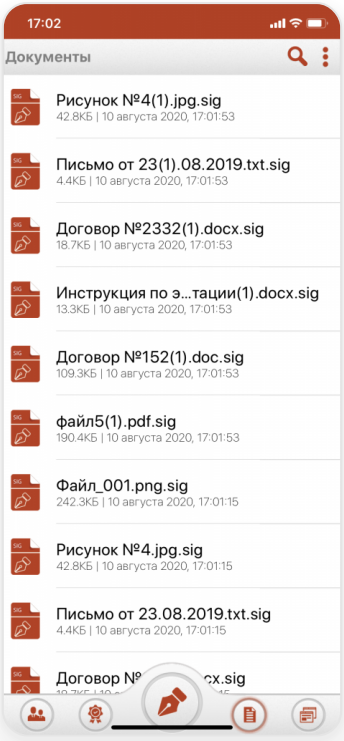
Подписываемые файлы обязательно необходимо просмотреть перед операцией. Далее появляется диалоговое окно с вопросом: «Документы просмотрены перед подписанием?». Если документы просмотрены, то необходимо нажать **Да** и начнется процесс подписи. В противном случае, рекомендуется нажать **Отмена** и просмотреть документы.



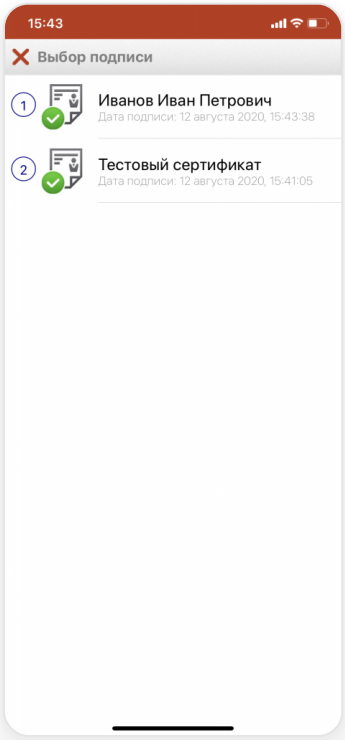
Результат добавления подписи отобразится в отдельном мастере Результаты операций.



Если в разделе Операции выбрано «Сохранение архивной копии в Документы», то дополнительно результат подписи добавляется в раздел **Документы**.



В информации о подписи будут содержаться сведения о всех подписях. Чтобы посмотреть информацию о конкретном подписчике, нужно выбрать подписчика из списка, нажав на Свойства подписи.

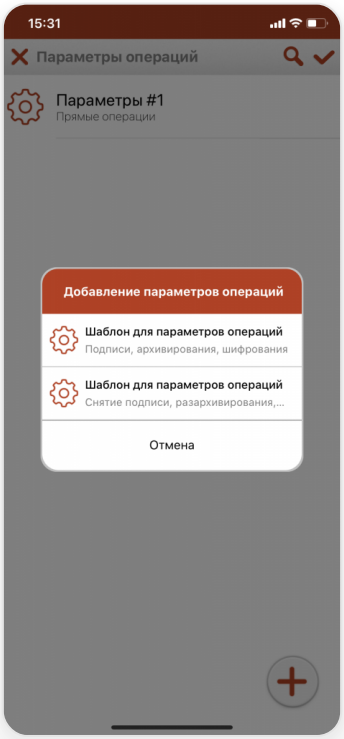

15:43
Выбор подписи
1
Иванов Иван Петрович
Дата подписи: 12 августа 2020, 15:43:38
2
Тестовый сертификат
Дата подписи: 12 августа 2020, 15:41:05

Открыть статью на сайте

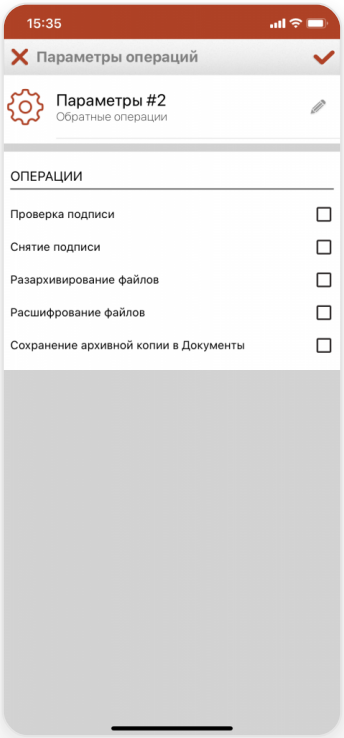
Снятие электронной подписи

Архив. КриптоАРМ ГОСТ для iOS.

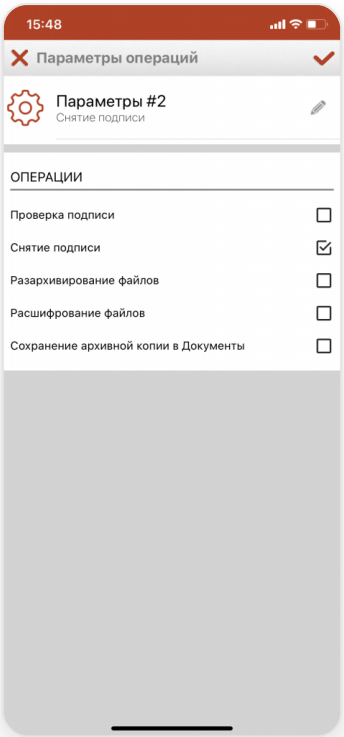
Для снятия подписи необходимо создать новый шаблон параметра операции. При добавлении выбрать шаблон «Шаблон для параметров операций (Снятие подписи, разархивирование...)».



Далее после выбора шаблона откроется настройка Параметров операции.

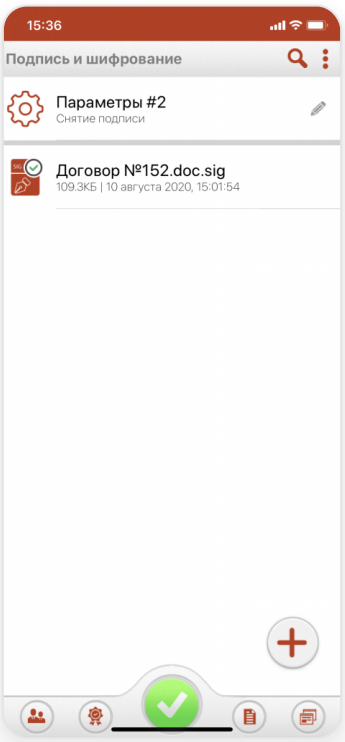


В разделе операции выбрать опцию **Снятие подписи**.

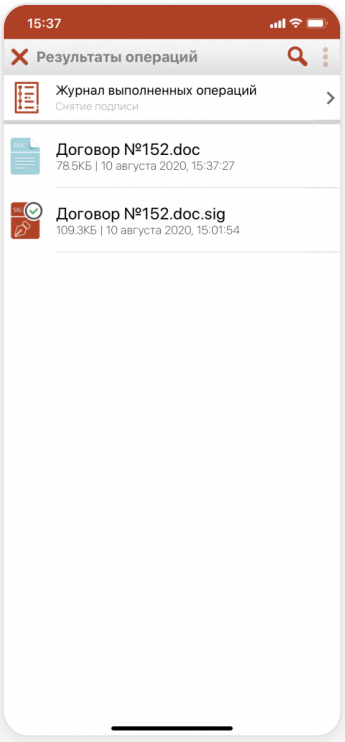


Для сохранения нужно нажать на галочку . Далее в списке Параметров операций выделить параметр и снова нажать на галочку.

Если в Мастере подписи и шифрования добавлены файлы с расширением **.sig** и выбран необходимый параметр, то появится кнопка **Выполнить** . Нажатие на кнопку **Выполнить** запускает процесс снятия подписи.



При снятии подписи у файлов меняется иконка, расширение и дата создания.



У отделенной подписи при выполнении операции снятия подписи возникает сообщение об ошибке.

Открыть статью на сайте

Подпись сертификатом DSS

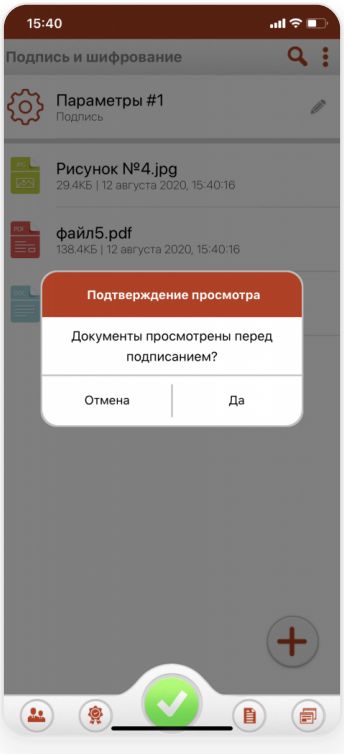
Архив. КриптоАРМ ГОСТ для iOS.

Для того, чтобы подписать файлы сертификатом DSS необходимо выполнить следующие действия:

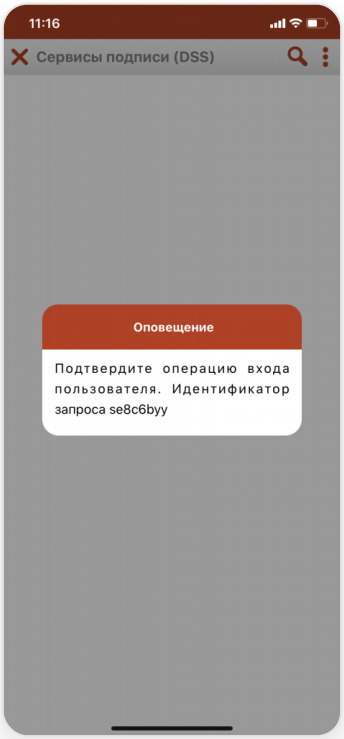
1. В разделе **Личные сертификаты** установить сертификаты из DSS.
2. Добавить файлы в **Мастер подписи и шифрования** для подписи.
3. В настройках **Параметра операции** в блоке **Сертификат подписи** выбрать облачный сертификат DSS.

После выполнения всех действий появится кнопка **Выполнить** . Нажатие на кнопку **Выполнить** запускает процесс подписи.

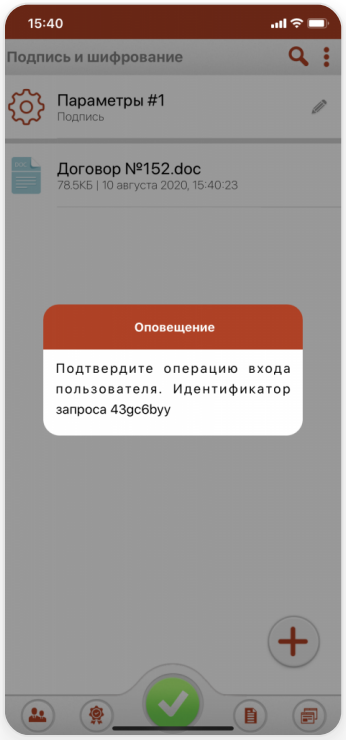
Подписываемые файлы обязательно необходимо просмотреть перед операцией. Далее появляется диалоговое окно с вопросом: «Документы просмотрены перед подписанием?». Если документы просмотрены, то необходимо нажать **Да** и начнется процесс подписи. В противном случае, рекомендуется нажать **Отмена** и просмотреть документы.

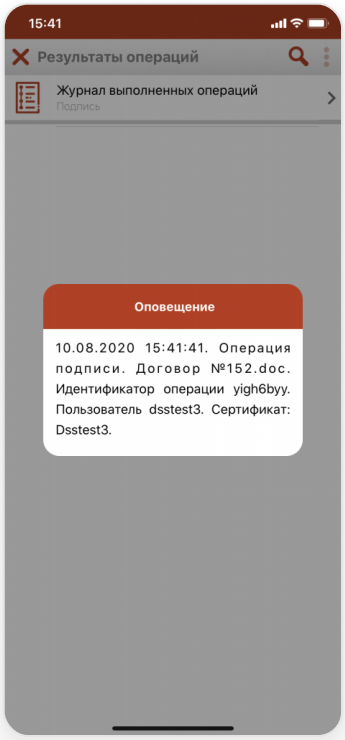


Если у пользователя в личном кабинете DSS в настройках стоит подтверждение аутентификации по SMS, электронной почте или с помощью мобильного приложения, то при нажатии **Да** появляется сообщение, что операцию нужно подтвердить. Если нет, то данный шаг пропускается.

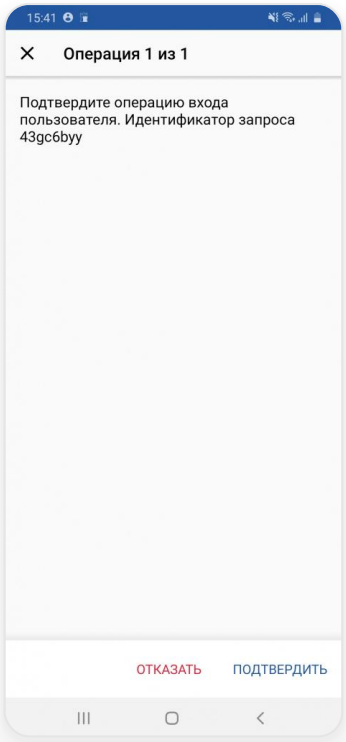


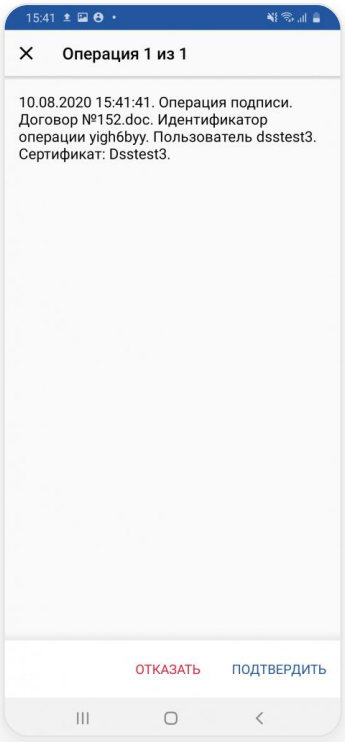
Если в личном кабинете также настроено подтверждение операций по SMS, электронной почте или с помощью мобильного приложения, то появляется сообщение, что операцию нужно подтвердить.





Подтверждение операции входа и подтверждение об операции в приложении myDSS:





При успешной аутентификации и по окончании процесса исходные документы (оригиналы) и результаты операции подписи отображаются в мастере **Результаты операций**.

Открыть статью на сайте

Шифрование файлов

Архив. КриптоАРМ ГОСТ для iOS.

Для того, чтобы зашифровать файлы необходимо:

1. В **Мастер подписи и шифрования** добавить файлы для шифрования.

2. В **Параметрах операций** выбрать/создать шаблон, в котором нужно указать сертификаты шифрования и задать параметры шифрования.

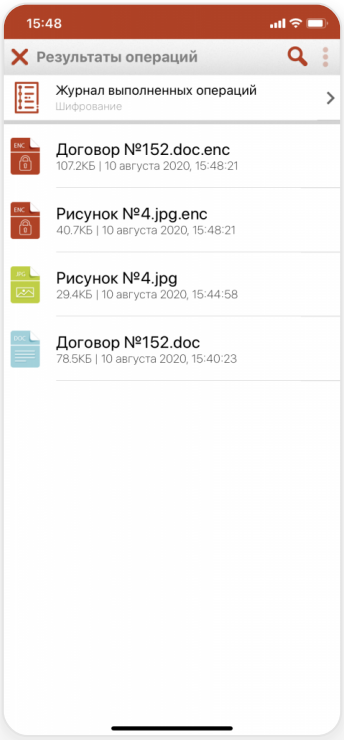
В приложении КриптоАРМ ГОСТ доступно шифрование одного или сразу нескольких файлов.

После выполнения всех условий:

1. Добавлен хотя бы один файл;

2. В настройках параметра операции выбран сертификат шифрования и установлена опция Шифрование файлов (если необходимо только зашифровать файлы, то опция Подпись файлов должна быть не активна); появляется кнопка **Выполнить** . Нажатие на кнопку **Выполнить** запускает процесс шифрования.

По окончании процесса исходные документы (оригиналы) и результаты операций (файлы с расширением **.enc**) отображаются в отдельном мастере **Результаты операций**.

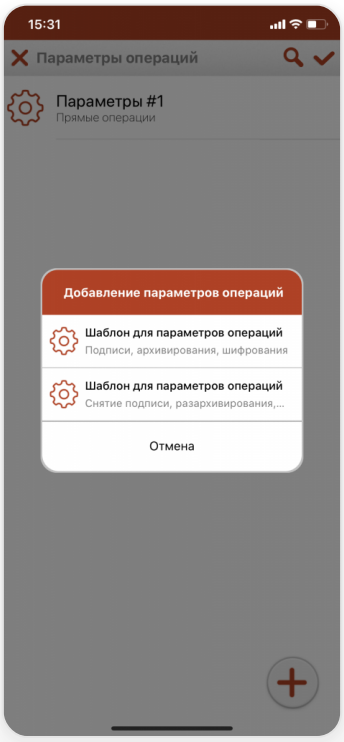

15:48
Результаты операций
Журнал выполненных операций
Шифрование
Договор №152.doc.enc
107.2КБ | 10 августа 2020, 15:48:21
Рисунок №4.jpg.enc
40.7КБ | 10 августа 2020, 15:48:21
Рисунок №4.jpg
29.4КБ | 10 августа 2020, 15:44:58
Договор №152.doc
78.5КБ | 10 августа 2020, 15:40:23

Открыть статью на сайте

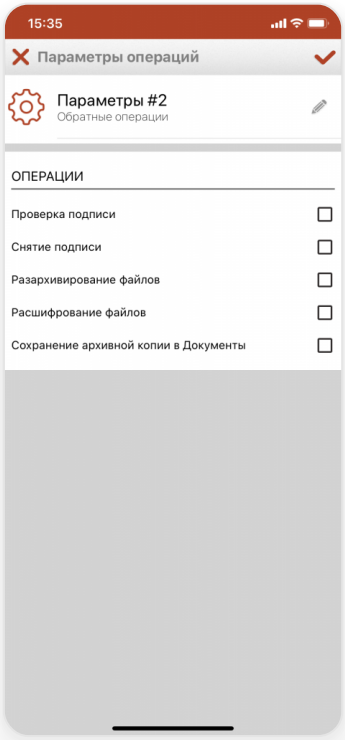
Расшифрование файлов

Архив. КриптоАРМ ГОСТ для iOS.

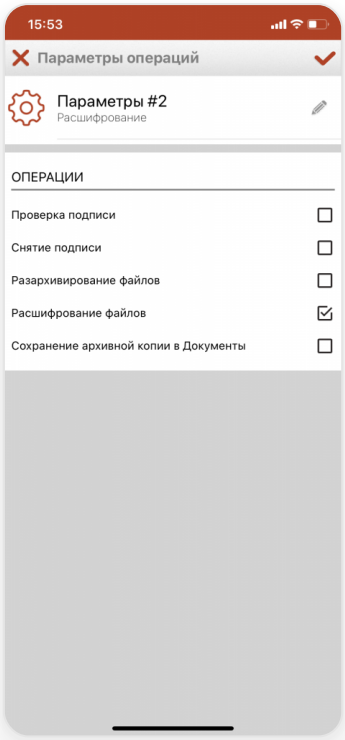
Для расшифрования файлов необходимо создать новый шаблон параметра операции. При добавлении выбрать шаблон «Шаблон для параметров операций (Снятие подписи, разархивирование...)».



Далее после выбора шаблона откроется настройка Параметров операции.



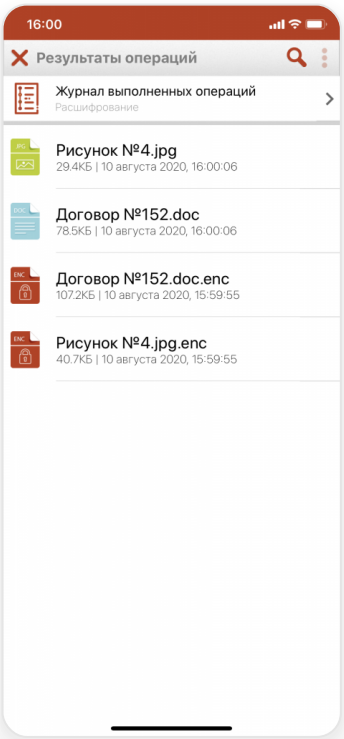
В разделе операции выбрать опцию **Расшифрование файлов**.



Для сохранения нужно нажать на галочку . Далее в списке Параметров операций выделить параметр и снова нажать на галочку.
Если в Мастере подписи и шифрования добавлены файлы с расширением **.enc** и выбран

необходимый параметр, то появится кнопка **Выполнить** . Нажатие на кнопку **Выполнить** запускает процесс расшифрования файла.

При расшифровании у файлов меняется иконка, расширение и дата создания.



Открыть статью на сайте

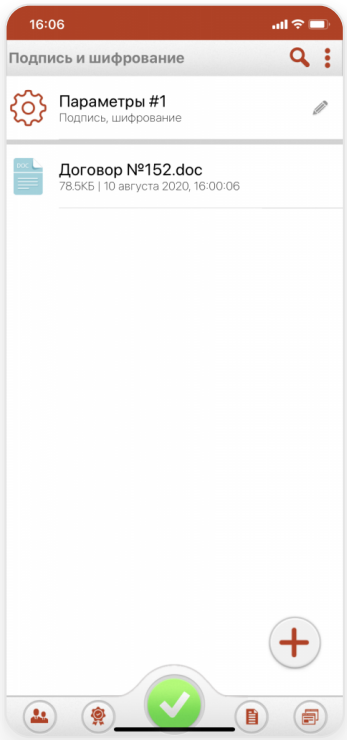
Подпись и шифрование

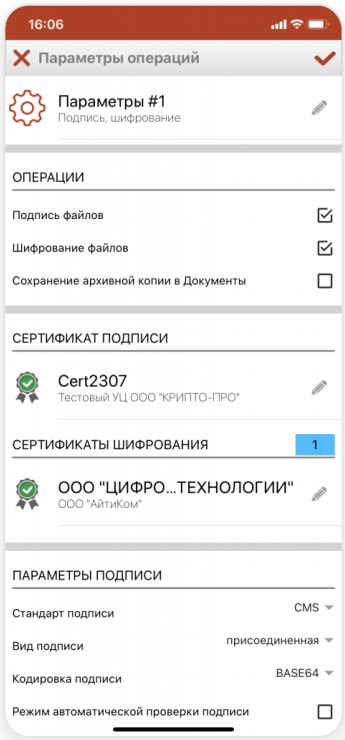
Архив. КриптоАРМ ГОСТ для iOS.

Для подписи и шифрования файлов нужно:

1. В мастере **Подпись и шифрование** добавить файлы;

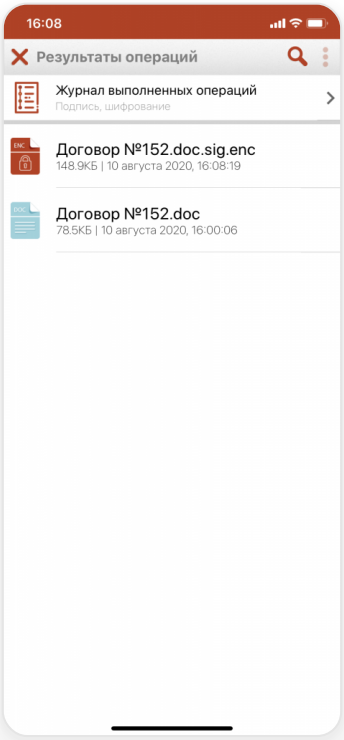
2. В настройках **Параметры операции** выбрать опции Подпись файла и Шифрование файла, задать Сертификаты подписи и Сертификаты шифрования.





После выполнения всех условий появляется кнопка **Выполнить** . Нажатие на кнопку **Выполнить** запускает процесс. Сначала файл подписывается, затем следует процесс шифрования.

По окончании процесса исходные документы (оригиналы) и результаты операций (файлы с расширением **.sig.enc**) отображаются в отдельном мастере **Результаты операций**.


16:08
Результаты операций
Журнал выполненных операций
Подпись, шифрование
Договор №152.doc.sig.enc
148.9КБ | 10 августа 2020, 16:08:19
Договор №152.doc
78.5КБ | 10 августа 2020, 16:00:06

Открыть статью на сайте

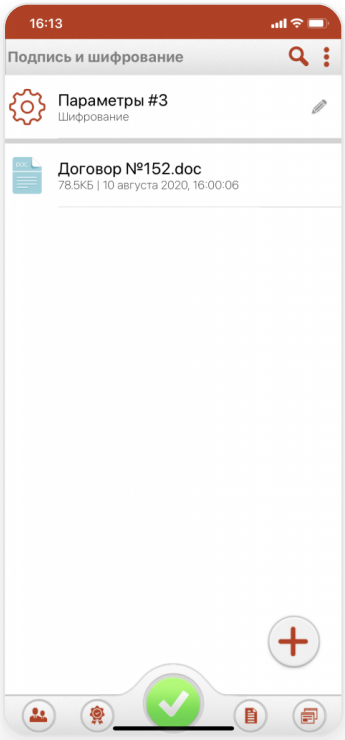
Шифрование и архивирование

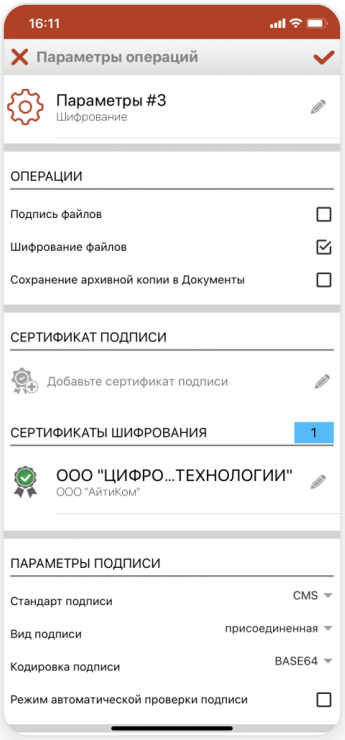
Архив. КриптоАРМ ГОСТ для iOS.

Для шифрования и архивирования файлов нужно:

1. В мастере **Подпись и шифрование** добавить файлы;

2. В настройках **Параметры операции** выбрать опции Шифрование файла, задать Сертификаты шифрования и настроить Параметры шифрования (выбрать опцию Архивировать файлы перед шифрованием).

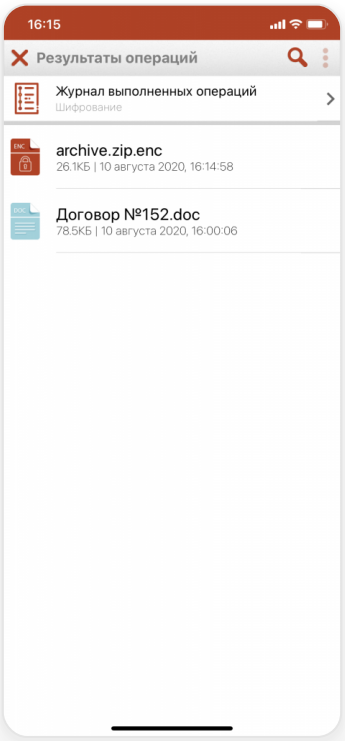






После выполнения всех условий появляется кнопка **Выполнить** . Нажатие на кнопку Выполнить запускает процесс. Сначала файл архивируется, затем следует процесс шифрования.

По окончании процесса исходные документы (оригиналы) и результаты операций (файлы с расширением **.zip.enc**) отображаются в отдельном мастере **Результаты операций**.



Открыть статью на сайте

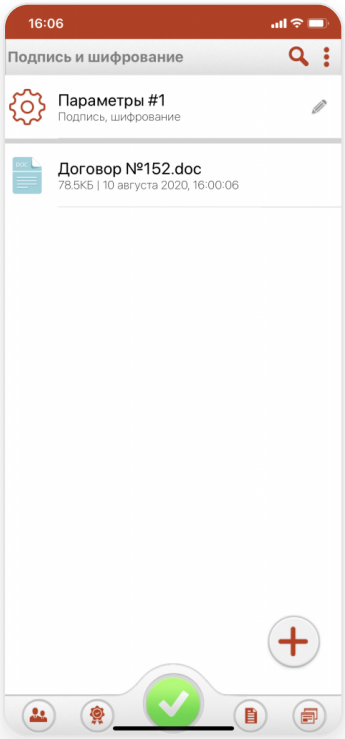
Подпись, шифрование и архивирование

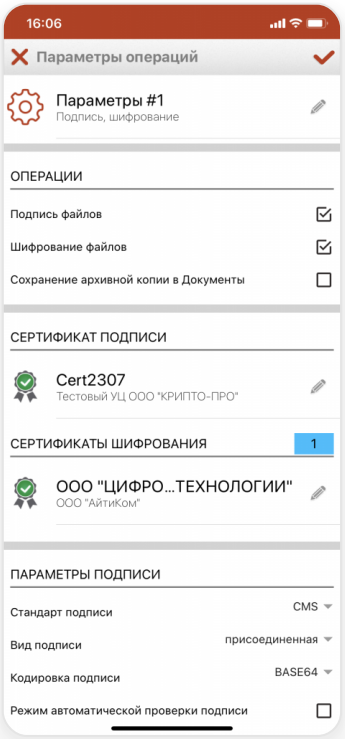
Архив. КриптоАРМ ГОСТ для iOS.

Для подписи и шифрования файлов нужно:

1. В мастере **Подпись и шифрование** добавить файлы;

2. В настройках **Параметры операции** выбрать опции Подпись файла и Шифрование файла, задать Сертификаты подписи и Сертификаты шифрования, настроить Параметры шифрования.

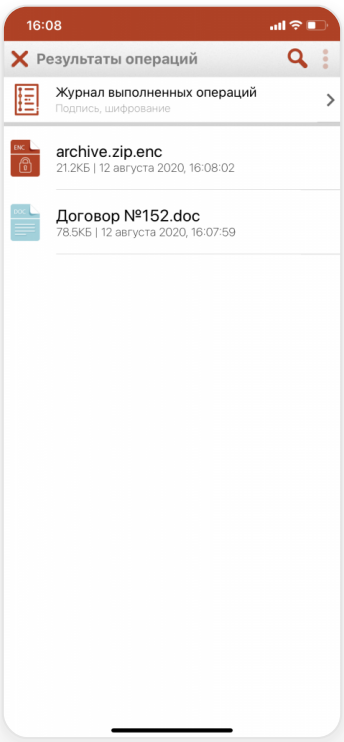






После выполнения всех условий появляется кнопка **Выполнить** . Нажатие на кнопку **Выполнить** запускает процесс. Сначала файл подписывается, архивируется, затем следует процесс шифрования.

По окончании процесса исходные документы (оригиналы) и результаты операций (файлы с расширением **.zip.enc**) отображаются в отдельном мастере **Результаты операций**.



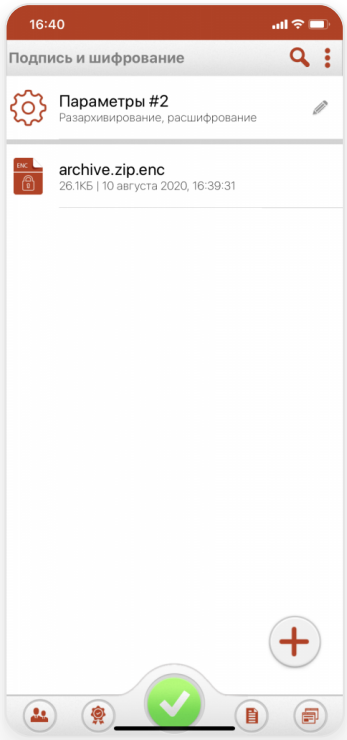
Открыть статью на сайте

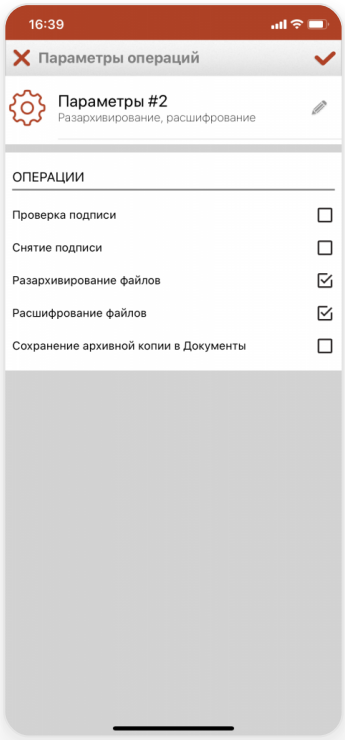
Расшифрование и разархивирование файлов

Архив. КриптоАРМ ГОСТ для iOS.

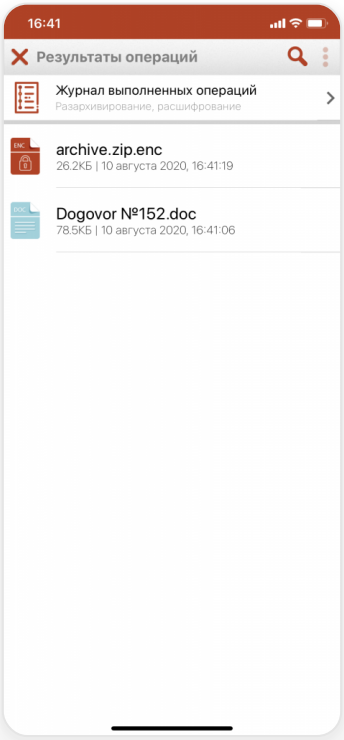
Для расшифрования и разархивирования нужно:

1. Выбрать зашифрованные архивы (файлы с расширением **.zip.enc**) и добавить в мастер Подписи и шифрования.
2. В **Параметрах операций** создать второй шаблон и в операциях выбрать опции Расшифрование файлов и Разархивирование файлов.
3. Нажать на кнопку **Выполнить**.





Исходные зашифрованные и полученные файлы отображаются в отдельном мастере **Результаты операций**.


16:41
Результаты операций
Журнал выполненных операций
Разархивирование, расшифрование
archive.zip.enc
26.2КБ | 10 августа 2020, 16:41:19
Dogovor №152.doc
78.5КБ | 10 августа 2020, 16:41:06

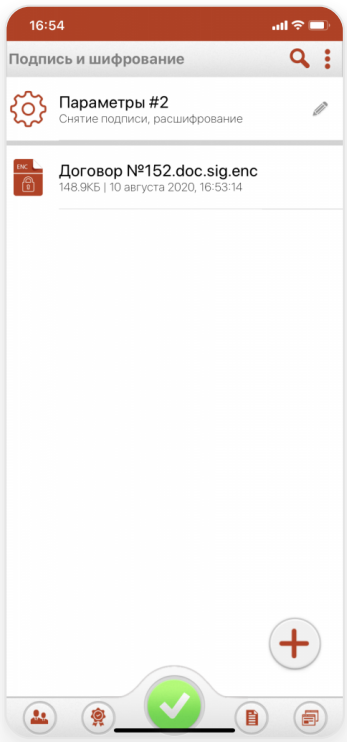
Открыть статью на сайте

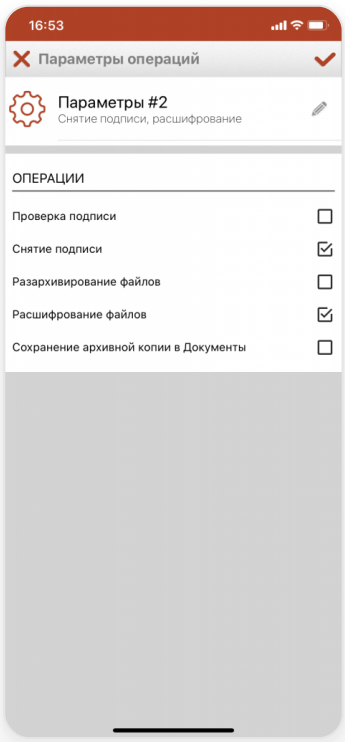
Расшифрование и снятие подписи

Архив. КриптоАРМ ГОСТ для iOS.

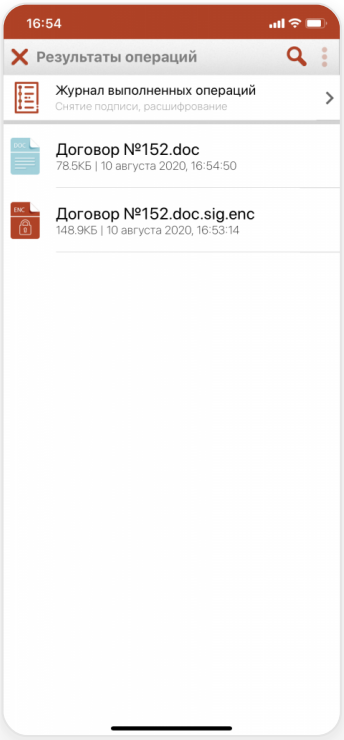
Для расшифрования и снятия подписи нужно:

1. Выбрать подписанный и зашифрованный файл (файлы с расширением **.sig.enc**) и добавить в мастер Подписи и шифрования.
2. В **Параметрах операций** создать второй шаблон и в операциях выбрать опции Расшифрование файлов и Снятие подписи.
3. Нажать на кнопку **Выполнить**.





Исходные файлы и полученные файлы отображаются в отдельном мастере **Результаты операций**.


16:54
Результаты операций
Журнал выполненных операций
Снятие подписи, расшифрование
Договор №152.doc
78.5КБ | 10 августа 2020, 16:54:50
Договор №152.doc.sig.enc
148.9КБ | 10 августа 2020, 16:53:14

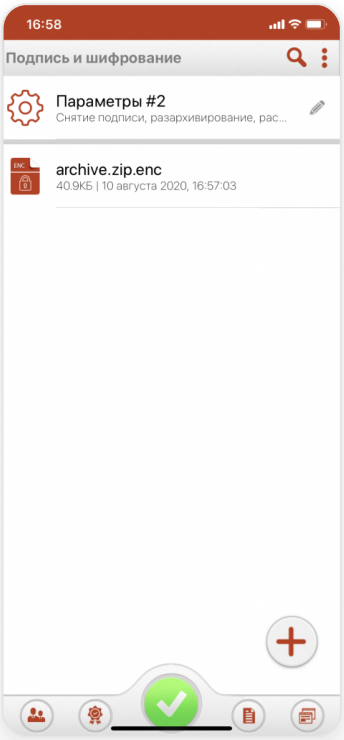
Открыть статью на сайте

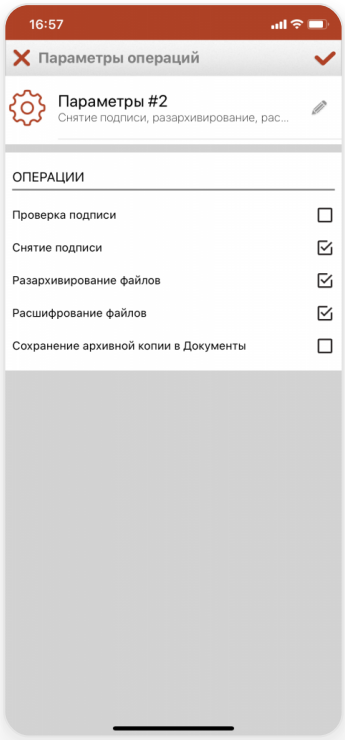
Расшифрование, разархивирование и снятие подписи

Архив. КриптоАРМ ГОСТ для iOS.

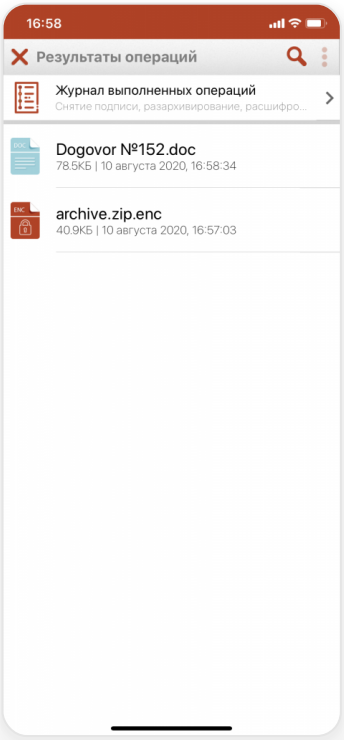
Для расшифрования и снятия подписи нужно:

1. Выбрать зашифрованный архив с подписанным файлом (файлы с расширением **.zip.enc**) и добавить в мастер Подписи и шифрования.
2. В **Параметрах операций** создать второй шаблон и в операциях выбрать опции Снятие подписи, Разархивирование файлов, Расшифрование файлов.
3. Нажать на кнопку **Выполнить**.





Исходные файлы и полученные файлы отображаются в отдельном мастере **Результаты операций**.

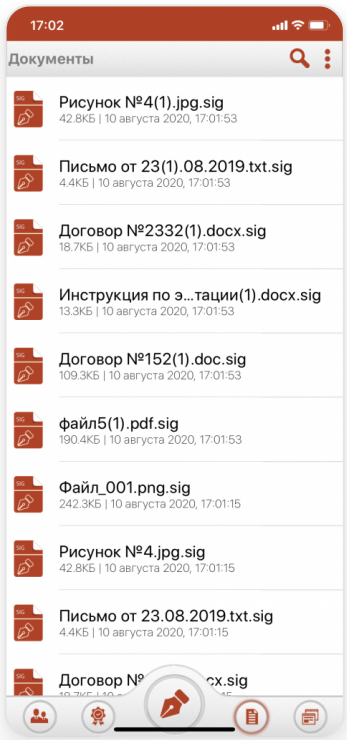

16:58
Результаты операций
Журнал выполненных операций
Снятие подписи, разархивирование, расшифро...
Dogovor №152.doc
78.5КБ | 10 августа 2020, 16:58:34
archive.zip.enc
40.9КБ | 10 августа 2020, 16:57:03

Открыть статью на сайте

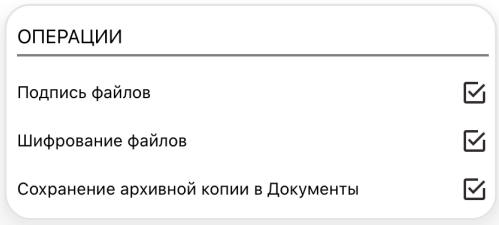
Документы

Архив. КриптоАРМ ГОСТ для iOS.

По нажатию на кнопку открывается раздел **Документы**.



Документы – это список файлов из предустановленного каталога приложения, куда сохраняются результаты операций - подписанные и зашифрованные документы, при включении режима **Сохранение архивной копии в Документы** в параметрах операций.



В разделе **Документы** нельзя выполнять какие-либо операции по подписи и шифрованию, добавление в него файлов, минуя Мастер подписи и шифрования. Среди автоматически выполняемых операций – это проверка подписи под документами.

Все файлы раздела можно передать в мастер подписи и шифрования для выполнения операций. Операции в разделе **Документы**, доступные при выделении подписанного файла, представлены в таблице:

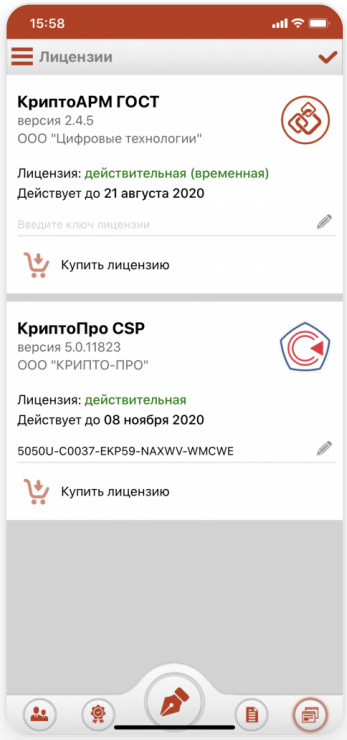
Операция	**Описание**
 Просмотреть документ	Просмотр документа. Доступно при выделении одного документа.
 Копировать в мастер подписи	Выбранный документ передается в мастер подписи и шифрования для выполнения операций.
 Отправить	Данная операция осуществляет передачу выбранного документа любому приложению из отображаемого списка для последующей обработки.
 Удалить	Операция позволяет удалить выбранный документ из текущего списка.
 Выделить все	Происходит выделение всех элементов списка документов.
 Снять выделение	При выборе операции выделение с документов сбрасывается.

Открыть статью на сайте

Лицензии

Архив. КриптоАРМ ГОСТ для iOS.

Раздел **Лицензии** предназначен для установки лицензий на приложение КриптоАРМ ГОСТ и КриптоПРО CSP.



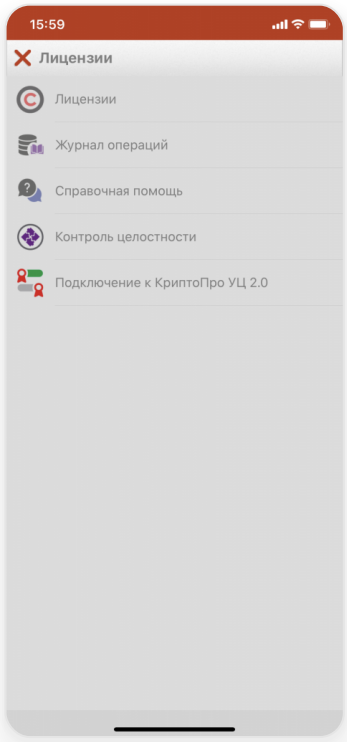
При установке приложения доступны временные тестовые лицензии: на КриптоАРМ ГОСТ на 14 дней, на КриптоПро CSP на 3 месяца.

Без лицензии на приложение КриптоАРМ ГОСТ доступна только операция проверки подписи. Для выполнения операций подписи, шифрования, расшифрования и генерации сертификата должна быть установлена лицензия на приложение.

Без лицензии на КриптоПро CSP доступны операции проверки подписи, шифрования. Для выполнения операций подписи, шифрования, расшифрования и генерации сертификата должна быть установлена лицензия КриптоПро CSP.

При нажатии на в разделе **Лицензии** открывается меню со следующими пунктами:

- **Лицензии** – возврат в компонент Лицензии;
- **Журнал операций** – для отображения выполняемых операций в приложении;
- **Справочная помощь** – для открытия полного руководства пользователя приложения;
- **Контроль целостности** – для проверки целостности приложения;
- **Подключение к КриптоПро УЦ 2.0** – для подключения к КриптоПро УЦ 2.0.

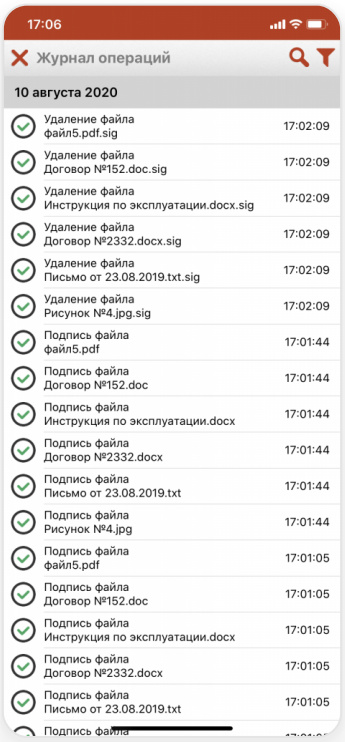


Открыть статью на сайте

Журнал операций

Архив. КриптоАРМ ГОСТ для iOS.

Журнал операций предназначен для отображения операций, выполняемых пользователем.

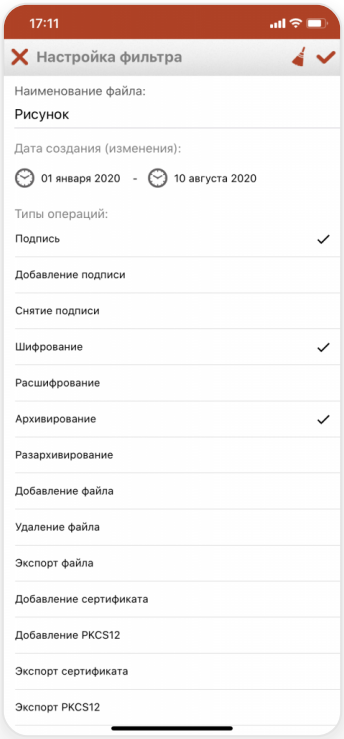


В журнале отображаются следующие типы операций:

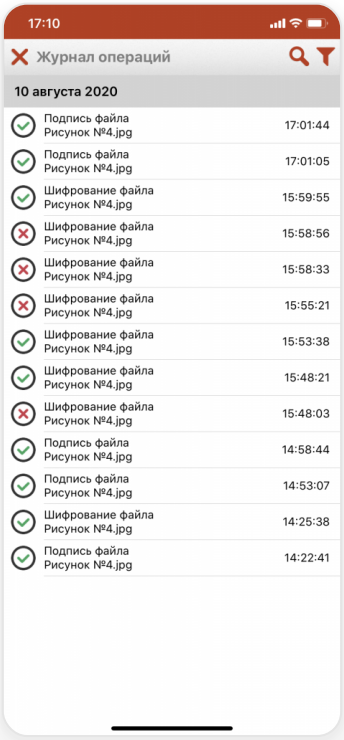
- добавление подписи;
- снятие подписи;
- шифрование;
- расшифрование;
- архивирование;
- разархивирование;
- добавление файла;
- удаление файла;
- экспорт файла;
- добавление сертификата;
- добавление pkcs12;
- удаление сертификата;
- генерация сертификата;
- генерация запроса;
- экспорт запроса;

- удаление запроса;
- установка сертификата;
- удаление контейнера;
- установка crl;
- удаление crl.

Для записей в журнале операций предусмотрена фильтрация.



Применение фильтрации выполняется по кнопке . В зависимости от выставленных критериев фильтра в журнале остаются только те записи, которые удовлетворяют (суммарно) этим критериям. Для сброса фильтра используется кнопка сброса  на форме настроек фильтрации.


17:10
Журнал операций
10 августа 2020
Подпись файла Рисунок №4.jpg 17:01:44
Подпись файла Рисунок №4.jpg 17:01:05
Шифрование файла Рисунок №4.jpg 15:59:55
Шифрование файла Рисунок №4.jpg 15:58:56
Шифрование файла Рисунок №4.jpg 15:58:33
Шифрование файла Рисунок №4.jpg 15:55:21
Шифрование файла Рисунок №4.jpg 15:53:38
Шифрование файла Рисунок №4.jpg 15:48:21
Шифрование файла Рисунок №4.jpg 15:48:03
Подпись файла Рисунок №4.jpg 14:58:44
Подпись файла Рисунок №4.jpg 14:53:07
Шифрование файла Рисунок №4.jpg 14:25:38
Подпись файла Рисунок №4.jpg 14:22:41

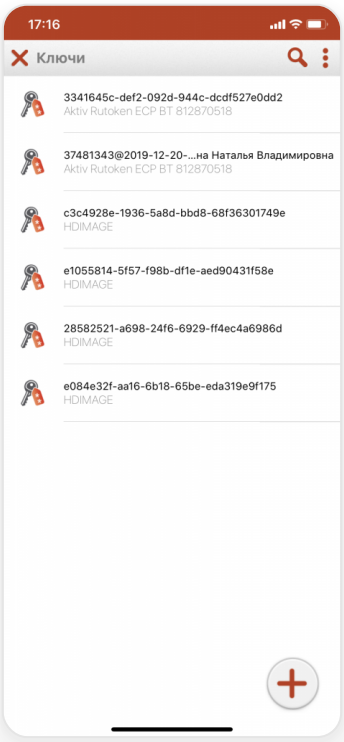
Открыть статью на сайте

Подключение Рутокен

Архив. КриптоАРМ ГОСТ для iOS.

В первую очередь необходимо подключить Рутокен ЭЦП Bluetooth к телефону. Для этого необходимо включить Bluetooth на обоих устройствах, дождаться обнаружения Рутокен и установить соединение.

Следующим шагом необходимо запустить приложение КриптоАРМ ГОСТ и убедиться, что Рутокен начал мигать (это значит, что приложение считывает ключи). Нужно дождаться окончания мигания индикатора и убедиться, что в разделе **Контейнеры** появились закрытые ключи.



Если же КриптоАРМ уже запущен, то в Контейнерах необходимо нажать на **Обновить список ключей** в контекстном меню.

Для того, чтобы сертификат отобразился в разделе Личные сертификаты, необходимо выделить нужный ключ и вызвать контекстное меню в Контейнерах, далее нажать на **Установить сертификат**. Если в контейнере есть сертификат, то он отобразится в разделе Личные сертификаты. Сертификат готов к использованию.