

АО «СИГНАЛ-КОМ»

УТВЕРЖДЕН

ШКНР.00051-01 34 05-ЛУ

ПРОГРАММНО-АППАРАТНЫЙ КОМПЛЕКС

SIGNAL-COM MOBILE DSS

Версия 1.0

Руководство пользователя

ШКНР.00051-01 34 05

Листов 24

АННОТАЦИЯ

Настоящий документ содержит руководство пользователя для мобильного приложения «MobileDSS» для ОС Android.

СОДЕРЖАНИЕ

Аннотация	2
Содержание	3
Назначение программы	4
1.1. Общие сведения	4
1.1. Список сокращений	4
1.2. Термины и определения	4
1.3. Технические характеристики	5
2. Условия выполнения программы	6
2.1. Требования к окружению	6
2.1.1. Мобильное приложение	6
2.2. Установка и удаление «MobileDSS» на ОС Android	6
2.2.1. Установка мобильного приложения	6
2.2.2. Удаление мобильного приложения	6
2.2.3. Обновление мобильного приложения	7
3. Выполнение программы	8
3.1. Использование мобильного приложения «MobileDSS»	8
3.1.1. Язык интерфейса мобильного приложения	8
3.1.2. Первый запуск мобильного приложения «MobileDSS»	8
3.1.3. Запуск мобильного приложения «MobileDSS»	11
3.1.4. Общие принципы работы с приложением «MobileDSS»	12
3.1.5. Главное меню	14
3.1.6. Меню «Настройки»	20
4. Сообщения оператору	22
4.1. Сообщения в мобильном приложении «MobileDSS»	22
Литература	24

НАЗНАЧЕНИЕ ПРОГРАММЫ

1.1. Общие сведения

Мобильное приложение «MobileDSS» предназначено для подтверждения электронных транзакций в информационных системах, для чего мобильное приложение сохраняет и использует ключи электронной подписи в неэкспортируемом зашифрованном виде. Также мобильное приложение позволяет визуализировать данные при подтверждении электронных транзакций обеспечивает недоказуемость от подтверждённых операций.

Мобильное приложение «MobileDSS» используется в системе «облачной» электронной подписи Signal-COM Cloud DSS.

1.1. Список сокращений

В настоящем руководстве используются следующие сокращения:

ДСЧ – датчик случайных чисел;

ОС – операционная система;

ПК – персональный компьютер;

ПО – программное обеспечение;

УЦ – удостоверяющий центр;

ЭП – электронная подпись;

API – Application Programming Interface;

APK – Android Package;

DMG – Apple Disk Image;

IEEE – Institute of Electrical and Electronics Engineers;

PKCS – Public-Key Cryptography Standards;

QR – Quick Response (Code).

1.2. Термины и определения

В настоящем руководстве используются следующие термины:

- 1) ключи – пары ключей проверки электронной подписи и ключей электронной подписи;
- 2) мобильное приложение – приложение MobileDSS, установленное на мобильном устройстве пользователя;
- 3) уровень API – целочисленное значение, однозначно идентифицирующее версию API, предлагаемую платформой Android;
- 4) Android – мобильная ОС компании Google;

- 5) APK – формат файла, используемый операционной системой Android для распространения и установки мобильных приложений;
- 6) MacOS – ОС компании Apple;
- 7) PUSH-уведомление – короткое всплывающее сообщение на устройстве, отображающее информацию для пользователя мобильного приложения.
- 8) QR-код – матричный двумерный штрихкод с закодированной информацией;
- 9) Windows – ОС компании Microsoft;
- 10) Wi-Fi – технология беспроводной локальной сети с устройствами на основе стандартов IEEE 802.11.

1.3. Технические характеристики

Мобильное приложение «MobileDSS» (исполнение 1) поставляется для следующих операционных систем (при условии их поддержки производителем):

- Android 4.4/5.0/5.1/6.0/7.0/7.1/8.0/8.1/9/10/11/12/13/14 (ARM, ARM64, x86, x86_64).

Примечание. В скобках указаны аппаратные платформы

Перечисленные ОС для мобильного приложения «MobileDSS» должны обладать следующими характеристиками:

- оперативная память объемом не менее 1 Гб;
- внутренний накопитель с объемом свободного пространства не менее 100 Мб.

В мобильном приложении «MobileDSS» поддерживаются следующие криптографические алгоритмы и схемы:

- алгоритм хэширования ГОСТ Р 34.11-2012 [1];
- программный датчик случайных чисел.

Реализации перечисленных выше алгоритмов выполнены в соответствии с рекомендациями ТК 26 [2].

Мобильное приложение позволяет просматривать подробную информацию о ключах электронной подписи, хранящихся в зашифрованном ключевом контейнере.

2. УСЛОВИЯ ВЫПОЛНЕНИЯ ПРОГРАММЫ

2.1. Требования к окружению

2.1.1. Мобильное приложение

Мобильное приложение «MobileDSS» (исполнение 1) поставляется для следующих операционных систем (при условии их поддержки производителем):

- Android 4.4/5.0/5.1/6.0/7.0/7.1/8.0/8.1/9/10/11/12/13/14 (ARM, ARM64, x86, x86_64).

Примечание. В скобках указаны аппаратные платформы.

Перечисленные ОС для мобильного приложения «MobileDSS» должны обладать следующими характеристиками:

- оперативная память объемом не менее 1 Гб;
- внутренний накопитель с объемом свободного пространства не менее 100 Мб.

Также мобильное приложение должно иметь доступ к интернету для получения ключей по QR коду, а также для подтверждения транзакций.

Для корректной инициализации биологического датчика случайных чисел в мобильном приложении (см. п. 3.1.2.2) разрешение дисплея мобильного устройства и размер окна, развернутого на весь экран, должно быть не меньше 2265×1080 пикселей.

2.2. Установка и удаление «MobileDSS» на ОС Android

2.2.1. Установка мобильного приложения

Порядок установки мобильного приложения «[MobileDSS](#)» из магазина приложений Google Play (Play Маркет) следующий:

1. открыть приложение Google Play (Play Маркет);
2. в строке поиска приложений ввести «MobileDSS»;
3. выбрать приложение разработчика «Signal-COM»;
4. нажать кнопку «Установить».

2.2.2. Удаление мобильного приложения

Порядок удаления мобильного приложения «MobileDSS» на устройстве с ОС Android следующий:

1. открыть меню устройства;
2. выбрать пункт «Настройки»;
3. выбрать пункт «Приложения» или «Диспетчер приложений»;
4. выбрать пункт «Показать все приложения», если он есть на вашем устройстве;
5. найти приложение «MobileDSS»;

6. нажмите кнопку «Удалить».

Примечание: названия пунктов меню в процессе удаления приложения могут отличаться на различных устройствах на базе ОС Android, используйте инструкции и этапы по удалению приложений из информации от производителя вашего устройства.

При удалении приложения также удаляются все данные, хранящиеся в приложении, в том числе ключи электронной подписи.

2.2.3. Обновление мобильного приложения

Порядок обновления мобильного приложения «[MobileDSS](#)» из магазина приложений Google Play (Play Маркет) следующий:

1. открыть приложение Google Play (Play Маркет);
2. в строке поиска приложений ввести «MobileDSS»;
3. выбрать приложение разработчика «Signal-COM»;
4. нажать кнопку «Обновить».

3. ВЫПОЛНЕНИЕ ПРОГРАММЫ

3.1. Использование мобильного приложения «MobileDSS»

3.1.1. Язык интерфейса мобильного приложения

Язык интерфейса мобильного приложения определяется в зависимости от используемого основного языка в ОС. Если основным языком в ОС – русский, то язык интерфейса мобильного приложения будет так же на русском, если язык системы другой, то язык интерфейса мобильного приложения будет на английском языке. Далее все примеры будут для русского языка интерфейса.

3.1.2. Первый запуск мобильного приложения «MobileDSS»

3.1.2.1 Требования к паролю

При первом запуске мобильного приложения «MobileDSS» на устройстве смартфона/планшета необходимо задать пароль (см. Рисунок 1), удовлетворяющий следующим требованиям:

1. длина пароля должна быть не менее 6 символов;
2. в числе символов пароля обязательно должны присутствовать буквы в верхнем и нижнем регистрах, цифры и специальные символы (@, #, \$, &, *, % и т.п.);
3. пароль не должен включать в себя легко вычисляемые сочетания символов (имена, фамилии и т.д.), а также общепринятые сокращения (USER, ADMIN и т.д.);
4. при смене пароля новое значение должно отличаться от предыдущего не менее чем в 4-х позициях;
5. личный пароль пользователь не имеет права сообщать никому;
6. периодичность смены пароля определяется принятой политикой безопасности, но не должна превышать 6 месяцев.

MTS RUS 46 % 22:26

Создание Ключевого Контейнера

Пароль должен содержать не менее:

- ☐ 6 символов;
- ☐ 1 цифры;
- ☐ 1 буквы в верхнем регистре;
- ☐ 1 буквы в нижнем регистре;
- ☐ 1 специального символа (+, -, % и т.п.).

Запомните пароль!
Его нельзя восстановить!

Введите новый пароль

Введите пароль повторно

УСТАНОВИТЬ ПАРОЛЬ

Navigation icons: back, home, recent apps

Рисунок 1 Экран установки пароля при первом запуске приложения

3.1.2.2 Инициализация датчика случайных чисел (ДСЧ)

После задания пароля, потребуется проинициализировать ДСЧ, для этого нужно нажимать (касаясь сенсорного экрана) на круги оранжевого цвета, пока прогресс инициализации ДСЧ не завершится (см. Рисунок 2).



Рисунок 2 Экран инициализации ДСЧ

3.1.3. Запуск мобильного приложения «MobileDSS»

Если пароль в мобильном приложении был установлен, а биологический датчик случайных чисел был инициализирован, то при последующих запусках приложения пользователь должен будет ввести пароль, установленный ранее, чтобы войти в приложение (см. Рисунок 3).

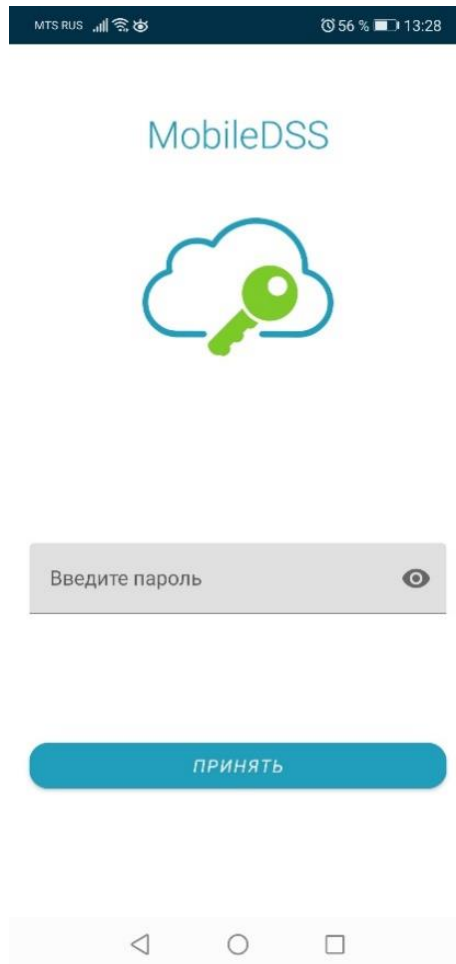


Рисунок 3 Экран ввода пароля для входа в приложение

При входе в приложение даётся 10 попыток для корректного ввода пароля, независимо от перезапуска мобильного приложения. После исчерпания всех попыток, приложение заблокирует доступ к вводу пароля на 10 минут (см. Рисунок 4). После истечения данного времени, будет снова доступно 10 попыток для ввода пароля.

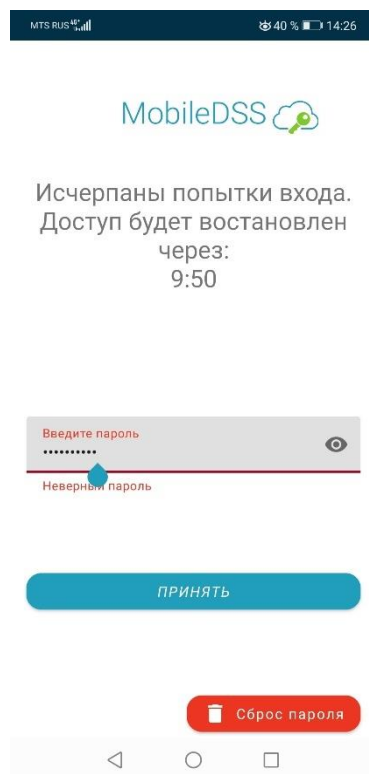


Рисунок 4 Предупреждение об исчерпании всех попыток для входа в приложение и кнопка сброса пароля

3.1.4. Общие принципы работы с приложением «MobileDSS»

3.1.4.1 Сброс пароля

В случае, если пароль от мобильного приложения был забыт или утерян, существует возможность его сбросить. При этом удаляются все данные (ключи и ключевой контейнер, зашифрованный на пароле).

Для сброса пароля нужно потратить все попытки на его ввод (см. п. 3.1.3), после чего появится кнопка сброса (см. Рисунок 4).

3.1.4.2 Требования к изменению пароля

Если при входе в приложение пароль был введен верно, откроется экран главного меню приложения (см. Рисунок 5).

Если пользователь не менял пароль более 5 месяцев, то при запуске приложения будет выводиться предупреждение о необходимости смены пароля (см. Рисунок 5). Пользователь может либо отказаться, либо перейти к смене пароля.

Если пользователь не менял пароль больше 6 месяцев, то при запуске приложения будет выводиться предупреждение об обязательной смене пароля (см. Рисунок 5). Работа мобильного приложения будет заблокирована, пока пользователь не сменит пароль на новый.

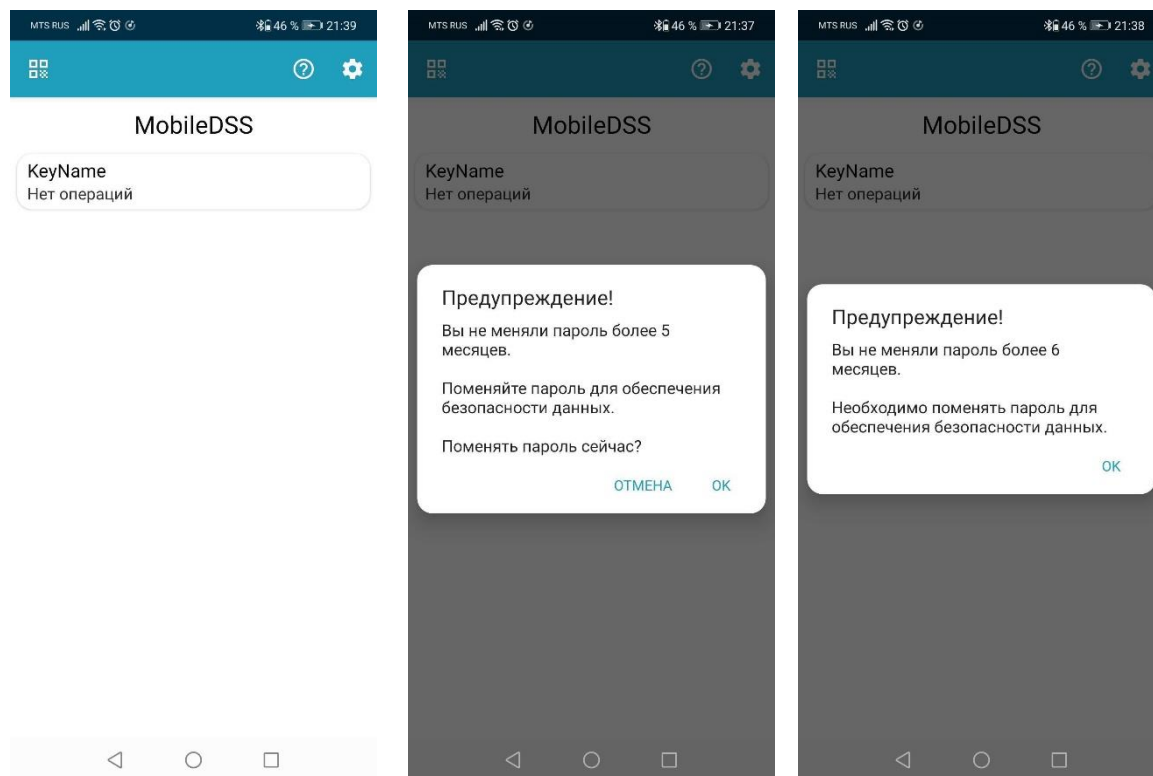


Рисунок 5 Экран главного меню приложения и экран с предупреждением о необходимости смены пароля

Если с момента последней активности с приложением «MobileDSS» прошло больше заданного времени, то произойдёт таймаут работы, то есть запрос повторного ввода пароля, как при запуске приложения (см. п. 3.1.3).

3.1.5. Главное меню

В главном меню отображаются добавленные в приложение ключи для подтверждения операций, кнопка перехода к подтверждению/отклонению операций для этих ключей и количество доступных для подтверждения операций для конкретного ключа. В правом верхнем углу находится кнопка перехода к меню «Настройки» и кнопка «Помощь», описывающая возможности данного меню. В левом верхнем углу находится кнопка для добавления новых ключей с помощью камеры.



Рисунок 6 Экран с главным меню

3.1.5.1 Добавление ключей в мобильное приложение

Если в приложении не было добавлено ни одного ключа для подтверждения операций, нужно нажать на кнопку сканировать QR-код, если в приложение уже были добавлены ключи нужно нажать на кнопку в левом верхнем углу.

ШКНР.00051-01 34 05



Добро пожаловать в MobileDSS

Для начала работы отсканируйте
QR-код с ключевой информацией



Рисунок 7 Экран с главным меню до добавления первого ключа

Для сканирования QR с ключом для подтверждения операций мобильному приложению понадобится доступ к камере смартфона. Необходимо предоставить доступ к камере, иначе дальнейшая работа с приложением не будет возможна. Камера в приложении «MobileDSS» используется только для сканирования QR с ключом.

После сканирования QR с ключом нужно задать ключу имя, которое будет использоваться для отображения в приложении «MobileDSS» (имя ключа можно будет впоследствии поменять):

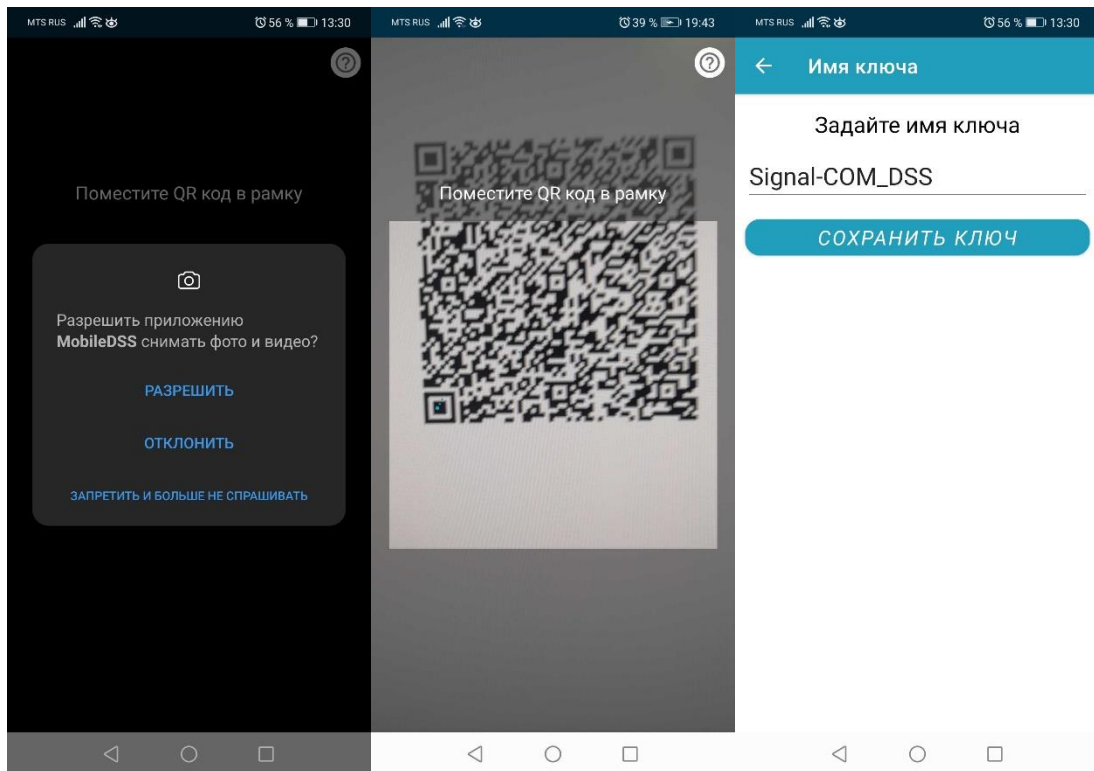


Рисунок 8 Экраны сканирования QR кода

Далее произойдёт обращение к серверу для загрузки ключа. Для этого на устройстве должен быть активирован доступ к интернет-сети. Если запрос к серверу прошёл без ошибок, ключ будет сохранён на устройстве.

3.1.5.1.1 Получение QR кода

QR код для добавления ключа для подтверждения операций можно получить у оператора системы.

3.1.5.2 Информация о ключе

Для получения информации о конкретном ключе нужно нажать на отображение соответствующего ключа:

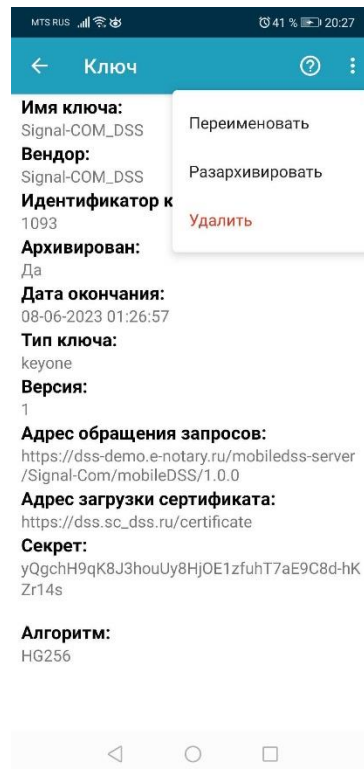


Рисунок 9 Экран с информацией о ключе

В правом верхнем углу данного меню, при нажатии на кнопку «⋮» откроется окно с доступными действиями для ключа. Ключ можно переименовать, архивировать (см. п. 3.1.5.2.1) и удалить (см. п. 3.1.5.2.2).

3.1.5.2.1 Архивирование ключей

Чтобы архивировать ключ, нужно в меню «Информация о ключе» нажать в правый верхний угол (см. п. 3.1.5.2) и выбрать «Архивировать».

Ключ при архивировании попадает в архив, который можно посмотреть в меню «Настройки». Особенности архивированных ключей:

- архивированный ключ не удаляется с устройства;
- для архивированных ключей не приходят PUSH-уведомления о подтверждении операций;
- для архивированных ключей могут приходить PUSH-уведомления со справочной информацией;
- архивированные ключи можно разархивировать (то есть они снова будут отображаться на главном экране), переименовать или удалить с устройства.

Архивировать ключ можно, например, если для ключа истёк срок действия и он занимает место на главном экране, но удалять его пока нет необходимости.

3.1.5.2.2 Удаление ключей

Чтобы удалить ключ нужно в меню «Информация о ключе» нажать в правый верхний угол (см. п. 3.1.5.2) и выбрать «Удалить».

Удалённый ключ окончательно удаляется с устройства. Его можно заново загрузить в приложение с помощью QR-кода (см. п. 3.1.5.1).

3.1.5.3 Срок действия ключей

У ключей для подтверждения операций существует срок действия, дату окончания которого можно посмотреть в информации о ключе (см. п. 3.1.5.2). Если у ключа истек срок действия, то на главном экране появляется соответствующее предупреждение:

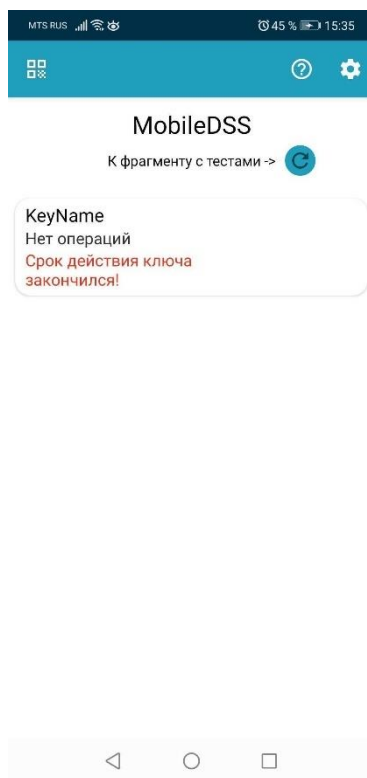


Рисунок 10 Ключ с истёкшим сроком действия

3.1.5.4 Подтверждение операции(й)

Когда в системе появляется операция для подтверждения, в мобильное приложение «MobileDSS» направляется PUSH-уведомление.

Если приложение не было запущено, то PUSH-уведомление отображается и, при нажатии на него, происходит вход в приложение и загрузка подробных данных о соответствующей операции. Для получения PUSH-уведомления и для загрузки подробных данных об операции на смартфоне должно быть активировано интернет-соединение.

Если приложение было запущено, то подробные данные о соответствующей операции загружаются автоматически.

Для подтверждения/отклонения операции нужно в главном меню нажать на кнопку «Открыть» для конкретного ключа (см. Рисунок 11). Количество операций для подтверждения будет указано рядом.

Если для подтверждения была доступно только одна операция, то сразу откроется подробная информация об этой операции и кнопки для подтверждения/отклонения этой операции.

Если для подтверждения было доступно несколько операций, то откроется список операций для подтверждения с краткой информацией об операциях. При нажатии на конкретную операцию из списка, откроется подробная информация о выбранной операции. В меню со списком операций можно выбрать несколько операций для подтверждения/отклонения с помощью галочек рядом с соответствующей операцией.

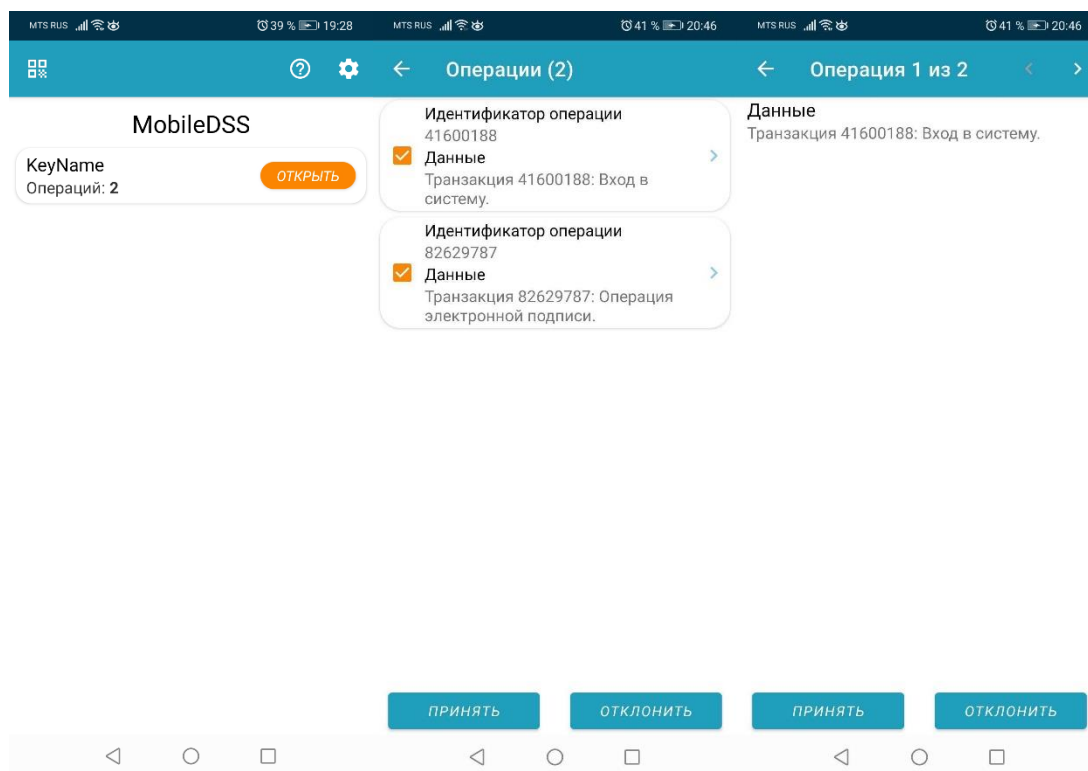


Рисунок 11 Процесс подтверждения операции(й)

3.1.6. Меню «Настройки»

При нажатии на значок шестерёнки в правом верхнем углу экрана открывается меню «Настройки» (см. Рисунок 12). Для изменения или доступа к определённой настройке нужно нажать на область данной настройки.

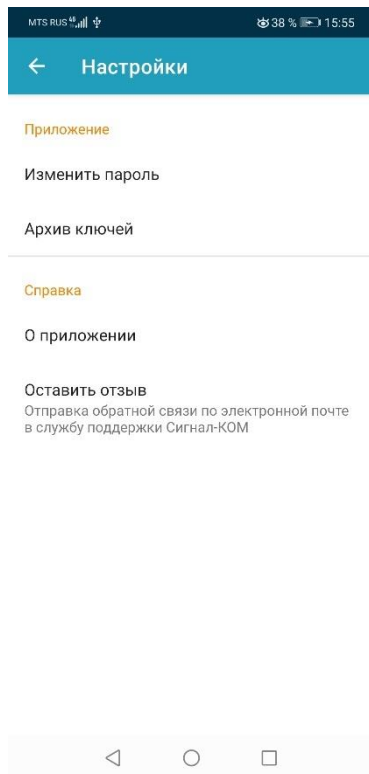


Рисунок 12 Экран меню «Настройки»

3.1.6.1 Изменить пароль

«Изменить пароль» – изменить пароль, на котором зашифрован ключевой контейнер и который используется для входа в приложение «MobileDSS».

3.1.6.2 Архив ключей

«Архив ключей» – открывает список ключей, которые были архивированы (см. п. 3.1.5.2.1).

3.1.6.3 О приложении

«О приложении» – данный пункт настроек содержит информацию о мобильном приложении и его версии, версии используемой криптографической программной библиотеки Signal-COM JCP для выполнения криптографических операций, а также ссылку на интернет-сайт компании «Сигнал-КОМ».

3.1.6.4 Оставить отзыв

«Оставить отзыв» предоставляет шаблон для отправки обратной связи по электронной почте в службу поддержки Signal-COM. Для этого на мобильном устройстве должен быть включен интернет.

4. СООБЩЕНИЯ ОПЕРАТОРУ

4.1. Сообщения в мобильном приложении «MobileDSS»

Сообщения оператору во время работы с мобильным приложением.

Таблица 1 Сообщения во время работы мобильного приложения

Сообщение	Описание
Запуск приложения	
Приложение было повреждено или изменено, работа в таком состоянии небезопасна, пожалуйста, переустановите приложение.	Ошибка при проверке подписи мобильного приложения. Возможно, была нарушена целостность приложения при установке.
Устройство имеет признаки наличия ROOT прав! Ваше устройство имеет рутированный доступ. Вы не можете использовать приложение.	Ошибка при проверке на рутированность устройства. Устройства с наличием ROOT прав могут нести угрозу безопасности данных в мобильном приложении.
Нарушены основные функции приложения! Попробуйте перезагрузить или переустановить приложение.	Ошибка при самотестировании функций мобильного приложения.
Сканирование QR	
Некорректный QR код. Данный QR код не предназначен для этого приложения.	Отсканирован некорректный QR-код, т.е. неподходящий для работы с мобильным приложением «MobileDSS».
Для приложения не установлено разрешение на использование камеры. Это можно сделать в настройках приложения. Перейти в меню «Настройки»?	В настройках приложения «MobileDSS» в настройках устройства, приложению не были выданы права на использования камеры. Без них невозможно отсканировать QR код.
Сохранение ключа	
Ключ с именем «...» уже существует!	Ключ с заданным именем уже сохранён на устройстве. Для продолжения измените имя ключа.

Ошибка при сохранении ключа.	Произошла ошибка записи данных ключа в локальное хранилище. Попробуйте сохранить ключ ещё раз.
Ошибка при формировании запроса.	Внутренняя ошибка. Ошибка при формировании JWS или работе с JSON.
Ошибка при запросе к серверу.	Ошибка возникла при попытке отправки запроса к серверу. Попробуйте сохранить ключ ещё раз.
Ключ уже был зарегистрирован на другом устройстве.	Сервер вернул ошибку 501. С этим ключом уже ассоциируется другое устройство с другим отпечатком устройства. Обратитесь к оператору.
Сервер вернул ошибку.	Сервер вернул ошибку. Попробуйте сохранить ключ ещё раз.
Ошибка при проверке типа запроса.	Внутренняя ошибка. Был использован неизвестный тип запроса.
Возникла ошибка при запросе к серверу.	При попытке запроса к серверу произошла неизвестная ошибка. Попробуйте сохранить ключ ещё раз.
Интернет не включен на устройстве	На устройстве не включен доступ ни к интернет-сети, ни к Wi-Fi.
Проверьте включен ли интернет, установлены ли на устройстве Google сервисы (Google Play) и попробуйте ещё раз.	Произошла ошибка при регистрации устройства в сервисе получения PUSH-уведомлений.
Подтверждение операции	
Произошла ошибка при отправке запроса(ов).	При отправке запроса(ов) к серверу произошла ошибка. Повторите операцию.

ЛИТЕРАТУРА

1. ГОСТ Р 34.11-2012. Государственный стандарт Российской Федерации. Информационная технология. Криптографическая защита информации. Функция хеширования.
2. Использование криптографических алгоритмов, сопутствующих применению стандартов ГОСТ Р 34.10-2012 и ГОСТ Р 34.11-2012. Рекомендации по стандартизации. Федеральное агентство по техническому регулированию и метрологии (Росстандарт), Технический комитет 026 «Криптографическая защита информации», 2014.
3. Использование алгоритмов ГОСТ Р 34.10, ГОСТ Р 34.11 в профиле сертификата и списке отзыва сертификатов (CRL) инфраструктуры открытых ключей X.509. Рекомендации по стандартизации. Федеральное агентство по техническому регулированию и метрологии (Росстандарт), Технический комитет 026 «Криптографическая защита информации», 2014.
4. ITU-T Recommendation X.509 (1997 E): Information Technology - Open Systems Interconnection - The Directory: Authentication Framework, June 1997.
5. Housley, R., Polk, W., Ford, W. and D. Solo, Internet X.509 Public Key Infrastructure Certificate and Certificate Revocation List (CRL) Profile, RFC 3280, April 2002.
6. R. Housley, "Cryptographic Message Syntax (CMS)", RFC 5652, September 2009.
7. D. Pinkas, N. Pope, J. Ross, "CMS Advanced Electronic Signatures (CAdES)", RFC 5126, February 2008
8. M. Nystrom, B. Kaliski, "PKCS #10: Certification Request Syntax Specification", RFC 2986, November 2000.
9. J. Schaad, M. Myers, "Certificate Management over CMS (CMC)", RFC 5272, June 2008.