



Удостоверяющий центр «ITCOM»

Облачная квалифицированная электронная подпись

Инструкция по установке и использованию

Оглавление

I. Запрос и выпуск сертификата	3
II. Настройка программы «КриптоПро 5.0»	7
III. Установка приложения My Dss	8
IV. Установка ключа аутентификации	9
V. Подтверждение операции подписания документа.....	12

I. Запрос и выпуск сертификата

1. На указанную Вами электронную почту автоматически направлено письмо от удостоверяющего центра с темой «**Данные для входа в личный кабинет ОКЭП**»:

Уважаемый клиент!

Ваши данные для входа в личный кабинет пользователя облачной квалифицированной электронной подписи (ОКЭП).

Логин: dss_123456789

Пароль: 12qwaszx

Ссылка на личный кабинет: <https://dss.itcomgk.ru/Frontend/>

Возможности личного кабинета пользователя ОКЭП:

- управление сертификатом электронной подписи
- загрузка, подписание, шифрование/расшифрование документа прямо в ЛК
- проверка подписанного документа
- хранение истории операций с сертификатом ОКЭП

ВАЖНО! Чтобы использовать Облачную электронную подпись завершите процедуру валидации!

В течение нескольких минут Вы получите 2 письма с секретным ключом и QR-кодом для приложения КриптоПро myDSS. Следуйте инструкциям, которые размещены в письмах. Если возникнут вопросы, обратитесь в техническую поддержку удостоверяющего центра ИТСОМ: 8 (800) 333-07-30
Это письмо отправлено автоматически. Пожалуйста, не отвечайте на него.

2. Для корректной работы рекомендуем использовать браузеры "[Спутник](#)" или [Google Chrome](#)
3. Откройте браузер перейдите по указанной в письме ссылке, введите логин и пароль.
4. После авторизации откроется страница «Запрос сертификата».



Запрос сертификата

Информация о токенах

1. Проверка программного обеспечения

- 1.1. Проверка ПО
- 1.2. Проверка версии
- 1.3. Получение разрешения
- 1.4. Получение сведений о криптопровайдере

2. Формирование запроса

- 2.1. Иванов Иван Иванович, Заявка ЕПГУ № 010101
Все готово для создания запроса **Продолжить**
- 2.1.1. Запрос на регистрацию пользователя
- 2.1.2. Подтверждение запроса на регистрацию пользователя
- 2.1.3. Формирование запроса сертификата
- 2.1.4. Отправка запроса сертификата

3. Завершение работы

5. Нажмите «**Продолжить**» и дождитесь выполнения всех пунктов
6. Когда все пункты будут зачеркнуты, нажмите на клавиатуре клавишу **F5** либо ссылку «**обновив страницу**»



Запрос сертификата

Консультации по телефону **8 861 204-01-32** добавочный 2203

Информация о токенах

1. Проверка программного обеспечения
 - 1.1. Проверка ПО
 - 1.2. Проверка версии
 - 1.3. Получение разрешения
 - 1.4. Получение сведений о криптопровайдере
2. Формирование запроса
 - 2.1. Иванов Иван Иванович, Заявка ЕПГУ № 010101
 - 2.1.1. Запрос на регистрацию пользователя
 - 2.1.2. Подтверждение запроса на регистрацию пользователя
 - 2.1.3. Формирование запроса сертификата
 - 2.1.4. Отправка запроса сертификата

3. Завершение работы

Запрос сертификата отправлен! Теперь запрос будет обрабатываться нашим Удостоверяющим Центром, после чего вы сможете получить свой сертификат. Отслеживать статус заявки можно, просто **обновив страницу.**

7. В открывшемся окне необходимо скачать бланк для подписи, нажав на соответствующую кнопку:



Спасибо за внимание!

Консультации по телефону **8 861 204-01-32** добавочный 2203

Вся необходимая на данный момент информация получена.

На этой странице вы можете отслеживать статус рассмотрения ваших заявок. Когда сертификат будет выпущен, вы сможете записать его на ключевой носитель или скачать на этой же странице.

Заявка

Статус

Ваш сертификат готов. Чтобы его получить, пожалуйста, следуйте инструкции:

1. **Скачайте** бланк для подписи
2. Распечатайте этот бланк
3. Поставьте подписи
4. Отсканируйте документ
5. Загрузите отсканированный документ:

ЕПГУ (Единого портал государственных услуг gosuslugi.ru) и пр. # 010101


Сертификат выдан



Бланк сертификата

[Получить реализацию](#)

8. Распечатайте и подпишите бланк сертификата.
9. Отсканируйте документ в хорошем качестве.
10. Загрузите скан-копию, нажав на кнопку «**Загрузить**».



Шаг 1
Заполнить форму

Шаг 2
Распечатать заявление

Шаг 3
Загрузить требуемые документы

Спасибо за внимание!

Вся необходимая на данный момент информация получена.

На этой странице вы можете отслеживать статус рассмотрения ваших заявок. Когда сертификат будет выпущен, вы сможете записать его на ключевой носитель или скачать на этой же странице.

Заявка	Статус
ЕПГУ (Единого портал государственных услуг gosuslugi.ru) и пр. # 010101	Сертификат выдан

Ваш сертификат готов. Чтобы его получить, пожалуйста, следуйте инструкции:

1. **↓ Скачайте** бланк для подписи
2. Распечатайте этот бланк
3. Поставьте подписи
4. Отсканируйте документ
5. Загрузите отсканированный документ:




Загрузить

Бланк сертификата

[Получить реализацию](#)

11. Сертификат выдан.



Шаг 1
Заполнить форму

Шаг 2
Распечатать заявление


Шаг 3
Загрузить требуемые документы

Спасибо за внимание!

Вся необходимая на данный момент информация получена.

На этой странице вы можете отслеживать статус рассмотрения ваших заявок. Когда сертификат будет выпущен, вы сможете записать его на ключевой носитель или скачать на этой же странице.

Заявка	Статус
	Сертификат выдан



Бланк сертификата [Скачать файл](#)

[Инструкция по установке корневого сертификата](#)
[Скачать сертификат](#)

Реализации не запрошены.

12. На указанную Вами электронную почту поступит 2 письма, содержащее данные для синхронизации с Вашим телефоном:

- Секретный ключ
- QR-код

Письмо с темой: «**QR-код для приложения myDSS**»

Уважаемый клиент!

Во вложении находится индивидуальный QR-код. Он нужен, что подключить Сертификат облачной электронной подписи к Вашему мобильному устройству.

1. Запустите на мобильном устройстве установленное заранее приложение «КриптоПро myDSS».
2. На главном экране нажмите кнопку с изображением QR-кода.
3. На экране сканирования нажмите кнопку «Сканировать».
4. Наведите камеру мобильного устройства на QR-код, который Вы получили в письме

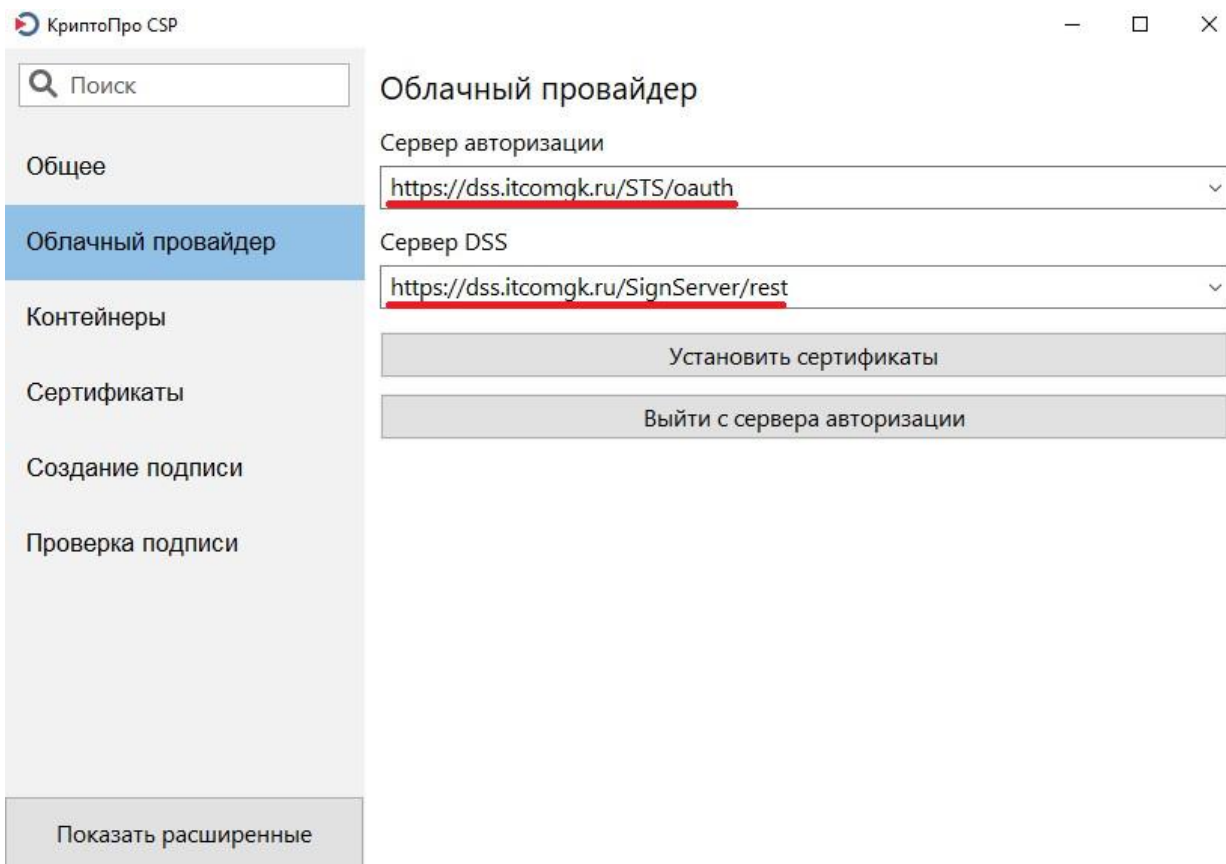
5. Введите в мобильном приложении Секретный ключ из предыдущего письма и нажмите кнопку «Продолжить».
6. Выберите, каким образом будет защищен ключ аутентификации. К примеру, ПИН-кодом (паролем), Face ID/Touch ID.
7. По желанию задайте имя ключа (по умолчанию «Ключ 1»).
8. Задайте ПИН-код (Пароль) для доступа к ключу аутентификации. ПИН-код НЕ ДОЛЖЕН быть короче 6 цифр. Повторно введите ПИН-код (Пароль) и нажмите кнопку «Продолжить».
9. После регистрации устройства на сервере ключ будет добавлен и отобразится на экране мобильного приложения. Закройте мобильное приложение. Валидация сертификата завершена.

Если возникнут вопросы, обратитесь в техническую поддержку удостоверяющего центра ИТСОМ: 8 (800) 333-07-30

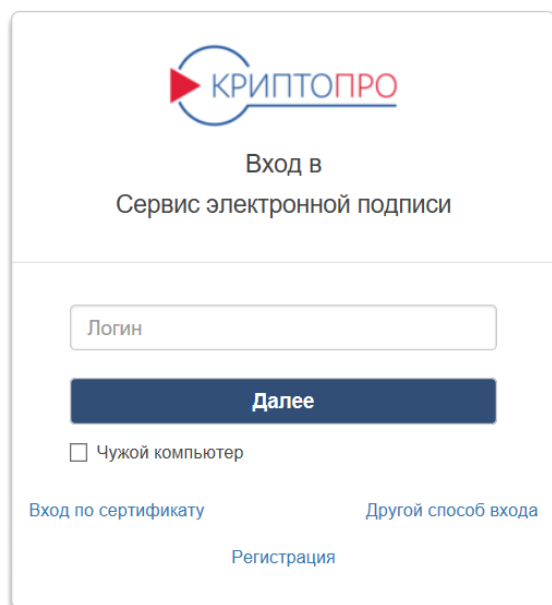
Это письмо отправлено автоматически. Пожалуйста, не отвечайте на него.

II. Настройка программы «КриптоПро 5.0»

1. Нажмите меню «Пуск», выберите «Инструменты КриптоПро».
2. В окне программы нажмите раздел «Облачный провайдер» и укажите:
Сервер авторизации - <https://dss.itcomgk.ru/STS/oauth>
Сервер DSS - <https://dss.itcomgk.ru/SignServer/rest>



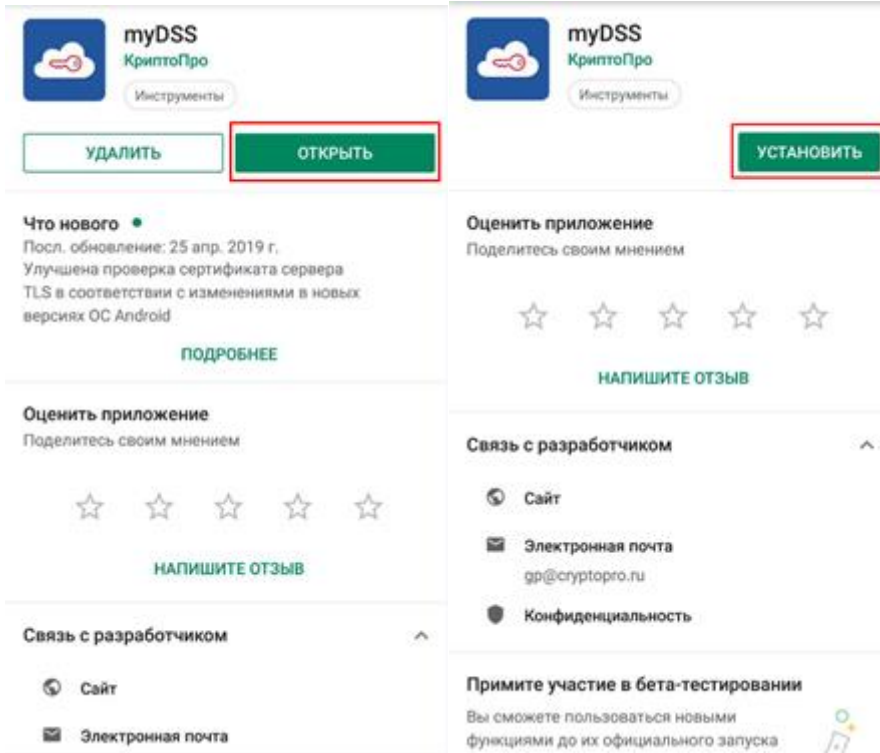
3. Нажмите кнопку «**Установить сертификаты**», в открывшемся окне введите **логин**, который Вы получили в разделе I пункт 12 данной инструкции. После нажатия кнопки «**Далее**», сертификаты будут установлены.



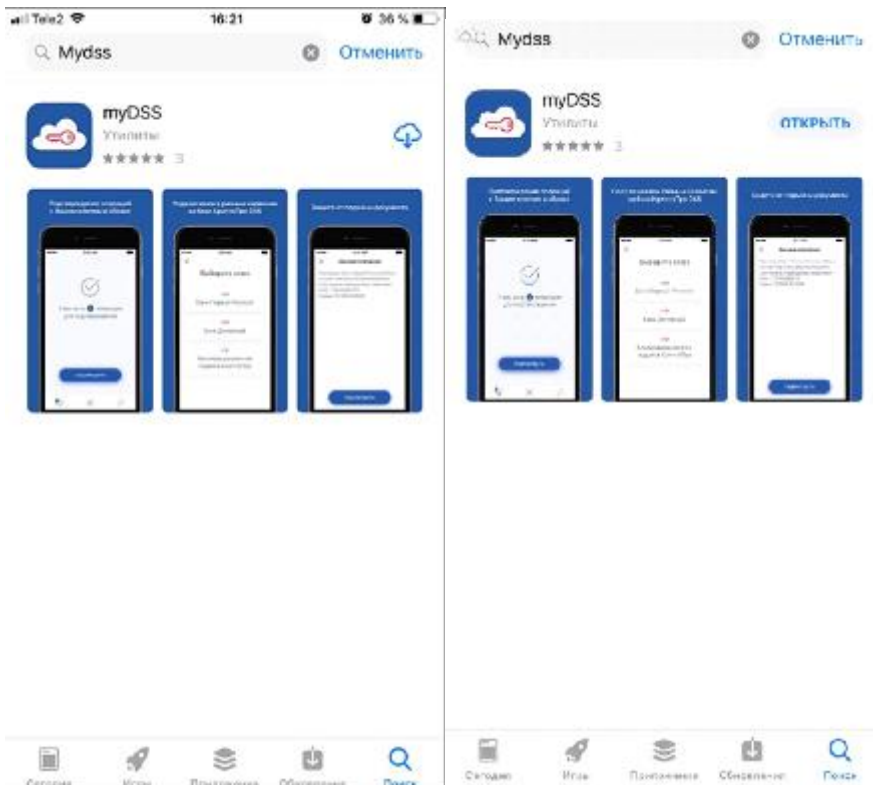
III. Установка приложения My Dss

1. В приложении **Play Market** или **Apple store**, в поиске, найдите приложение **myDSS** и нажмите **Установить**, а после установки нажмите **Открыть**

Android:

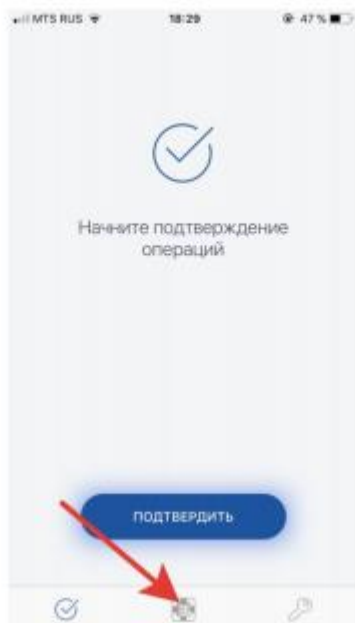


Ios:



IV. Установка ключа аутентификации

1. Запустите на мобильном устройстве установленное ранее приложение «КриптоПро myDSS».
2. На главном экране нажмите кнопку с изображением QR-кода.



3. На экране сканирования нажмите кнопку «Сканировать».



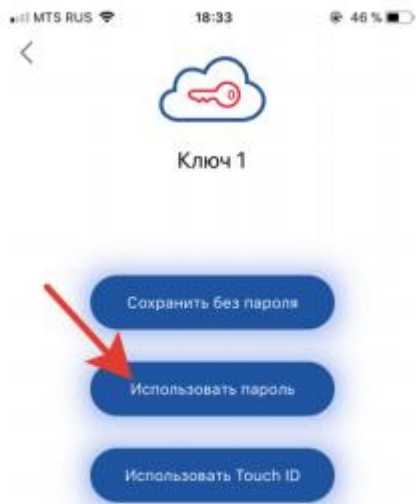
4. Наведите камеру мобильного устройства на QR-код, который Вы получили в разделе I пункт 12 данной инструкции.



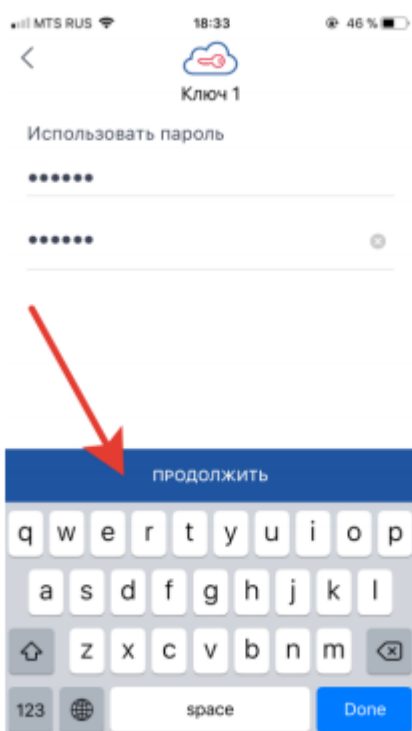
5. Введите в мобильном приложении Секретный ключ и письма и нажмите кнопку «Продолжить».



6. Выберите, каким образом будет защищен ключ аутентификации. К примеру, ПИН-кодом (паролем).



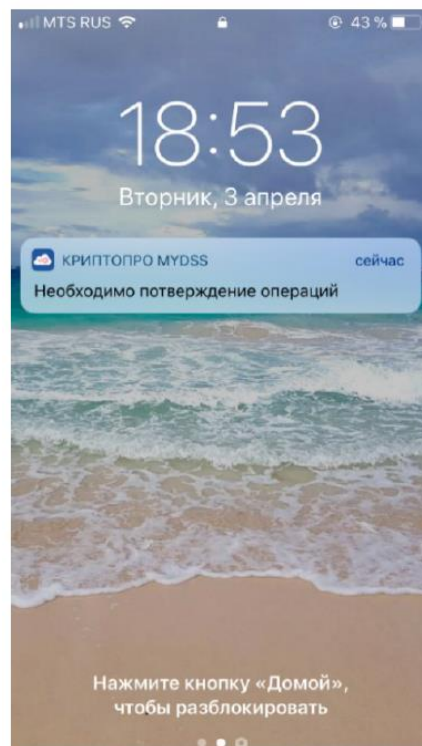
7. По желанию задайте имя ключа (по умолчанию «Ключ 1»).
8. Задайте ПИН-код (Пароль) для доступа к ключу аутентификации. ПИН-код НЕ ДОЛЖЕН быть короче 6 цифр. Повторно введите ПИН-код (Пароль) и нажмите кнопку «Продолжить».



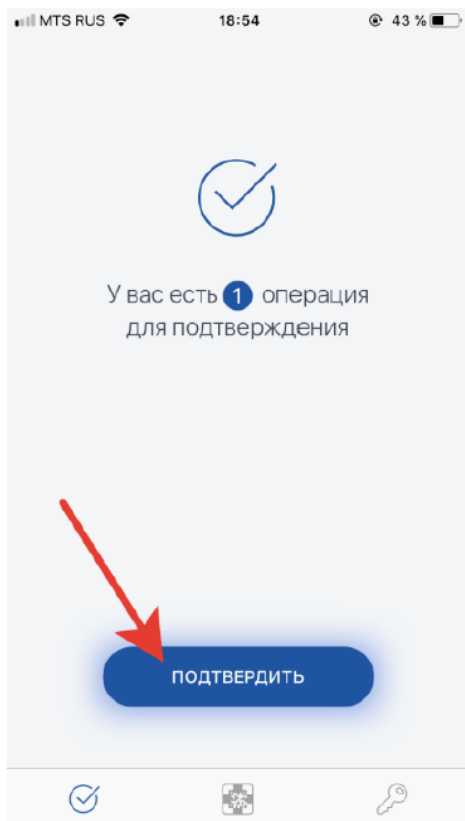
9. После регистрации устройства на сервере ключ будет добавлен и отобразится на экране мобильного приложения. Закройте мобильное приложение.

V. Подтверждение операции подписания документа

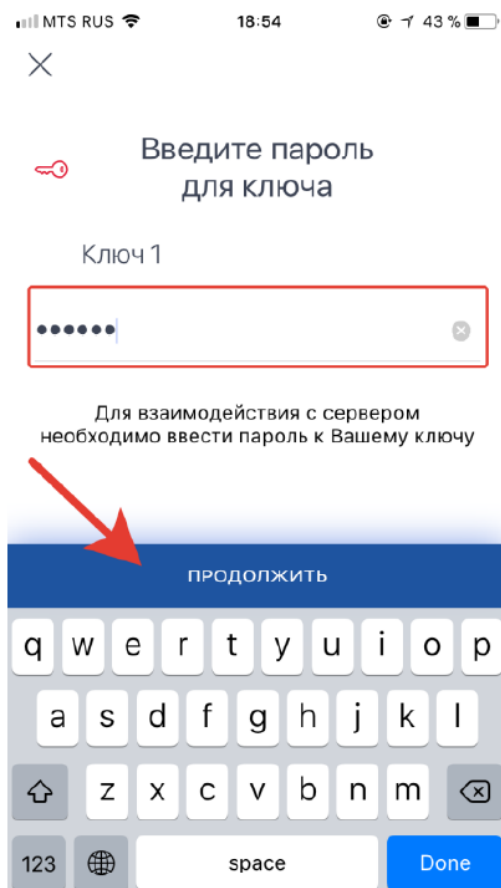
1. После подписания электронной подписью документа на экране смартфона появится предложение подтвердить операцию. Дождитесь PUSH-уведомления на Вашем мобильном устройстве об операции. Если PUSH-уведомление не приходит, просто откройте приложение «КриптоПро myDSS».



2. При входе в мобильное приложение «КриптоПро myDSS» нажмите кнопку «Подтвердить».



3. Введите ПИН-код (Пароль) доступа к ключу аутентификации и нажмите кнопку «Продолжить».



4. На экране мобильного устройства отобразится подписываемый документ и информация о нем. Убедитесь, что хотите подтвердить подпись именно этого документа и нажмите кнопку «Подтвердить».




5. Если операция подтверждена успешно, на экране появится соответствующее сообщение. Нажмите «**Продолжить**».

MTS RUS 18:56 42%



Операция успешно
подтверждена



ПРОДОЛЖИТЬ

6. В случае успешного подтверждения операции браузер предложит скачать или открыть подписанный документ. Откройте его или сохраните на жестком диске.