АКТ № FIL-260608-96872

от 2026-06-08 15:30:22 MSK

Акт криптографической фиксации электронного файла

Идентификатор акта	`00f07f2f95089f8293846cfc461bf0c3`
Имя файла	`Договор_оказания_услуг_образец.pdf`
Размер файла	17.4 KB (17791 байт)
Время фиксации	2026-06-08 15:30:22 MSK
Удостоверение времени	Время удостоверено
OpenTimestamps (Bitcoin)	Хеш опубликован

Сканируйте для проверки акта и сверки хешей

Сводные хеши файла

SHA-256 (RFC 6234)

`c47839aa5ae14e7c8c8b4369f5fed73dac7964b65cce1bad33bac0be8172e718`

Стрибог-256 (ГОСТ Р 34.11-2012)

`80f434138a22f01e1cb8349f1a7b82ee50d99bbf86841e5eb0e98c4e04f5aaf3`

Настоящий акт фиксирует факт существования файла с указанным содержимым на момент фиксации. Целостность файла гарантируется криптографически: изменение хотя бы одного байта файла приведёт к расхождению указанных выше хешей и недействительности удостоверяющих меток времени. Подробности проверки — на стр. 4.

1. Преамбула

Настоящий акт составлен автоматизированной системой «Подписал.ру» (https://podpisal.ru) по запросу инициатора фиксации и удостоверяет факт существования файла с указанным содержимым на дату и время фиксации.

1.1. Инициатор фиксации

IP-адрес инициатора	`113.22.236.228`
User-Agent инициатора	`curl/8.7.1`
Идентификатор заказа	`00f07f2f95089f8293846cfc461bf0c3`

1.2. Объект фиксации

Имя файла	`Договор_оказания_услуг_образец.pdf`
Размер	17.4 KB (17791 байт)
Время загрузки	2026-06-08 15:30:22 MSK

2. Методика фиксации

2.1. Получение файла

Файл получен сервером «Подписал.ру» по защищённому каналу HTTPS (TLS 1.2+). На стороне сервера файл сохранён без какой-либо обработки или модификации содержимого. Размер сохранённого файла совпадает с размером, зафиксированным в заголовках HTTP-запроса.

2.2. Подсчёт хешей

Для содержимого файла подсчитаны две независимые криптографические контрольные суммы за один проход чтения файла:

- **SHA-256** — международный стандарт хеширования (RFC 6234), широко используемый в банковской и государственной сфере.
- **Стрибог-256** — национальный стандарт Российской Федерации (ГОСТ Р 34.11-2012). Используется в качестве «российского» алгоритма хеширования при работе с электронными документами в РФ.

2.3. Удостоверение времени

Подсчитанные хеши собраны в файл `manifest.txt`; сводный SHA-256 этого файла подписан независимой службой меток времени (RFC 3161 Time-Stamp Protocol) и опубликован в реестре OpenTimestamps, что обеспечивает публикацию хеша в

блокчейне Bitcoin. Подделка времени фиксации задним числом без потери удостоверяющих меток математически невозможна.

3. Выполненные системой действия

В ходе фиксации система последовательно выполнила следующие действия:

№	Действие	Результат
1	Приём файла `Договор_оказания_услуг_образец.pdf` по HTTPS-каналу. Сохранение без модификации содержимого.	17.4 KB
2	Подсчёт SHA-256 (RFC 6234) и Стрибог-256 (ГОСТ Р 34.11-2012) для содержимого файла за один проход чтения.	2 хеша
3	Формирование `manifest.txt` с указанием имени, размера и обоих хешей файла.	ok
4	Запрос RFC 3161 Time-Stamp Token у независимого провайдера `freetsa.org` на хеш манифеста. Серийный номер токена: `0x05756478` Время согласно TSA: `2026-06-08 12:30:19 UTC` `2026-06-08 15:30:19 МСК` Файл доказательства: `manifest.tsr`	ok
5	Публикация хеша манифеста в реестре OpenTimestamps (подтверждение в Bitcoin появляется в течение ~3 часов). Файл OTS-доказательства: `manifest.txt.ots` Проверка: `ots verify <имя>.ots`	ok
6	Формирование настоящего PDF-акта и публикация страницы верификации.	ok

3.1. Сводные хеши файла

SHA-256 (RFC 6234)	`c47839aa5ae14e7c8c8b4369f5fed73dac7964b65cce1bad33bac0be8172e718`
Стрибог-256 (ГОСТ Р 34.11-2012)	`80f434138a22f01e1cb8349f1a7b82ee50d99bbf86841e5eb0e98c4e04f5aaf3`

3.2. Сводные хеши манифеста

SHA-256 (RFC 6234)	`e2ba1ed76e5fc9438cf613a38da3aafdafd21022b7506a6524a14d7468c39b62`
Стрибог-256 (ГОСТ Р 34.11-2012)	`b98e2b947b42c95a3ecfe4d948a1b55648c39c2c63b157872c9c451bd9ffcae7`

4. Юридическое основание и проверка

Настоящий акт удостоверяет факт существования файла с указанным содержимым (зафиксированным двумя независимыми криптографическими хешами) на дату и время фиксации, удостоверённые независимой службой меток времени RFC 3161 и публичным реестром OpenTimestamps (сеть Bitcoin).

Согласно статье 71 Гражданского процессуального кодекса РФ и статье 75 Арбитражного процессуального кодекса РФ электронный документ может быть представлен в качестве письменного доказательства. Подлинность электронного документа во времени подтверждается криптографическими механизмами фиксации хеша в независимом реестре, что соответствует подходу, отражённому в пункте 55 Постановления Пленума Верховного Суда РФ от 23 апреля 2019 г. № 10.

Целостность зафиксированного файла обеспечивается математически: одновременная подделка двух независимых хеш-функций (SHA-256 и Стрибог-256) в рамках одного файла на сегодня практически невозможна.

4.1. Способ проверки акта любой третьей стороной

- Открыть публичную страницу верификации (см. ниже) и сверить SHA-256 и Стрибог-256 хеши файла с приведёнными в настоящем акте.
- На странице верификации можно загрузить оригинал файла — браузер пересчитает оба хеша локально и сравнит их с указанными в акте.
- Загрузить файл RFC 3161 TSA-токена и проверить его средствами `openssl ts -verify`. Информация о провайдере: `https://freetsa.org/`.
- Загрузить OpenTimestamps-доказательство и проверить публикацию хеша в сети Bitcoin утилитой `ots verify`. Открытая спецификация и инструменты: `https://opentimestamps.org/`.

4.2. Криптографические гарантии

Хеш-функция №1	SHA-256 (RFC 6234)
Хеш-функция №2	Стрибог-256 (ГОСТ Р 34.11-2012)
Удостоверение времени	RFC 3161 TSA — freetsa.org
Публичная фиксация	OpenTimestamps (Bitcoin)

Алгоритм Стрибог-256 является односторонней функцией без секретного ключа и не выполняет шифрования; его реализация не относится к СКЗИ и не требует получения лицензий ФСБ России.

Страница верификации:

https://api.podpisal.ru/tools/verify-file/00f07f2f95089f8293846cfc461bf0c3

Страница доступна публично и не требует регистрации. На ней можно сверить хеши, загрузить оригинал файла и проверить статус подтверждения в Bitcoin.