# Инструкция по проверке электронной подписи

## Назначение

Ключевые публичные документы ООО «Оператор банковской кооперации» публикуются вместе с отсоединенной электронной подписью `.sig`. Вы можете проверить, что сказали актуальную версию документа, проверив электронную подпись.

Проверка подписи позволяет убедиться, что:

- подпись относится именно к опубликованному PDF-файлу;
- PDF-файл не был изменен после подписания;
- документ подписан сертификатом подписанта оператора;
- сертификат действовал на момент подписания;
- подпись содержит отметку времени, если она была добавлена при подписании.

## Что скачать с сайта

Для проверки нужны:

1. PDF-документ.
2. Файл подписи `.sig` Сертификат подписанта содержится в этом же файле.
3. Контрольная сумма SHA-256, указанная на странице документа.

PDF-файл и файл подписи рекомендуется сохранить в одну папку.

## Рекомендуемый способ проверки: веб-сервис

Самый простой вариант - это веб-проверка электронной подписи без установки компонентов на рабочее место пользователя, которая выполняется прямо в браузере.

## Порядок проверки через веб-сервис

1. Скачать PDF-документ с сайта.
2. Скачать файл отсоединенной подписи `.sig`.
3. Открыть веб-сервис проверки электронной подписи.
4. Загрузить PDF-документ.
5. Загрузить файл подписи `.sig`.
6. Запустить проверку.
7. Убедиться, что сервис сообщает о действительности подписи.
8. Проверить сведения о подписанте и сертификате.
9. Сверить SHA-256 PDF-файла с контрольной суммой, опубликованной на сайте.

Положительный результат подтверждает, что подпись действительна и соответствует проверяемому документу.

## Альтернатива: проверка на рабочем месте

Если внутренний регламент банка запрещает использовать внешние веб-сервисы, банк может проверить подпись на своем рабочем месте или во внутреннем сервисе проверки.

В таком случае можно использовать:

- КриптоПро CSP;
- КриптоАРМ ГОСТ или совместимое средство проверки подписи.

По документации КриптоАРМ ГОСТ для проверки подписи на рабочем месте должен быть установлен криптопровайдер КриптоПро CSP. КриптоАРМ поддерживает проверку файлов подписи с расширениями `.sig`, `.p7s`, `.sgn`, `.sign`, `.bin`.

Официальные материалы:

- КриптоАРМ ГОСТ, проверка подписи: https://cryptoarm.ru/docs/cryptoarm_gost/latest/004-documents/18-verify/
- КриптоАРМ 6, проверка подписи и поддерживаемые расширения: https://cryptoarm.ru/docs/cryptoarm/v6.2/004-documents/14-verify/

## Порядок проверки в КриптоАРМ ГОСТ

1. Установить и запустить КриптоПро CSP.
2. Установить и запустить КриптоАРМ ГОСТ или совместимое средство.
3. Открыть мастер проверки подписи.
4. Выбрать файл подписи `.sig`.
5. Если программа попросит исходный файл, выбрать соответствующий PDF-документ.
6. Дождаться результата проверки.
7. Проверить сведения о подписанте и сертификате.
8. Сверить SHA-256 PDF-файла с контрольной суммой, опубликованной на сайте.

## Проверка SHA-256

SHA-256 не заменяет проверку электронной подписи, но помогает убедиться, что скачанный PDF совпадает с опубликованным файлом.

На macOS или Linux:

```
shasum -a 256 document.pdf
```

На Windows:

```
certutil -hashfile document.pdf SHA256
```

Полученное значение должно совпадать с SHA-256, опубликованным на странице документа.

## Командная строка

ИТ-служба участника может использовать командную строку КриптоАРМ или КриптоПро, если такой способ принят во внутреннем регламенте банка.

Команду для проверки не фиксируем в публичной инструкции до теста первого реально подписанного документа, потому что точный синтаксис зависит от установленного продукта, версии и настроек рабочего места.

Официальный ориентир:

- КриптоАРМ, операции в командной строке: https://cryptoarm.ru/docs/cryptoarm/latest/005-documents/08-CLI-operations/

## Если проверка не прошла

Если средство проверки сообщает об ошибке, нужно:

1. Убедиться, что PDF и `.sig` относятся к одному документу.
2. Скачать оба файла заново с сайта.
3. Проверить SHA-256 PDF-файла.
4. Проверить, установлен ли КриптоПро CSP и доступны ли списки отзыва сертификатов.
5. Направить запрос оператору платежной системы через форму на сайте с указанием документа, даты скачивания и текста ошибки.