

# Описание

---

Модуль цифровой подписи

## Проверка подписи

---

Для проверки подписи рекомендуется использовать сервис `SignerService` :

- `verify(InputStream, InputStream)` - для проверки открепленной подписи (base64)
- `verify(InputStream, InputStream, boolean)` - для проверки открепленной подписи (с признаком base64 - true/false)
- `verify(InputStream, SignatureType)` - для проверки прикрепленной/встроенной подписи

Существует два формата открепленной/прикрепленной подписи: Base64 и DER. При этом декодированный Base64 не равен DER. В текущей реализации сервис умеет проверять только подпись в формате Base64.

### Открепленная подпись

Открепленная подпись представляет собой файл с подписью, который передается вместе с исходным подписанным файлом.

### Прикрепленная/встроенная подпись

Прикрепленная подпись представляет собой один файл, в котором находится как подпись, так и контент исходного подписанного файла. Для просмотра подписанного контента необходим специальный софт, умеющий извлекать его.

Некоторые форматы данных (такие, как XML, PDF) имеют механизмы встраивания подписи. В таком случае подписанный файл доступен для чтения стандартными средствами.

Проверка разных видов прикрепленной/встроенной подписи осуществляется с помощью соответствующей реализации интерфейса `SignatureVerifier`. В случае, если запрошена валидация встроенной подписи, но она не найдена, происходит так же проверка реализацией по-умолчанию (прикрепленной подписи).