

# ???????? ?????

## Проверка подписи через КриптоПро

Предположим есть сертификат и текст, который подписывается ГОСТовским алгоритмом и затем кодируется в Urlsafe.

Устанавливаем КриптоПро и сертификат в раздел Личное.

Скрипт для преобразования urlsafe подписи в КриптоПро - читаемую:

```
# convert_signature.py
import base64

# Ваша подпись из логов
signature_urlsafe = "MIIKs...3RU8"

# 1. Преобразуем URL-safe → стандартный Base64
signature_b64 = signature_urlsafe.replace('-', '+').replace('_', '/')
# Добавляем padding
padding = 4 - len(signature_b64) % 4
if padding != 4:
    signature_b64 += '=' * padding

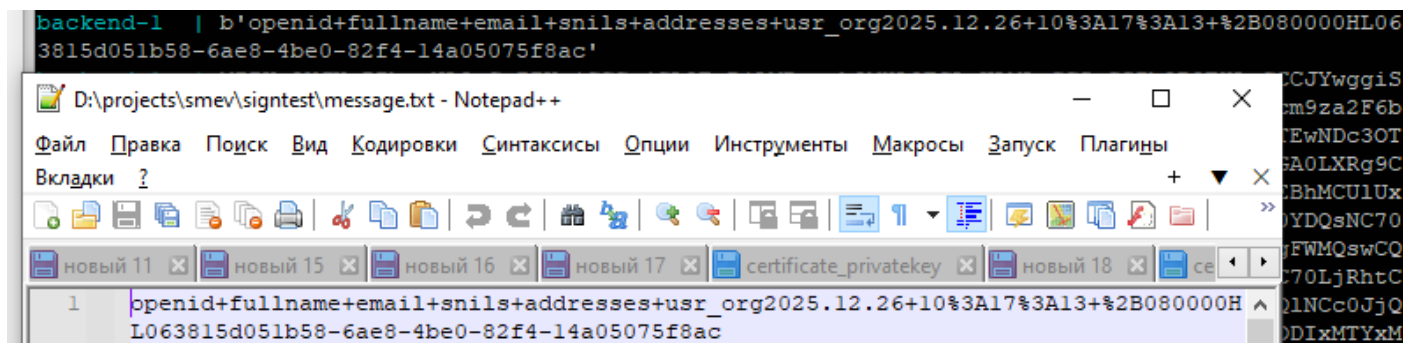
# 2. Декодируем Base64 → бинарный DER
signature_der = base64.b64decode(signature_b64)

# 3. Сохраняем в файл
with open('signature.der', 'wb') as f:
    f.write(signature_der)

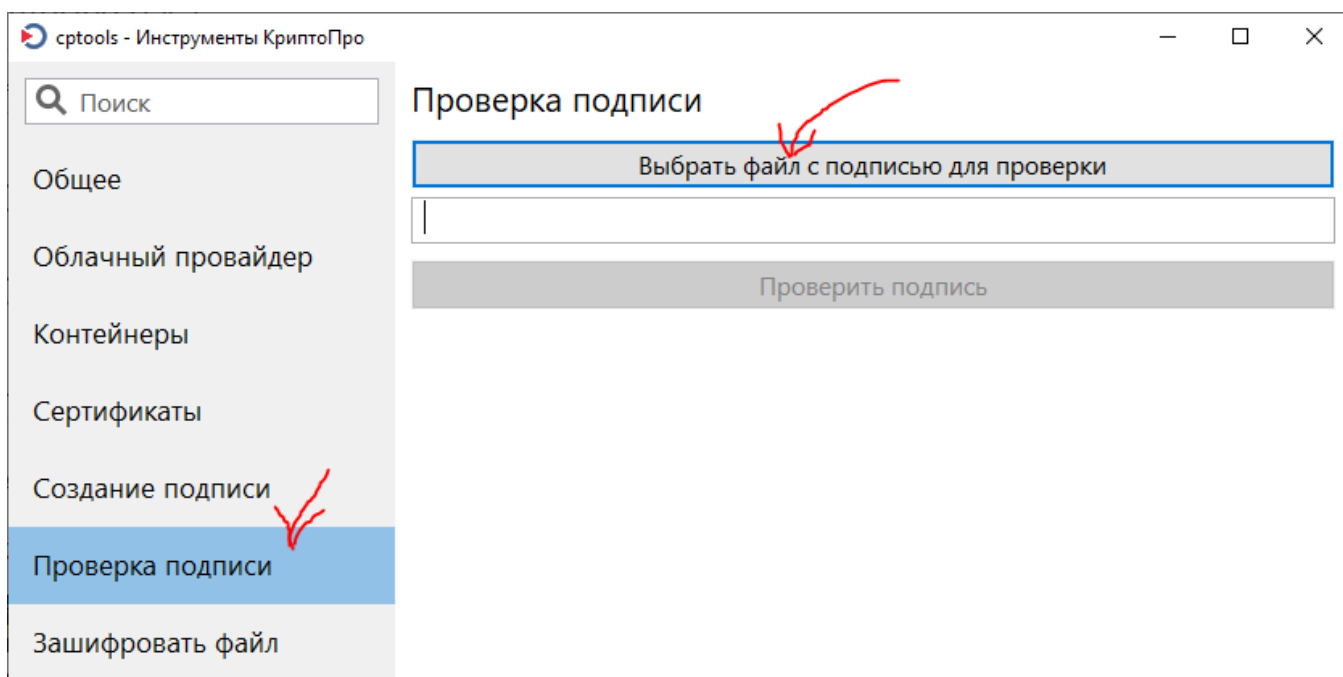
print("Подпись сохранена в signature.der")
```

Саму подпись сохраняем в переменную signature\_urlsafe. В результате сформируется файл signature.der

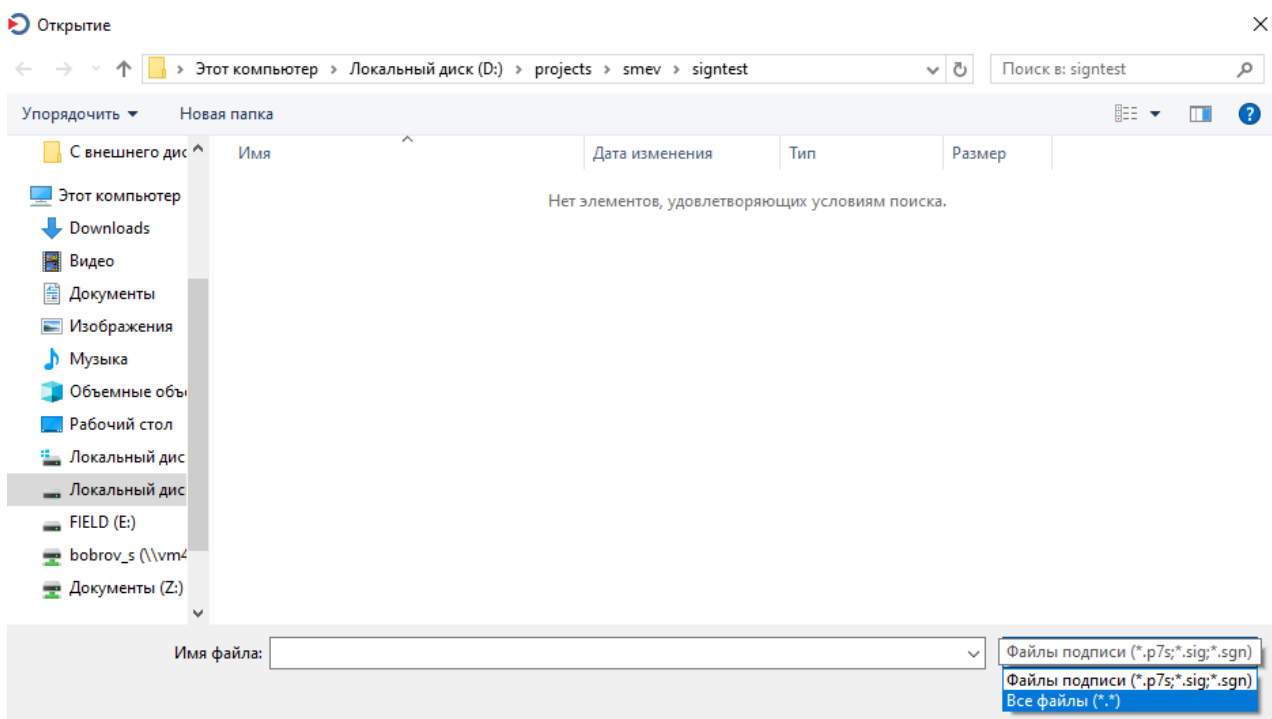
В файл message.txt сохранил напрямую бинарную часть сообщения, все то что внутри кавычек



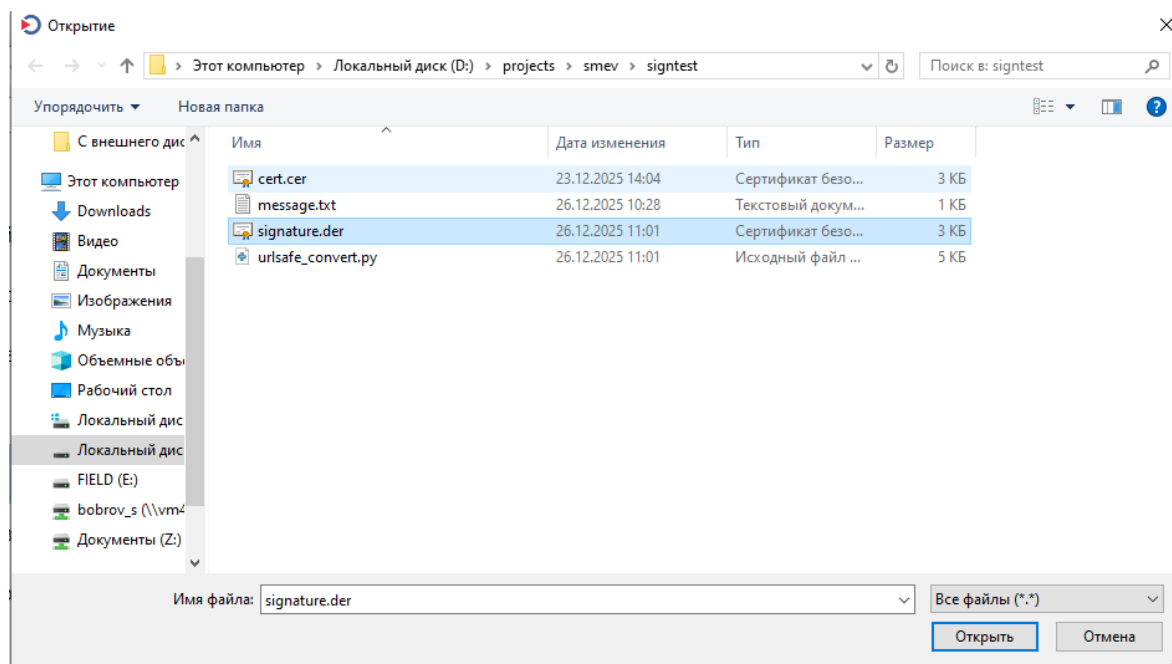
Запускаем Инструменты КриптоПро -> Проверка подписи -> Выбрать файл с подписью...



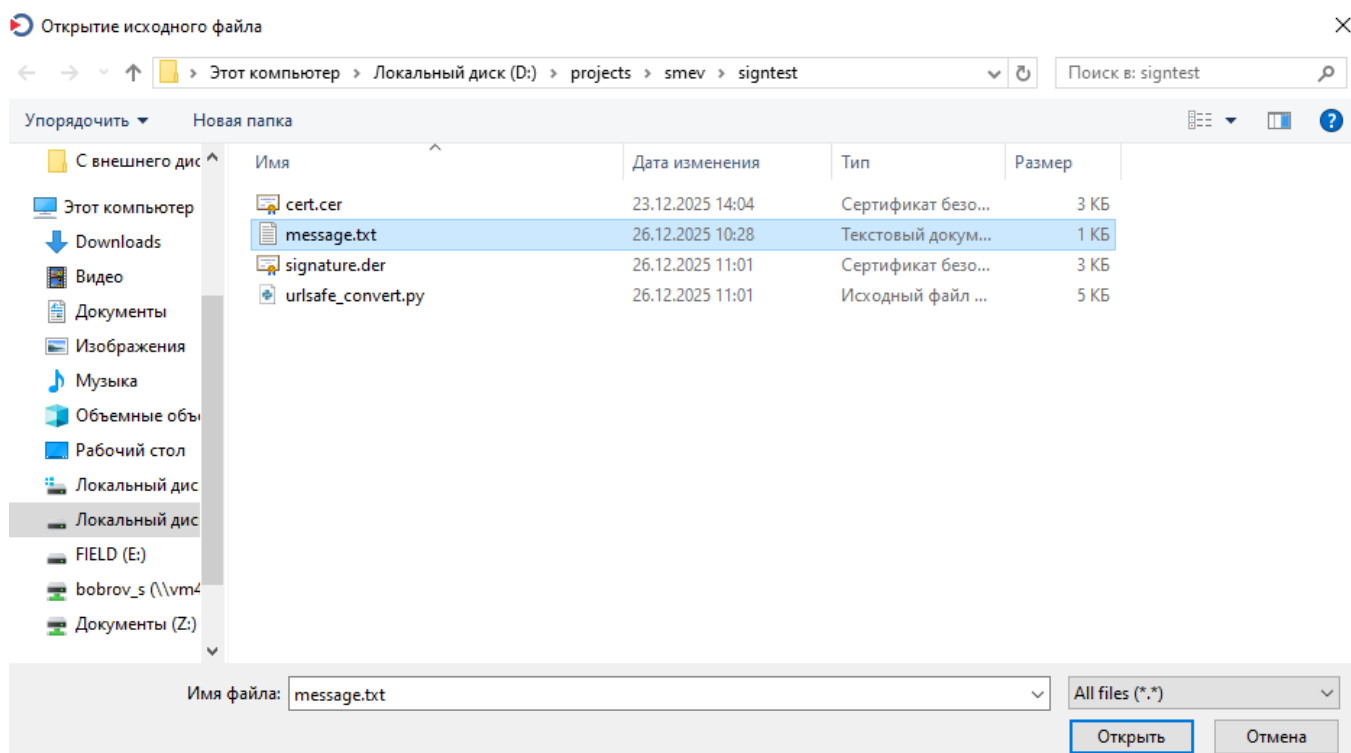
Меняем тип файла на "Все файлы"



## Открываем созданный файл signature.der



Нажимаем кнопку "Проверить подпись" и будет предложено указать исходный файл (который мы подписывали), так как файл signature.der это файл с открепленной подписью. Указываем message.txt



Подпись будет проверена

Поиск

Общее

Облачный провайдер

Контейнеры

Сертификаты

Создание подписи

Проверка подписи

## Проверка подписи

Выбрать файл с подписью для проверки

D:\projects\smev\signtest\signature.der

Проверить подпись

▼ Подпись была успешно проверена

Подпись 1/1: успешно проверена

Отпечаток: 9A51EDE7F2531FC55D59A80B13AD17B7B2B62724

Имя субъекта: АДМИНИСТРАЦИЯ ГОРОДА ИРКУТСКА

Revision #1

Created 26 December 2025 03:09:47 by Admin

Updated 26 December 2025 03:31:20 by Admin