

# Практические подходы к реализации подписи ПО в рамках инициативного эксперимента российских вендоров СКЗИ и его результаты



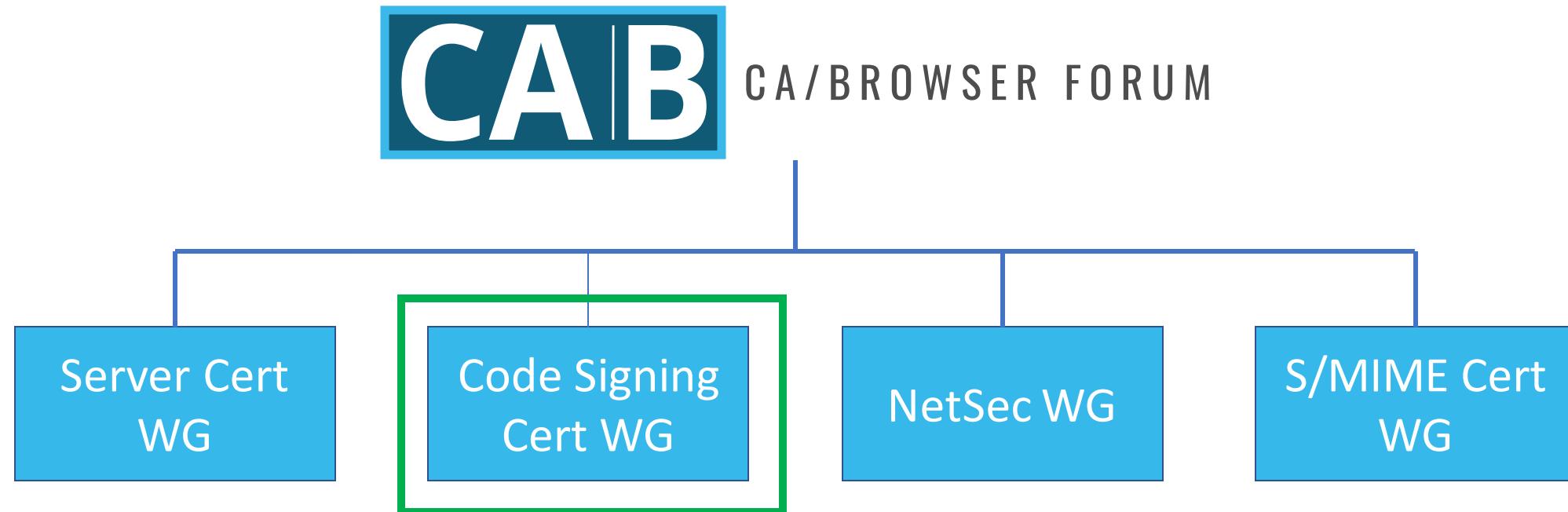
Александр Петров

**КриптоПро**

# Проблематика

1. Решения для создания и проверки меток доверенного кода с поддержкой российских криптоалгоритмов массово не применяются
2. Низкая степень интеграции таких решений в ОС российской разработки
3. Отсутствует интеграция таких решений в российские магазины приложений и фонды программного обеспечения
4. Нет массовой выдачи сертификатов метки доверенного кода
5. Отсутствует нормативное регулирование в области доверенного распространения программного обеспечения

# Международный опыт 1.3.6.1.5.5.7.3.3



A code signing certificate contains the public key corresponding to a private key that is used by a person or organization to digitally sign data—such data usually containing instructions (i.e. “code”) for hardware to perform certain tasks. A code signing certificate can be identified by the existence of an Extended Key Usage (EKU) Object Identifier (OID) of 1.3.6.1.5.5.7.3.3.



# Область действия Code Signing Cert WG

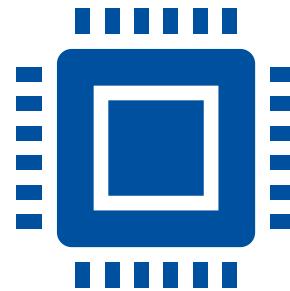
- Поставщик платформы принимает сертификаты подписи кода, выданные сторонним издателем сертификатов  
Microsoft Authenticode
- Поставщик платформы управляет процессом подписи кода или выдачи сертификатов  
Apple Developer ID, Google Android  
**Исключены из сферы действия рабочей группы**

# Code Signing Cert WG

- Рабочая группа по сертификатам подписи кода CA/Browser Forum была создана для работы над требованиями, предъявляемыми к центрам сертификации, выдающим сертификаты подписи кода.
- Категории участников рабочей группы:

Издатели сертификатов	Потребители сертификатов	Заинтересованные стороны	Ассоциированные участники
DigiCert Entrust GlobalSign Sectigo SSL.com ...	Microsoft	Amazon Cisco Systems DigitalTrust ETSI ...	IBM Intel ...

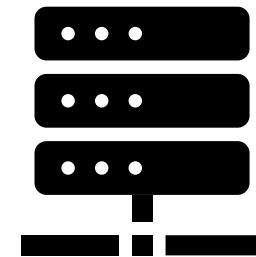
# Требования к разработчику в части защиты закрытого ключа (п. 6.2.7.4.1)



HSM  
FIPS 140-2 Level 2  
Common Criteria EAL 4+



Облако  
Ключ внутри облачного HSM,  
журнал всех доступов



Сервис подписи

# Проверка требований к разработчику в части защиты закрытого ключа (п. 6.2.7.4.2)

1) Предварительно сгенерированный УЦ



2) Проверка сертификатом производителя



3) Предписанные крипто-библиотеки и  
аппаратные крипто-модули



4) Внутренний или внешний аудит



# Проверка требований к разработчику в части защиты закрытого ключа (п. 6.2.7.4.2)

5) Подписка на облачное решение



6) Засвидетельствование аудитором



7) Согласие на использование Сервиса Подписи



# Начало эксперимента

 СБЕР

...

 Яндекс

...

 kaspersky

~50

лето 2025 года



 НТЦ ЦК

 КриптоПро

 infotechs

Сложно опробовать подходы  
сразу на большом количестве участников

# Начало эксперимента

 СБЕР

...

 Яндекс

...

 kaspersky

~50

Сложно опробовать подходы  
сразу на большом количестве участников

лето 2025 года



 НТЦ ЦК

 КриптоПро

 infotechs

 КОД  
безопасности

# Долгосрочные цели

## ЕДИНОЕ ПРОСТРАНСТВО ДОВЕРИЯ

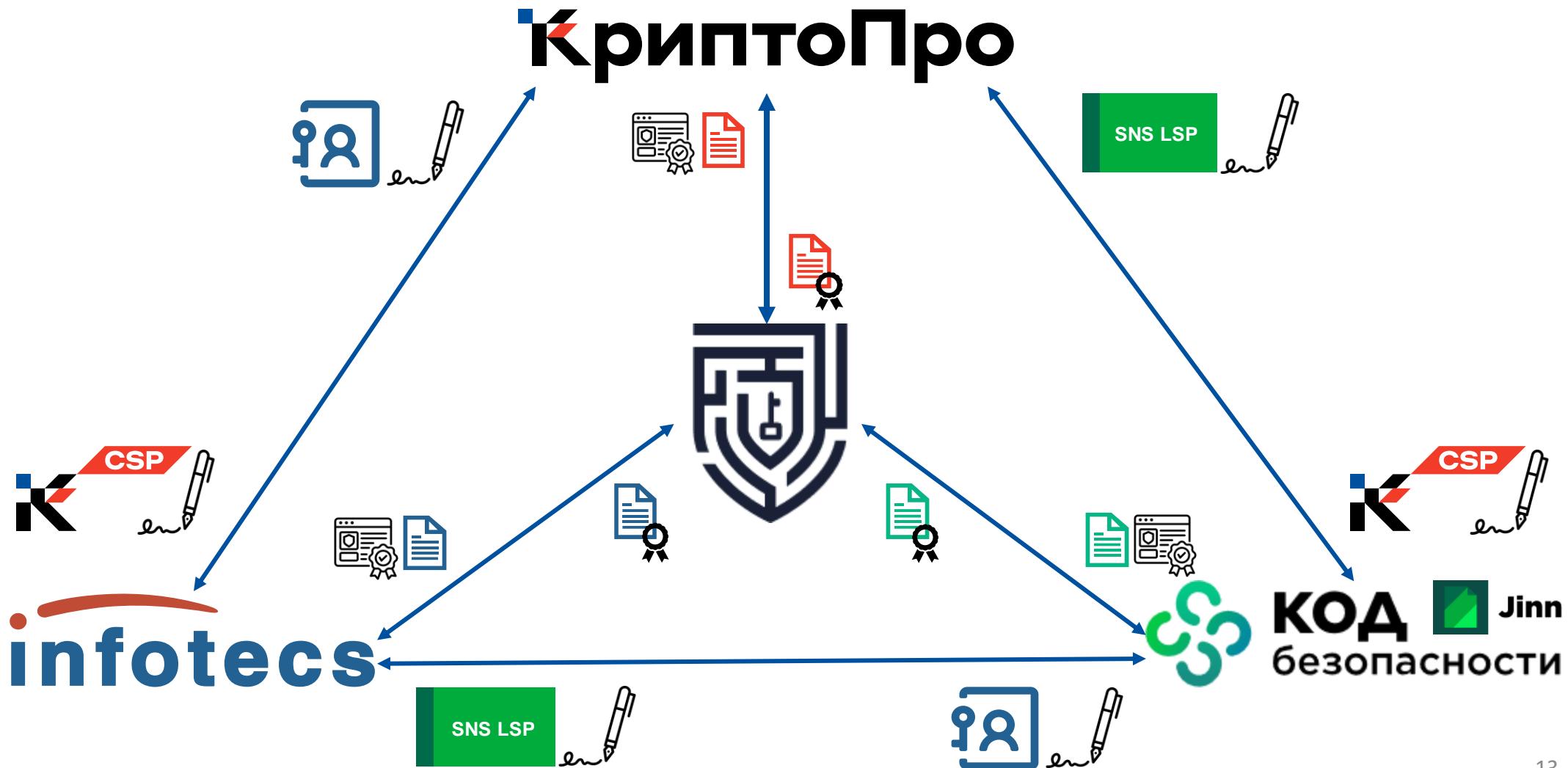
- ▶ Требования к механизмам и технологиям
- ▶ Типовые рекомендации:
  - ▶ проектирования для продуктов
  - ▶ конфигурирования инфраструктуры разработки организации
  - ▶ конфигурирования интеграционных взаимодействий в инфраструктуре организаций, участников взаимодействия
- ▶ Технологическая независимость

# Цели 1-ой итерации

ЭКСПЕРИМЕНТ, ПРОВЕДЁННЫЙ В РАМКАХ РГ

- ▶ Проработать частный подход к обеспечению целостности и подлинности дистрибутивов разрабатываемого ПО
- ▶ Протестировать использование системы ОТУЦ
- ▶ Наладить взаимодействие между организациями-участниками
- ▶ Привлечь более широкий круг участников

# Общая структура эксперимента





# Настройка окружения

Предварительно необходимо установить требуемые сертификаты и списки отзываемых сертификатов <https://otuc.digitalcryptography.ru/ca-info>

## Корневые и промежуточные сертификаты



Корневой УЦ

Срок действия 28.10.2024 - 28.10.2039

Скачать

## УЦ для выпуска сертификатов TLS-соединений

Срок действия 29.10.2024 - 28.10.2039

Скачать

## УЦ для выпуска сертификатов метки доверенного кода

Срок действия 29.10.2024 - 28.10.2039

Скачать

## Списки отзываемых сертификатов



Корневой УЦ

Обновлен 03.11.2025

Скачать

## УЦ для выпуска сертификатов TLS-соединений

Обновлен 28.11.2025

Скачать

## УЦ для выпуска сертификатов метки доверенного кода

Обновлен 28.11.2025

Скачать



# Получение сертификата подписи кода

## Выдача сертификата

⌚ Ожидает загрузки запроса и открепленной подписи

### 1 ЗАЯВИТЕЛЬ

Данные заявителя подставлены автоматически из вашего аккаунта.

ФИО

Филатов Давид Ефимович



ИНН

837486365979

СНИЛС

30397934493

Роль

Физическое лицо

### 2 ЗАПРОС

Загрузите запрос и открепленную подпись и отправьте заявку.

Загрузите запрос ⓘ

Файл в формате .p10

Выберите файл

Файл не выбран



.\\cryptcp.exe -creatrqst -provname "Crypto-Pro GOST R 34.10-2012 Cryptographic Service Provider" -provtype 80 -dn "E=test@test.ru,CN=Филатов Давид Ефимович,G=Давид Ефимович,SN=Филатов,C=RUS,=77 Москва,L=г. Москва,1.2.643.3.131.1.1=837486365979,1.2.643.100.3=30397934493" -certusage 1.3.6.1.5.5.7.3.3 -cont \\.\REGISTRY\\filatov\_MDK -exprt -ku filatov\_MDK.req

Загрузите подпись ⓘ

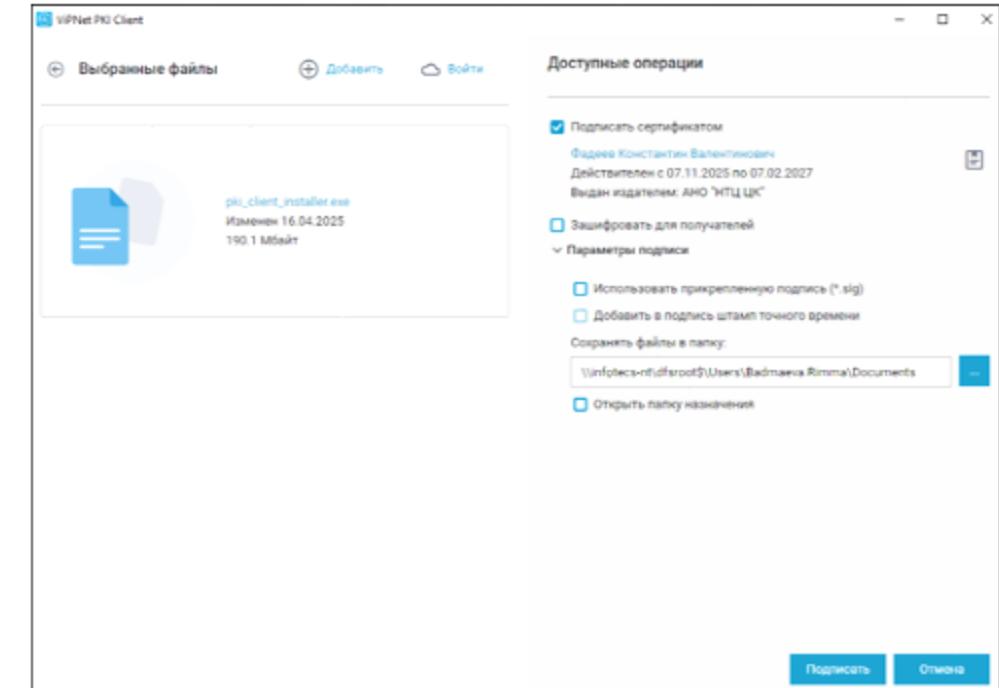
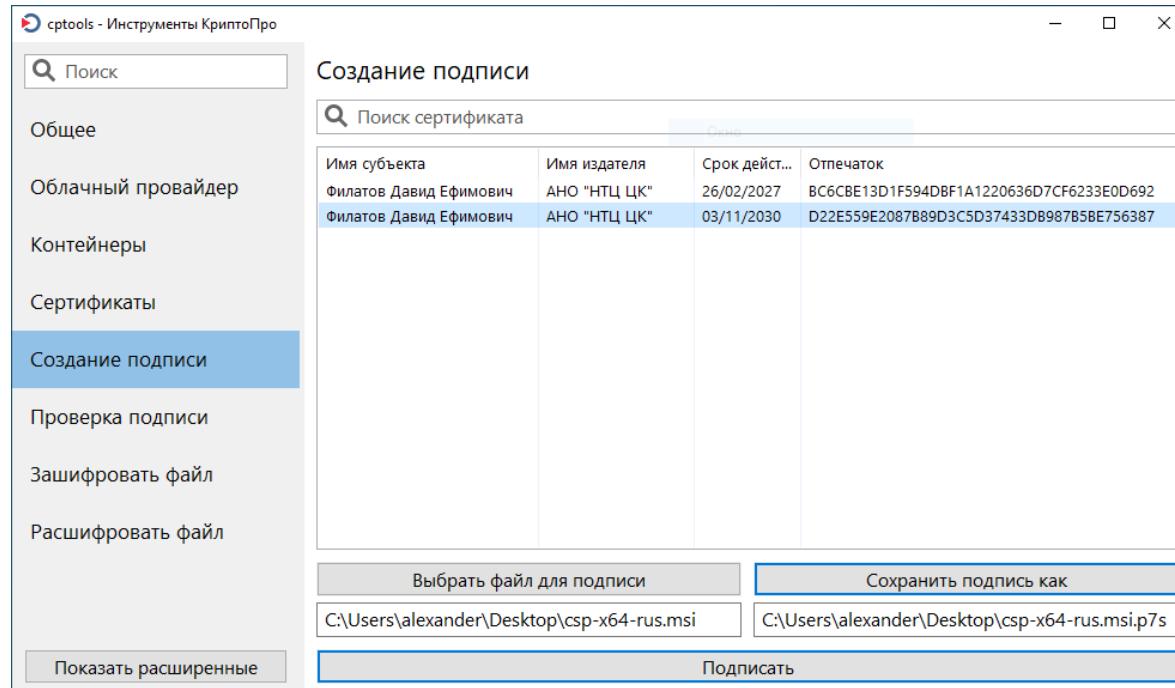
Файл в формате .sig, .p7s, .sgn

Выберите файл

Файл не выбран

.\\cryptcp.exe -sign -uMy -thumbprint d22e559e2087b89d3c5d37433db987b5be756387 -detached -der -cadesbes -fext .p7s filatov\_MDK.req

# Подпись



 Откреплённая подпись CAdES-BES



 Откреплённая подпись CAdES-BES

# Обмен дистрибутивами и подписями

Петров Алексан... : EPD\_OTUC

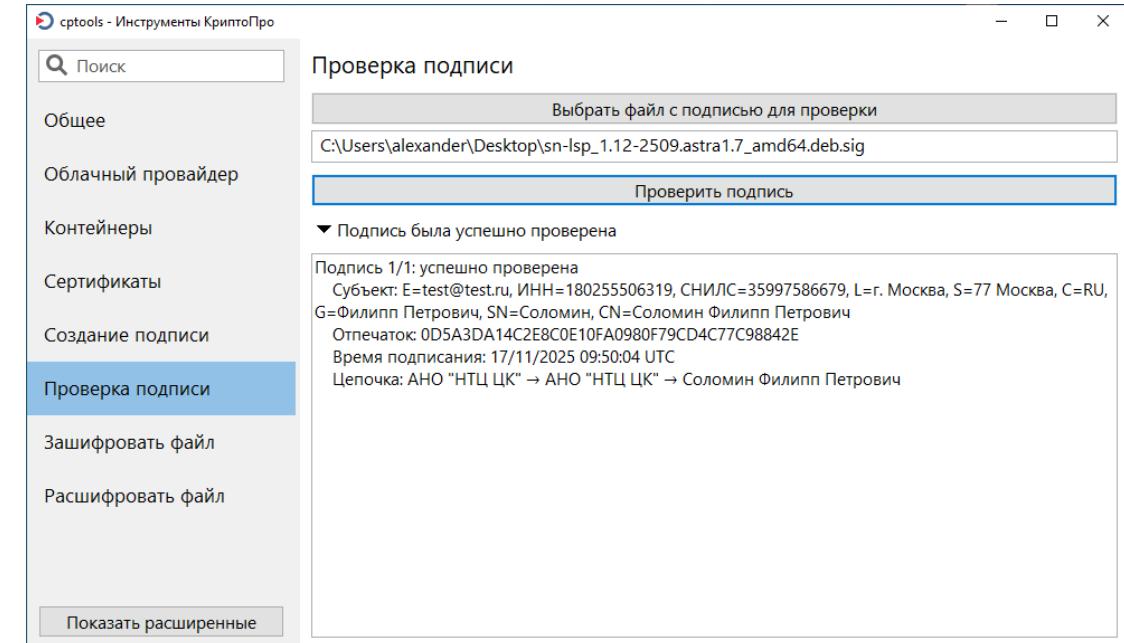
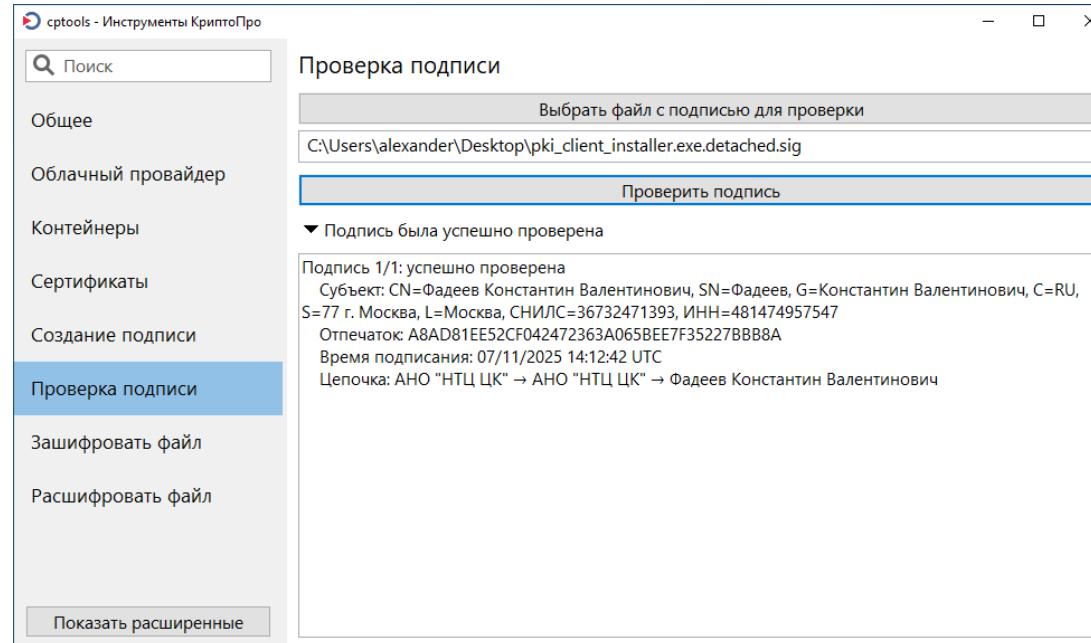
НОВЫЙ ▾ ДОПОЛНИТЕЛЬНО ▾

Общее со мной

EPD\_OTUC NEW ▾

- Подписанный дистрибутив ИнфоТeKC  
Изменен 14/11/ в 14:02 Папка 14/11/2025 17:02
- Подписанный дистрибутив Код Безопасности  
Изменен 17/11/ в 11:37
- Подписанный дистрибутив КриптоПро  
Изменен 14/11/ в 14:46

# Проверка



ViPNet PKI Client



Откреплённая подпись CAdES-BES



Secret Net LSP



Откреплённая подпись CAdES-BES



# Отзыв сертификата

Заявки    Мои сертификаты    Настройки

**Филатов Давид Ефимович**

Статус: **Действителен**  
Издатель: АНО "НТЦ ЦК"  
Дата начала: 02.12.2025 12:47:48  
Дата окончания: 02.03.2027 12:57:48  
Серийный номер:  
3430A400A7B3B2B14888495691C53EA3

[Открыть](#)   [Скачать](#)   [Отозвать](#)

**Филатов Давид Ефимович**

Статус: **Отозван**  
Дата отзыва: 01.12.2025 10:26:02  
Причина отзыва: Сертификат больше не нужен  
Издатель: АНО "НТЦ ЦК"  
Дата начала: 26.11.2025 16:55:03  
Дата окончания: 26.02.2027 17:05:03  
Серийный номер:  
1219E800A1B338AB4E4646DD342F9F80

[Открыть](#)   [Скачать](#)   [Заявка](#) →

**Филатов Давид Ефимович**

Статус: **Действителен**  
Издатель: АНО "НТЦ ЦК"  
Дата начала: 04.11.2025 23:36:21  
Дата окончания: 04.02.2027 23:46:21  
Серийный номер:  
365156018BB3B9B345C2E853595B005B

[Открыть](#)   [Скачать](#)   [Отозвать](#)

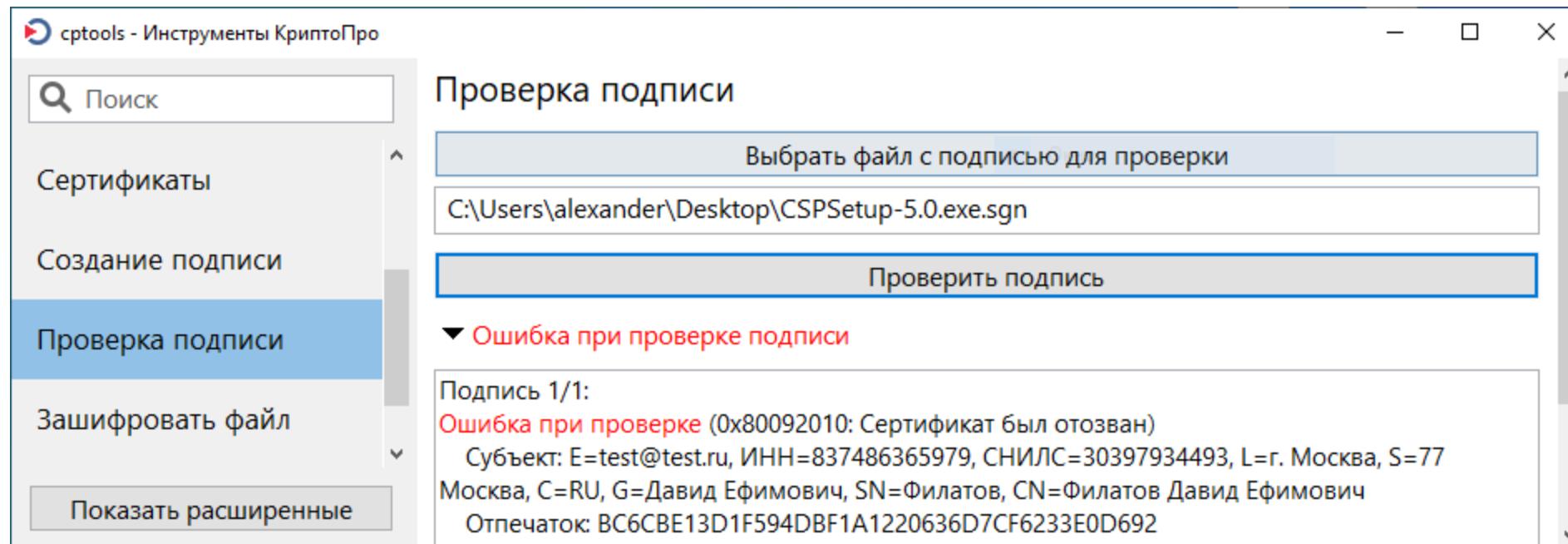
**Филатов Давид Ефимович**

Статус: **Действителен**  
Издатель: АНО "НТЦ ЦК"  
Дата начала: 04.11.2025 12:06:03  
Дата окончания: 04.02.2027 12:16:03  
Серийный номер:  
1EB998008BB33C9343E6316345256E75

[Открыть](#)   [Скачать](#)   [Отозвать](#)



# Проверка с отзыванным сертификатом



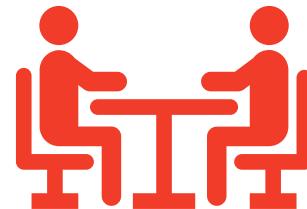
# Актуальные вопросы

- Требования, которым должно удовлетворять лицо, получающее сертификат подписи кода
- Встраивание подписи в исполняемые файлы
- Встраивание механизмов проверки подписи в ОС
- Корни доверия в АС
- Уточнение формата подписи кода
- Уточнение срока действия ключей подписи кода
- Уточнение полей в запросе и сертификате подписи кода
- Уточнение политики проверки подписи кода для отзываемых сертификатов и сертификатов с истёкшим сроком действия
- Применение сертификатов подписи кода в РБПО

# Результаты



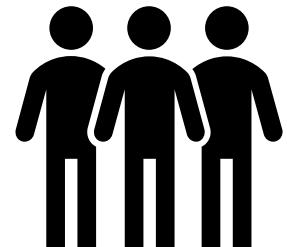
Взаимная договорённость



Совместная работа



Огласка и вовлечение



**Спасибо за внимание!**