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

Александр Петров
КриптоПро

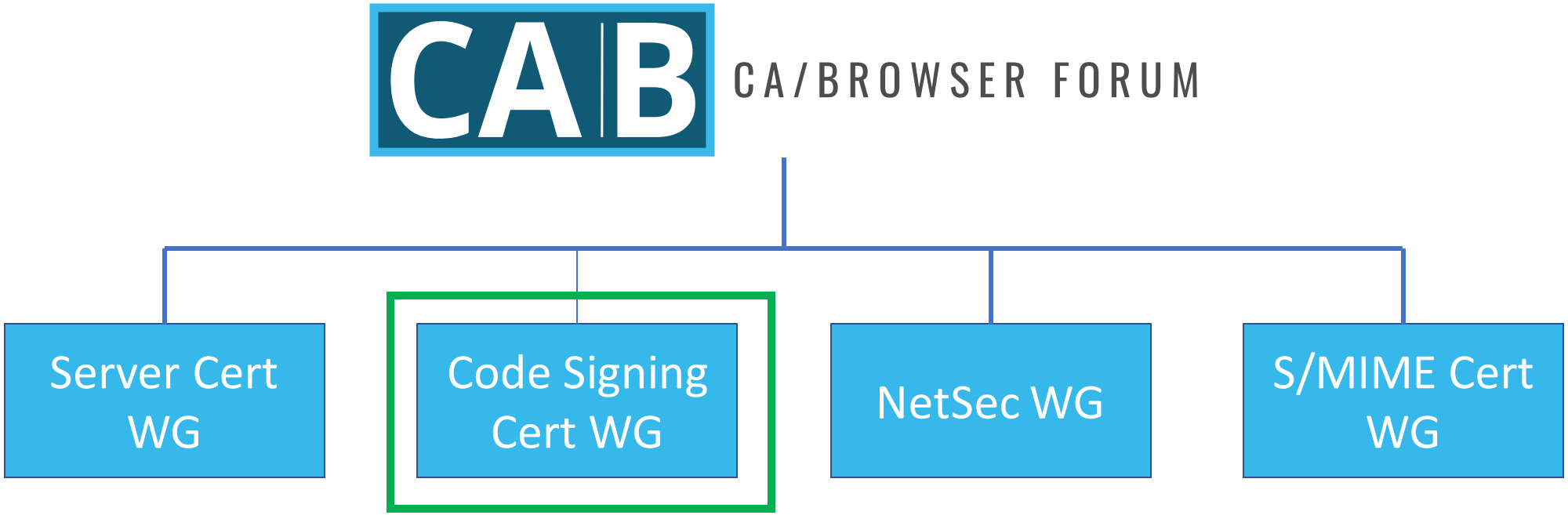
НТЦ ЦК

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

НТЦ ЦК

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.

НТЦ ЦК

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

НТЦ ЦК

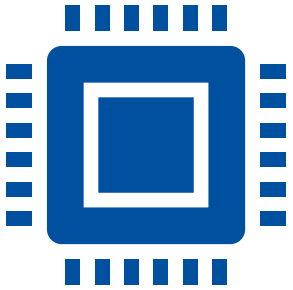
Code Signing Cert WG

- 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 …

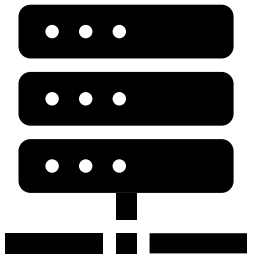
НТЦ ЦК

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



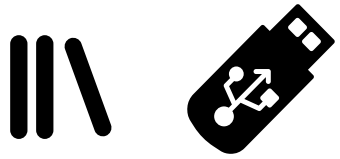
Сервис подписи

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



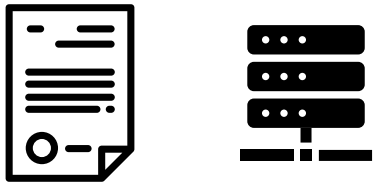
4) Внутренний или внешний аудит

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

Сложно опробовать подходы
сразу на большом количестве участников

НТЦ ЦК

КриптоПро

infotecs

НТЦ ЦК

Начало эксперимента

СБЕР

...

Яндекс

...

kaspersky

~50

Сложно опробовать подходы
сразу на большом количестве участников

НТЦ ЦК

КриптоПро

infotecs

КОД безопасности

НТЦ ЦК

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

НТЦ ЦК

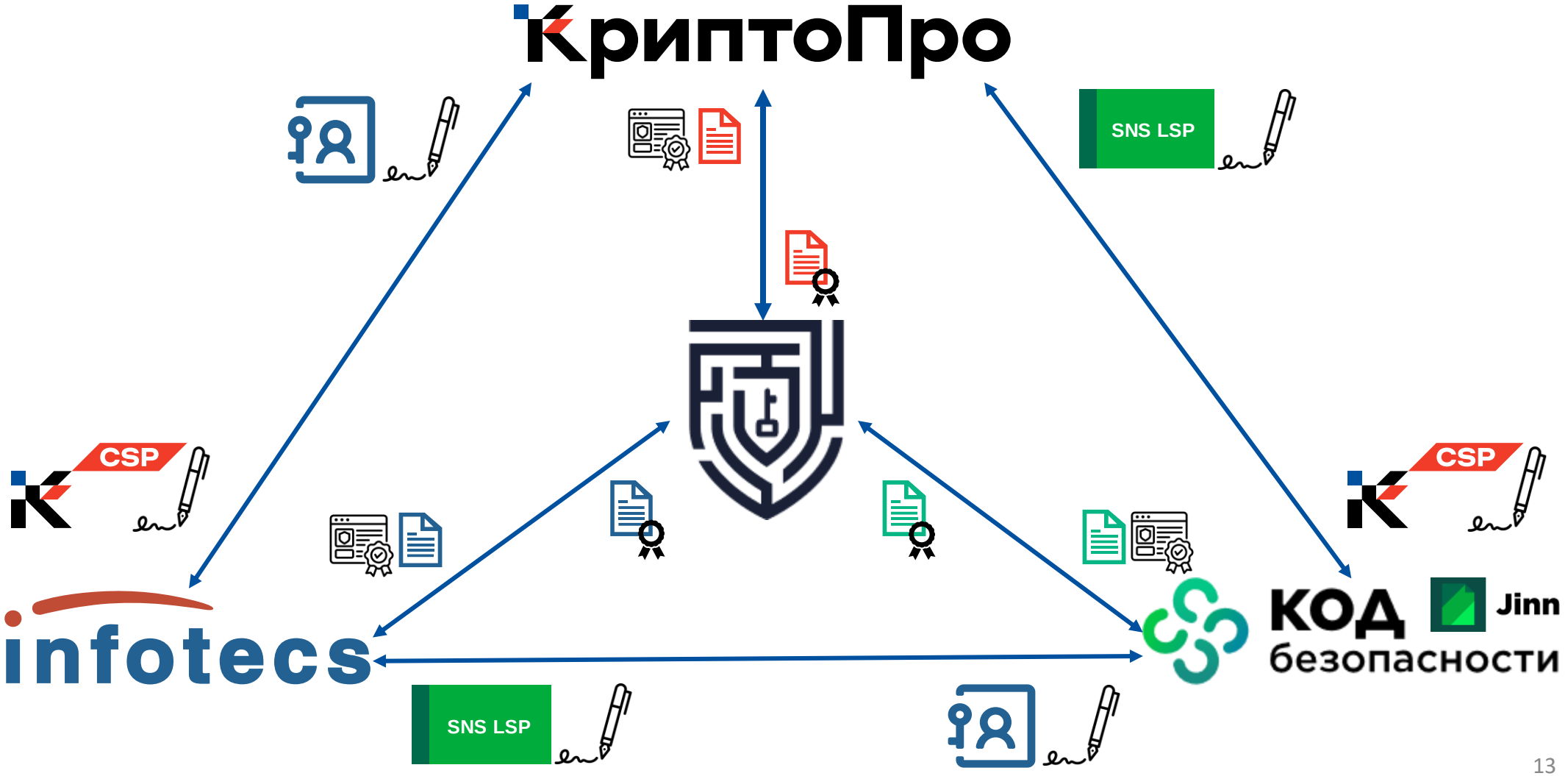
Цели 1-ой итерации

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

НТЦ ЦК

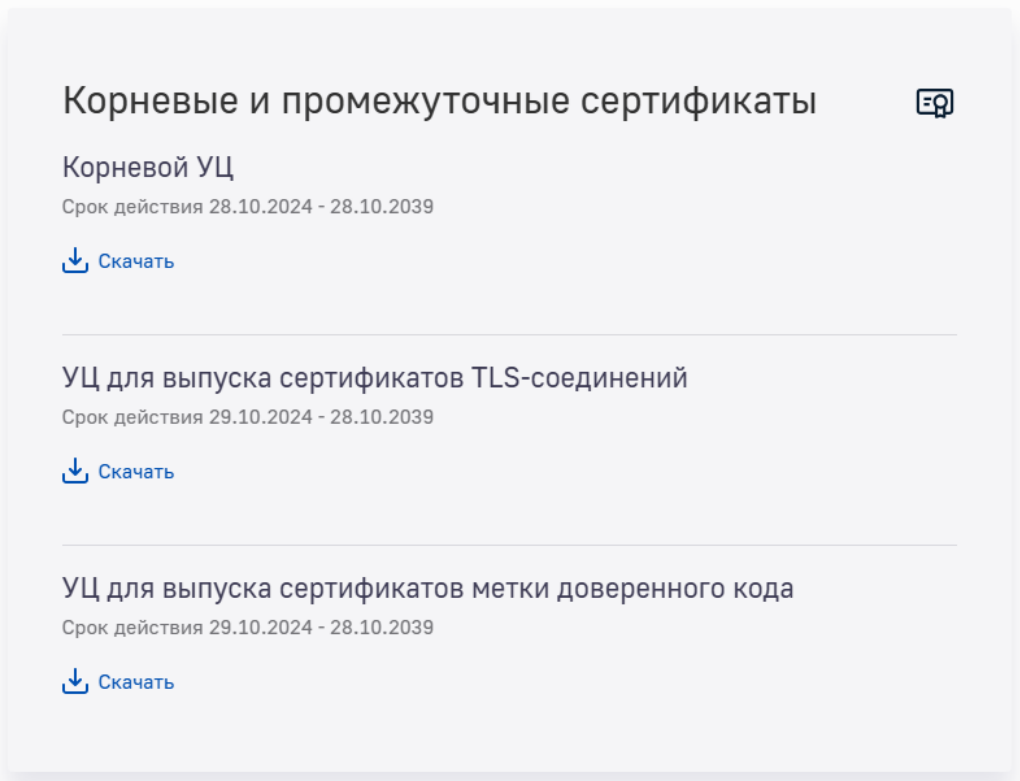
Общая структура эксперимента

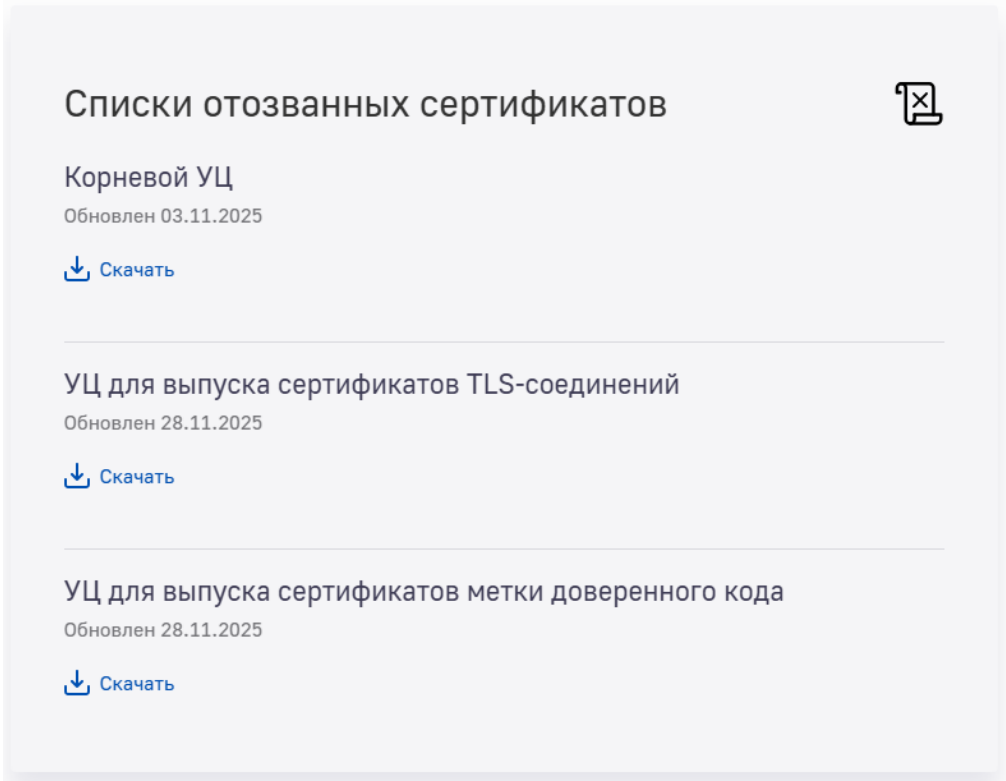


НТЦ ЦК

Настройка окружения

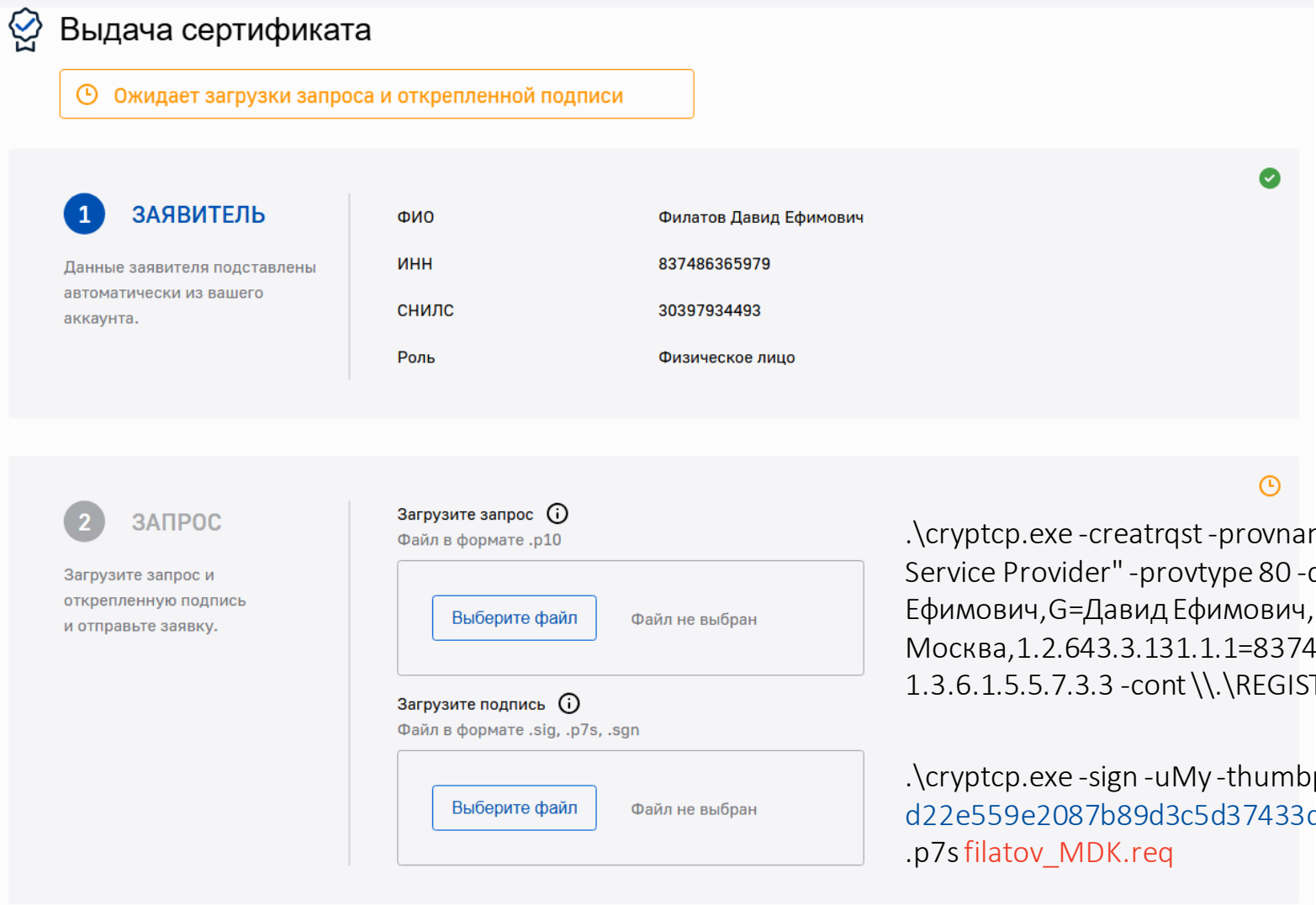
Предварительно необходимо установить требуемые сертификаты
и списки отозванных сертификатов https://otuc.digitalcryptography.ru/ca-info





НТЦ ЦК

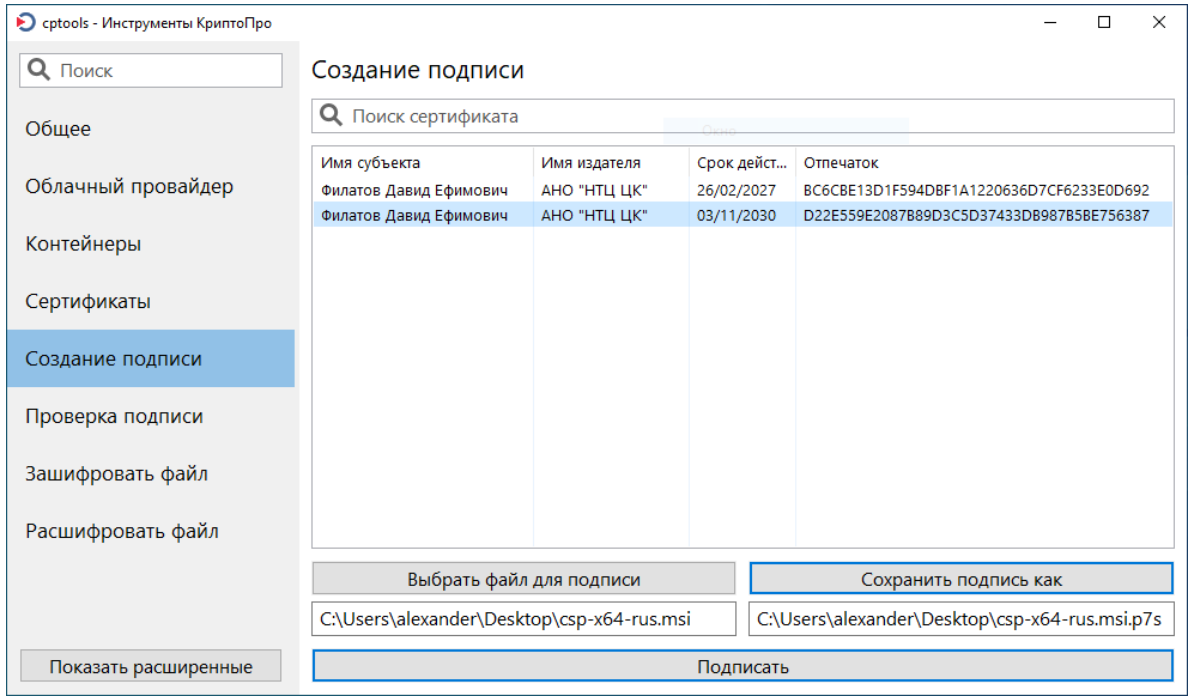
Получение сертификата подписи кода



.\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=RU,S=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

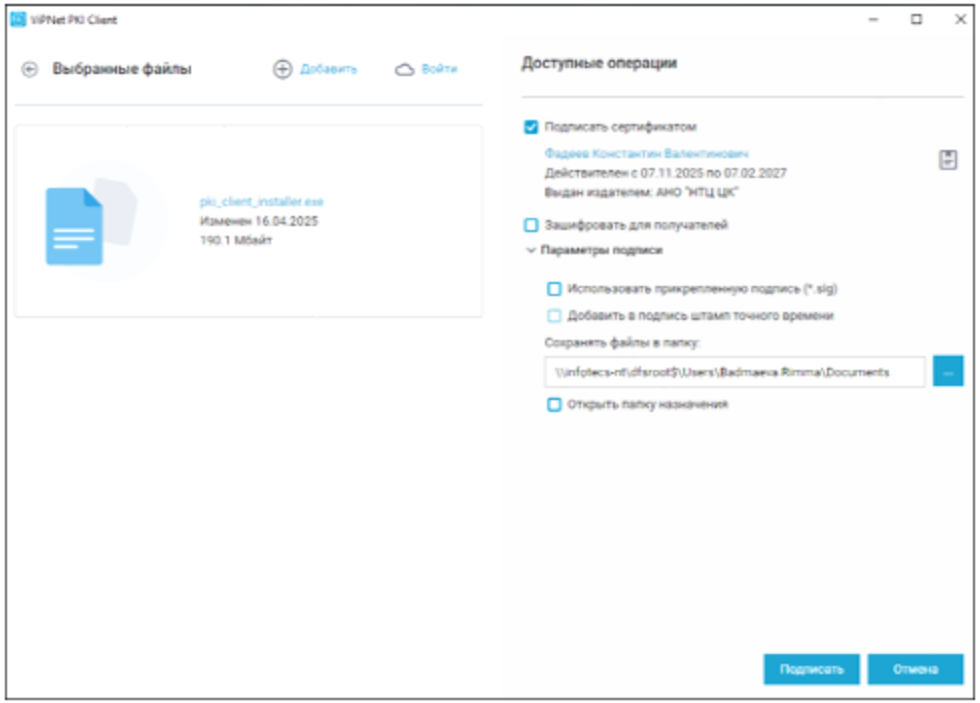
.\cryptcp.exe -sign -uMy -thumbprint d22e559e2087b89d3c5d37433db987b5be756387 -detached -der -cadesbes -fext .p7s filatov_MDK.req

Подпись



КриптоПро CSP 5.0 R3

Открепленная подпись CAdES-BES

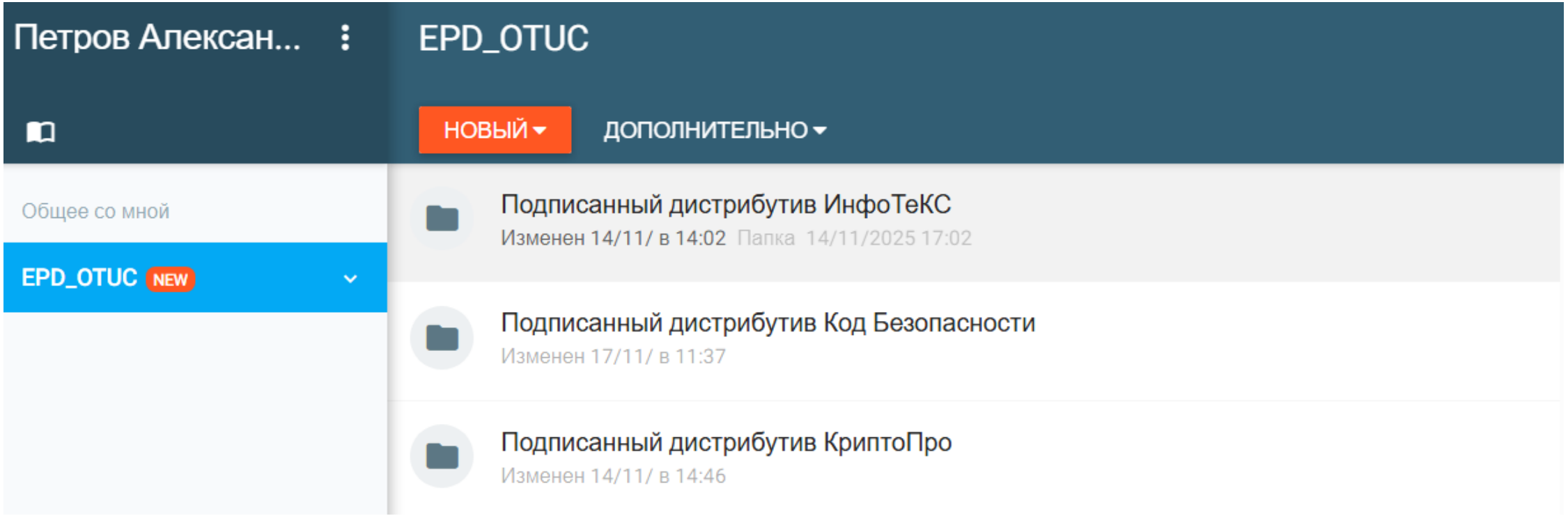


ViPNet PKI Client

Открепленная подпись CAdES-BES

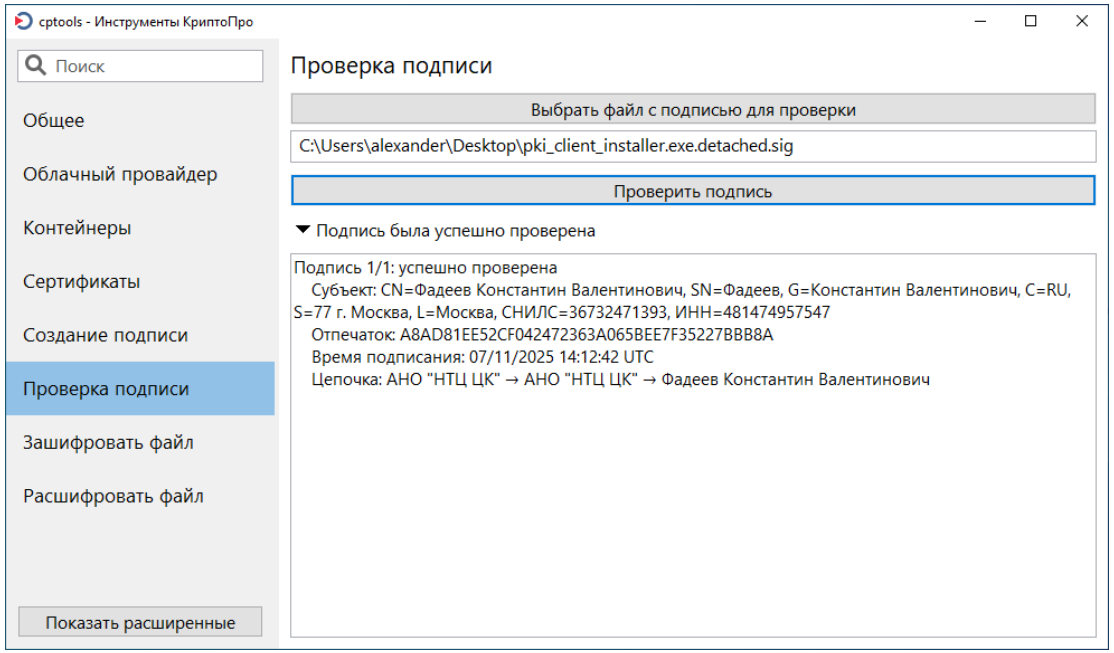
НТЦ ЦК

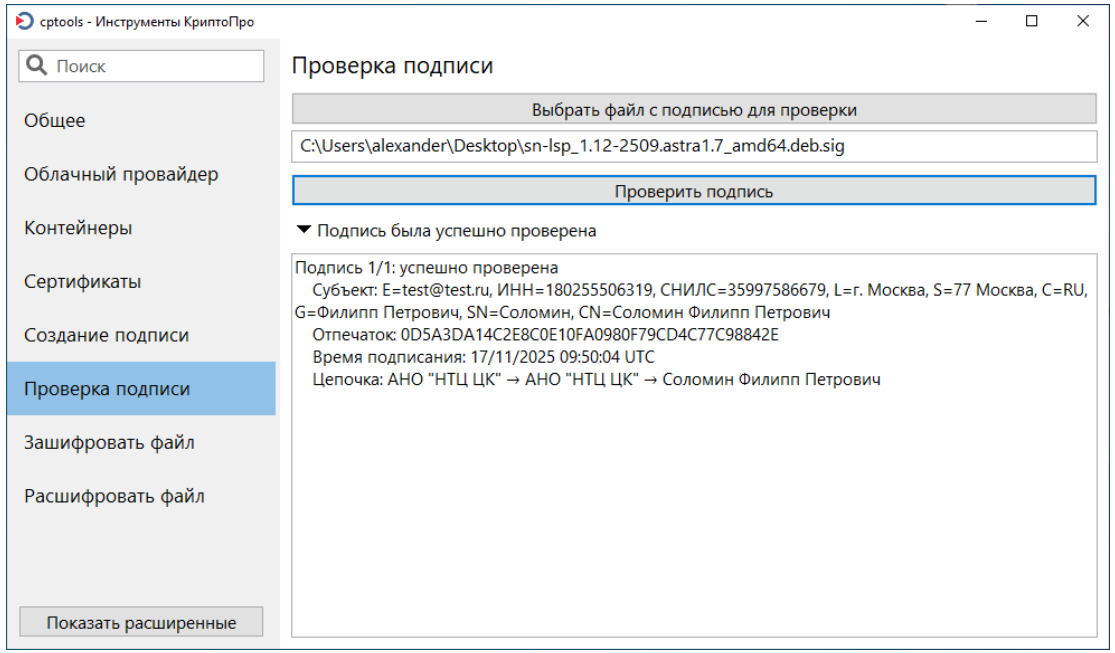
Обмен дистрибутивами и подписями



НТЦ ЦК

Проверка





ViPNet PKI Client

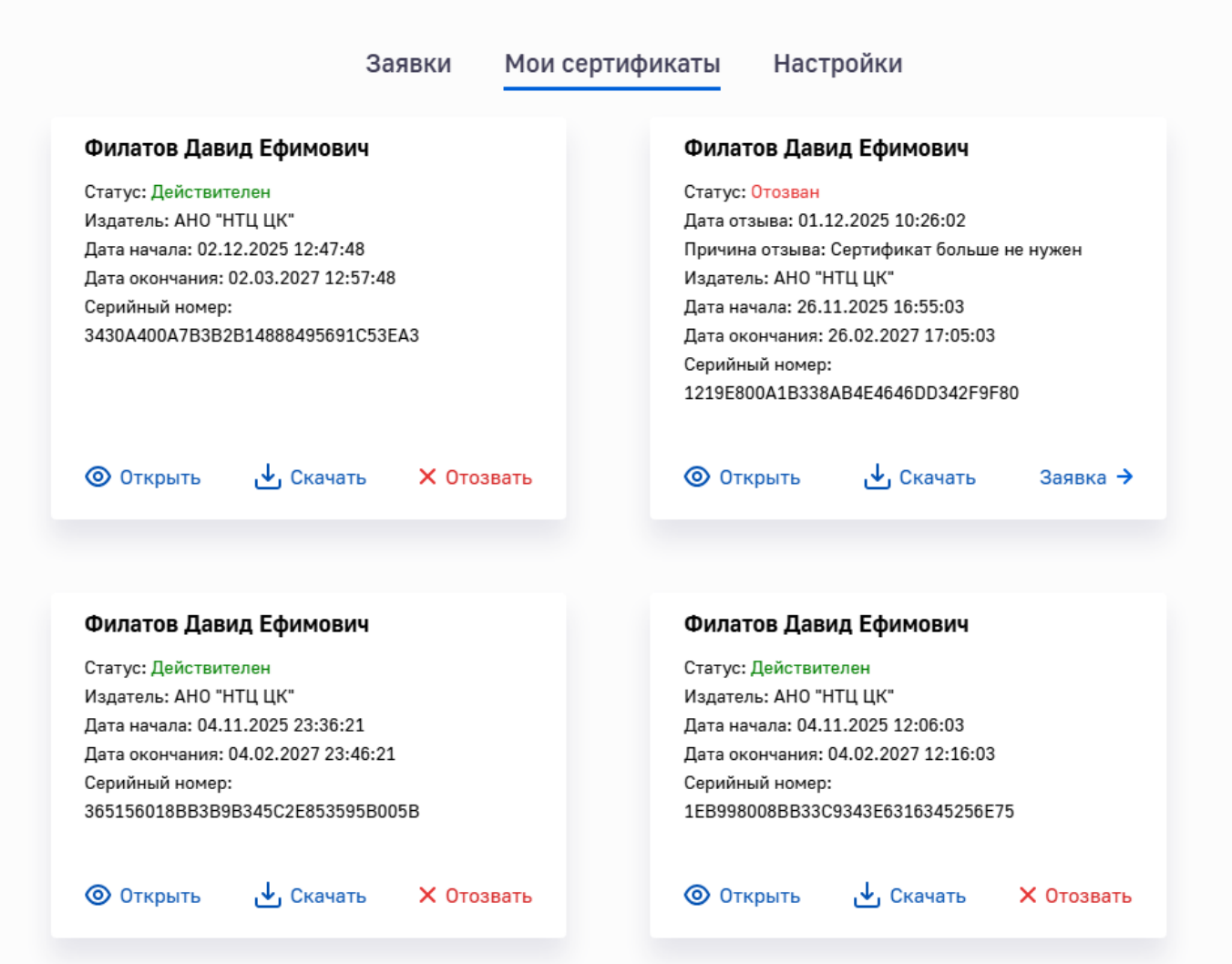
Откреплённая подпись CAdES-BES

SNS LSP Secret Net LSP

Откреплённая подпись CAdES-BES

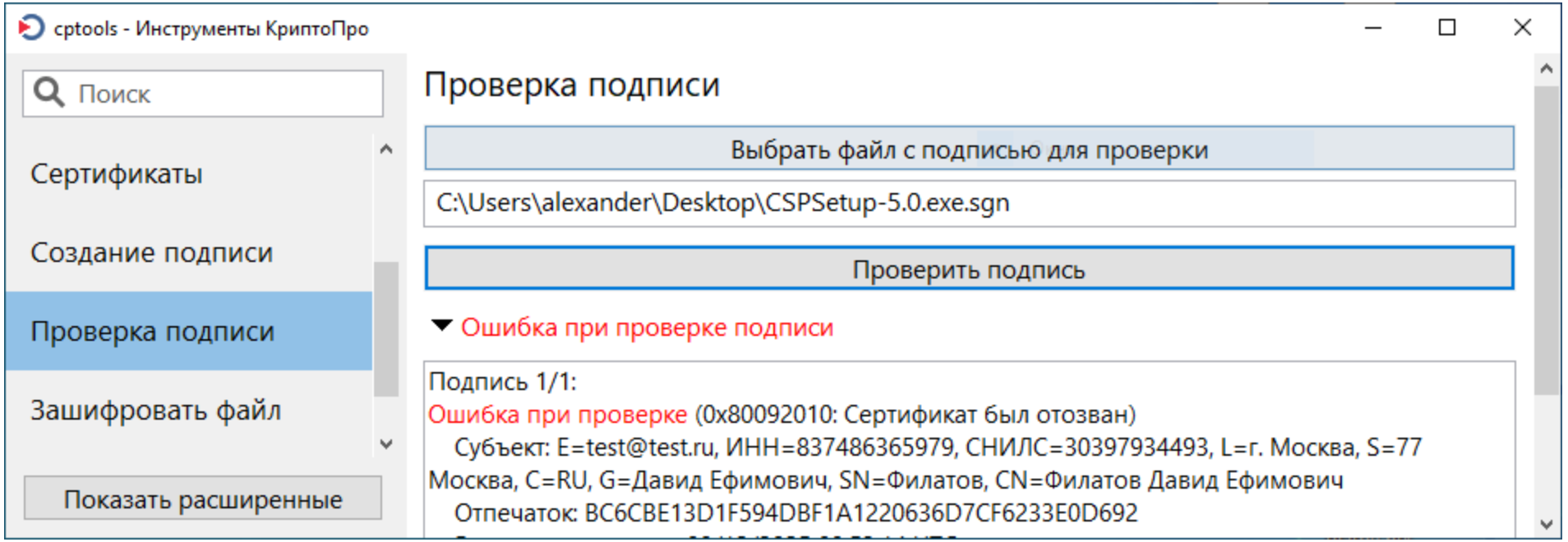
НТЦ ЦК

Отзыв сертификата



НТЦ ЦК

Проверка с отозванным сертификатом



НТЦ ЦК

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 отозванных сертификатов и сертификатов с истёкшим сроком действия
- Применение сертификатов подписи кода в РБПО

НТЦ ЦК

Результаты

Взаимная договорённость

Совместная работа

Огласка и вовлечение

Спасибо за внимание!