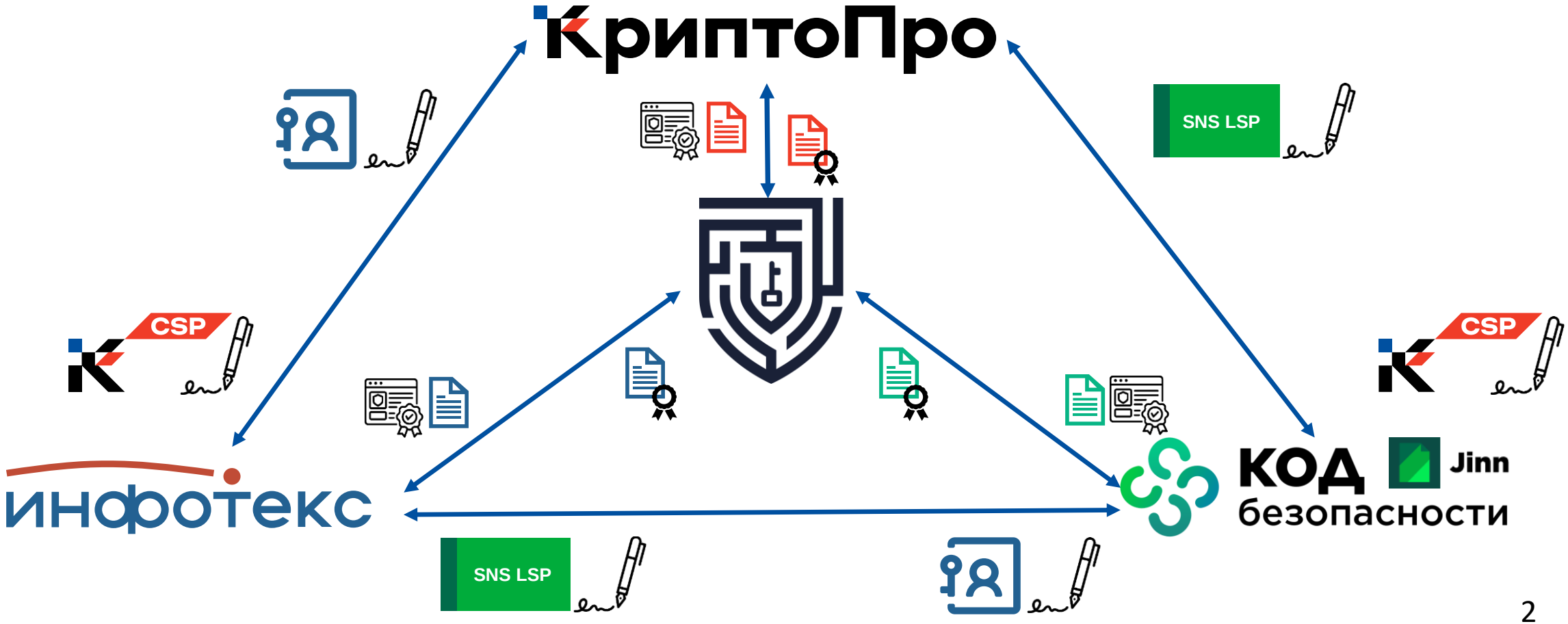
РусКрипто XXVIII НАУЧНО-ПРАКТИЧЕСКАЯ КОНФЕРЕНЦИЯ

Проект Регламента подписи дистрибутивов российского ПО

Александр Петров,
ведущий инженер-аналитик
КриптоПро

Анастасия Калугина, руководитель направления безопасной разработки и инфраструктуры
инфотекс

Общая структура эксперимента подписи дистрибутивов ПО

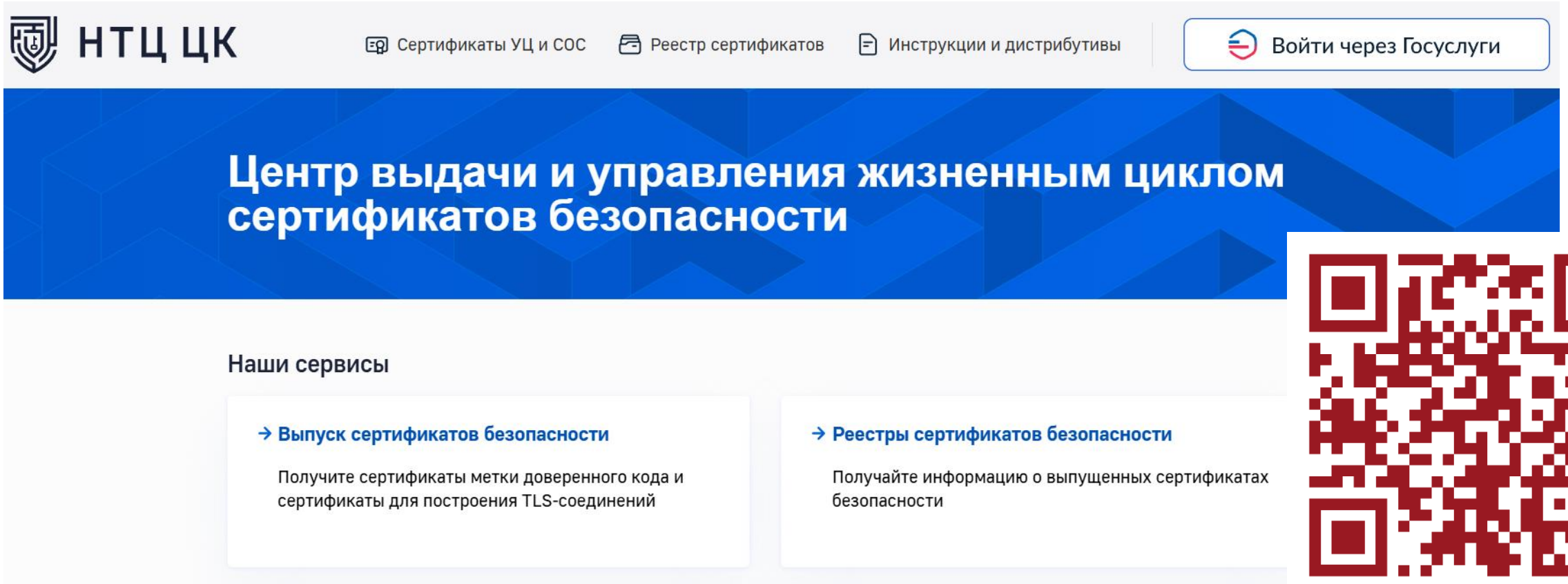


Цели 1-ой итерации
(эксперимент, проведённый в рамках РГ)

- Проработать подход по обеспечению целостности и подлинности дистрибутивов ПО
- Определить формат и вид ЭП
- Протестировать использование отечественного УЦ в качестве корня доверия (система ОТУЦ)
- Протестировать использование отечественных криптографических средств

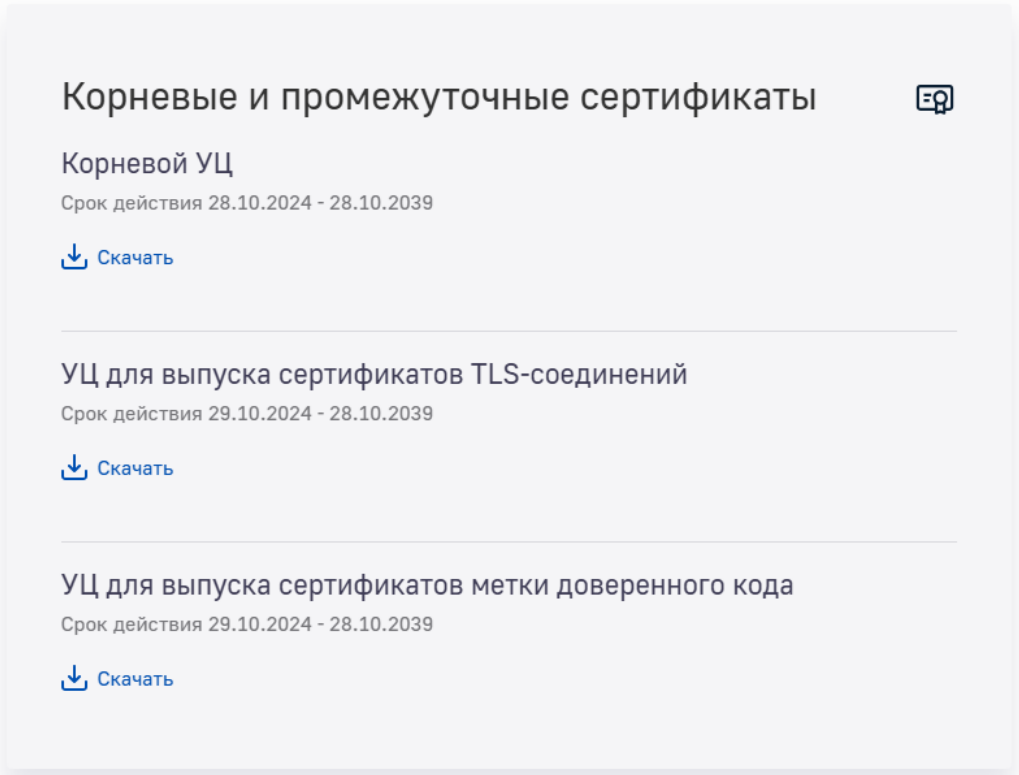
Регистрация в ЛК ЦВУЖЦ-СБ ОТУЦ

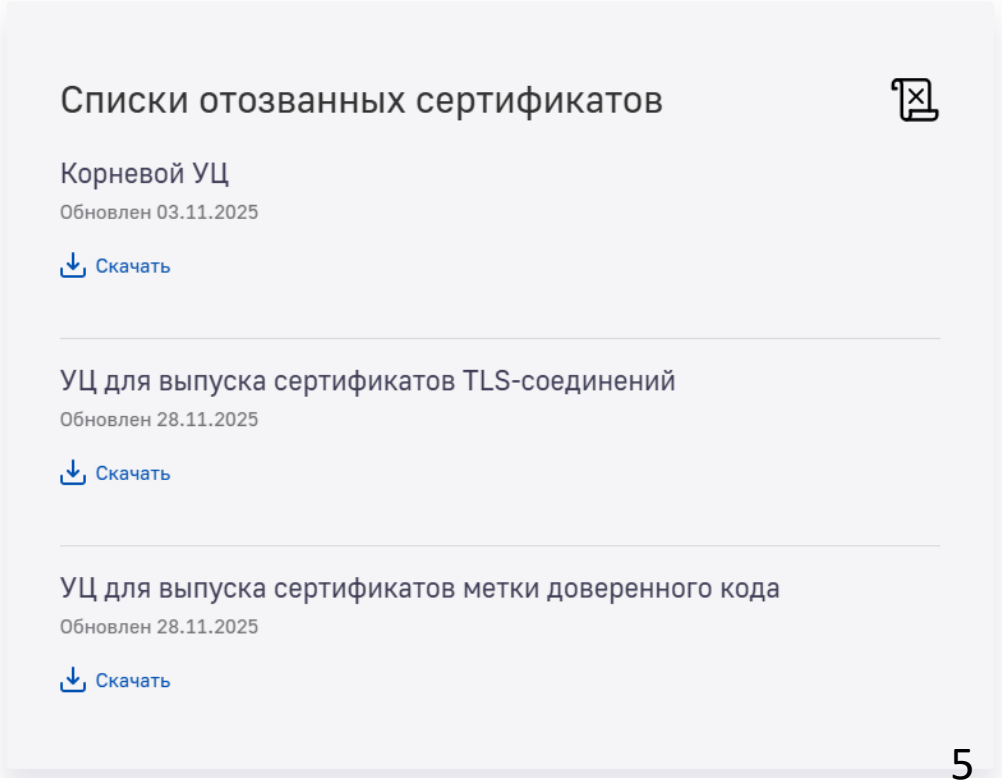
https://otuc.digitalcryptography.ru



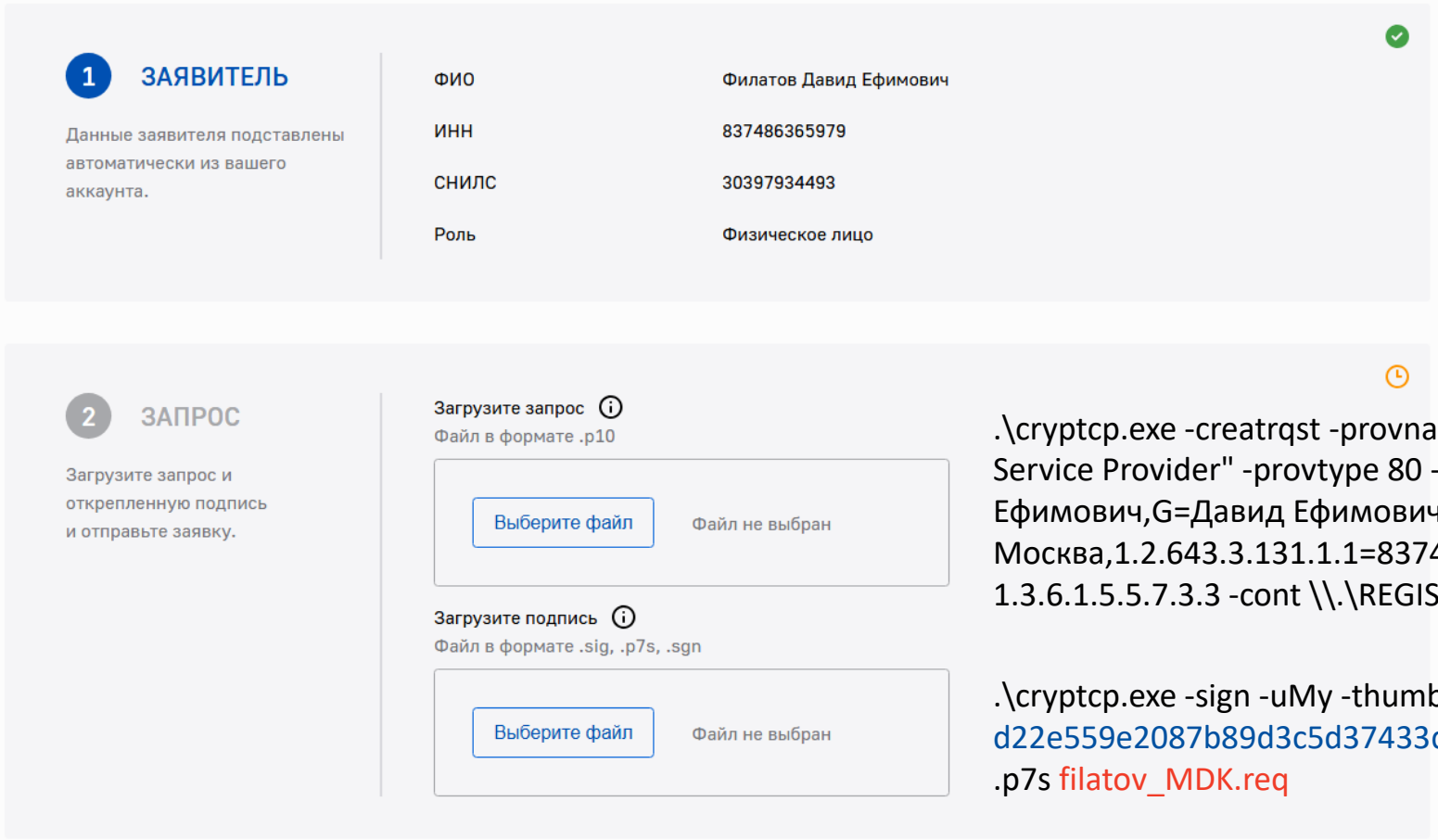
Настройка окружения

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





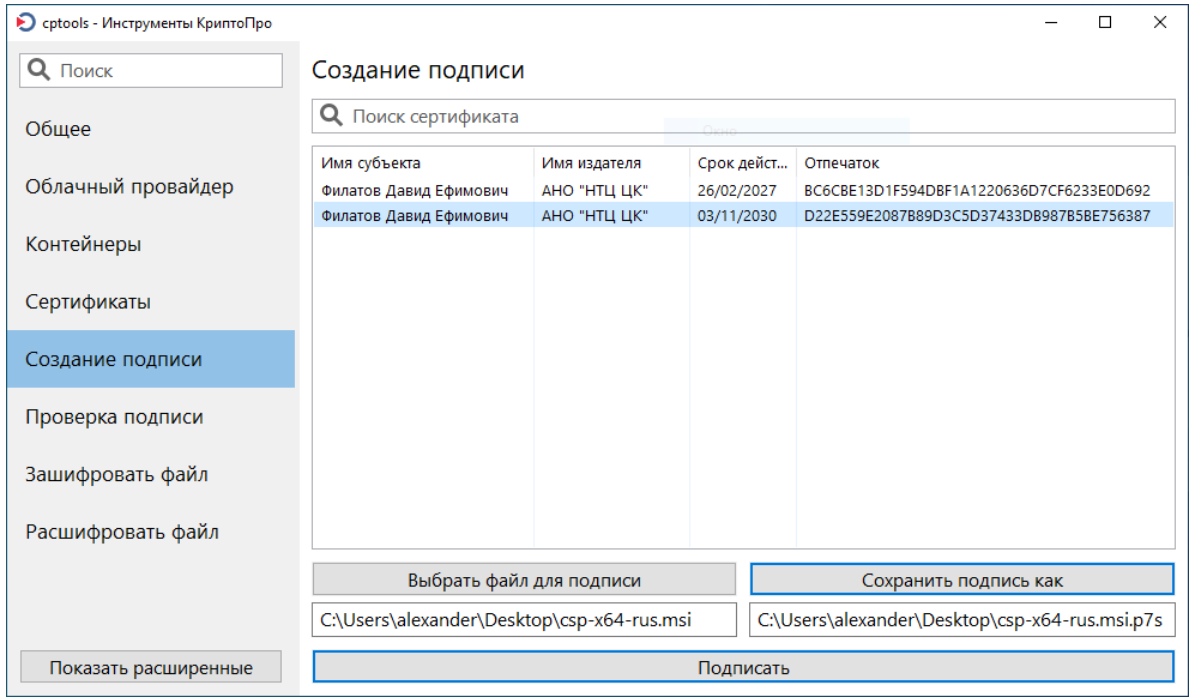
Получение сертификата подписи дистрибутивов ПО



.\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

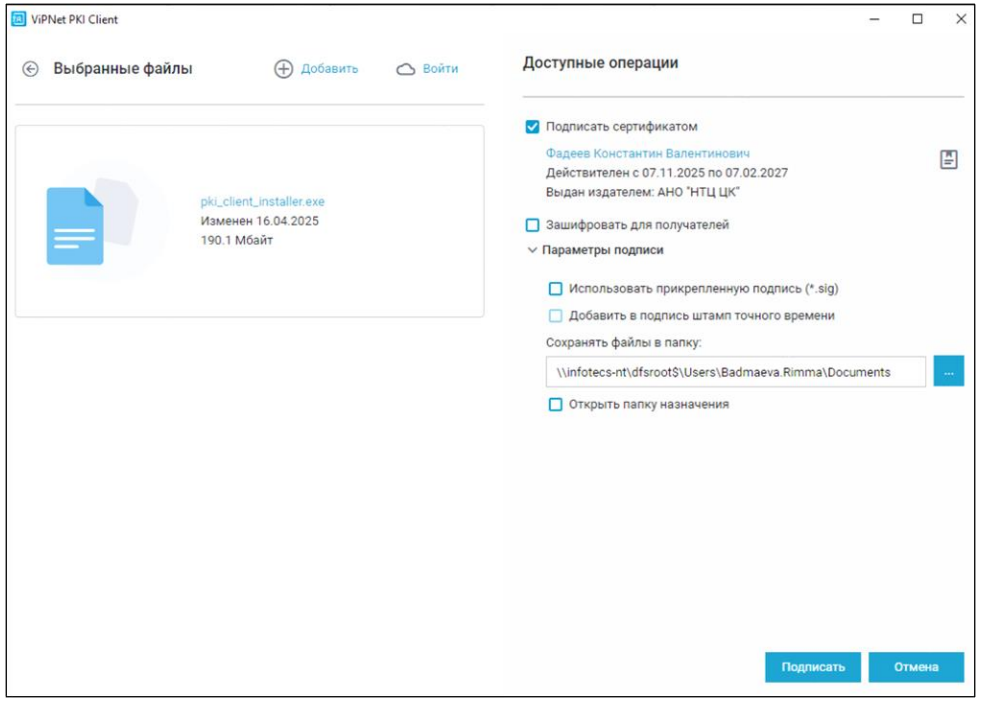
.\cryptcp.exe -sign -uMy -thumbprint d22e559e2087b89d3c5d37433db987b5be756387 -detached -der -cadesbes -fext .p7s filatov_MDK.req

Подпись



КриптоПро CSP 5.0 R3

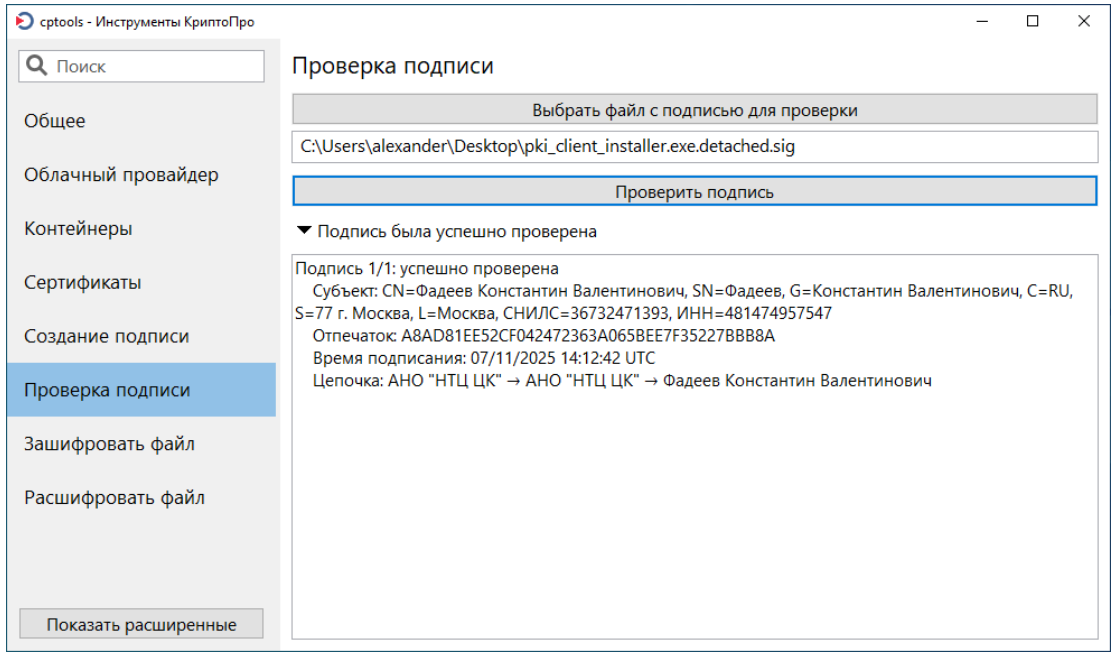
Откреплённая подпись CAdES-BES



ViPNet PKI Client

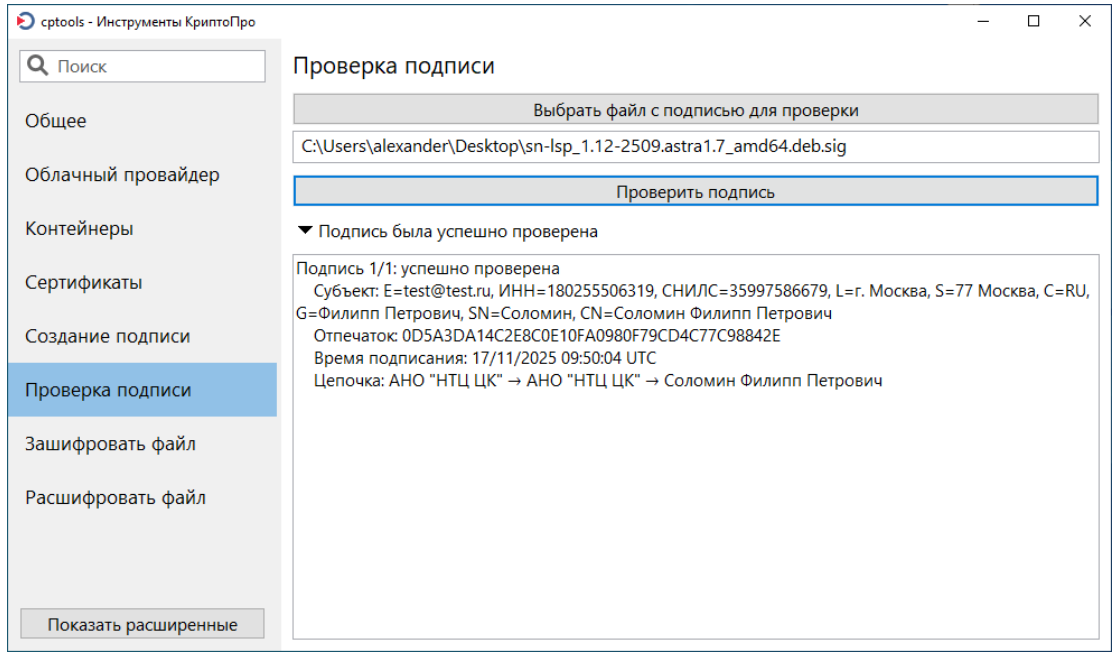
Откреплённая подпись CAdES-BES

Проверка подписи



ViPNet PKI Client

Открепленная подпись CAdES-BES



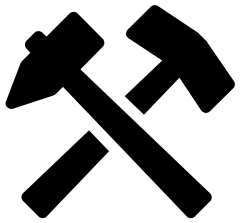
SNS LSP

Открепленная подпись CAdES-BES

Результаты 1-ой итерации

Совместная работа

Взаимные договорённости



Разработка подхода и тестирование механизмов на практике

Проблемы и их инструменты решения

Единый подход при разработке отечественного ПО в части обеспечения:

- целостности и подлинности разрабатываемого ПО
- аутентификации субъектов и объектов взаимодействия

РГ ЕПД

РБПО

СКЗИ, СЭП, УЦ

ОТУЦ

? Функционирующий доверенный УЦ для выпуска сертификатов безопасности

? Нормативное регулирование в части подписи ПО

? Обеспечение технологической независимости

Проблемы и их инструменты решения

? Единый подход при разработке отечественного ПО в части обеспечения:
- целостности и подлинности разрабатываемого ПО
- аутентификации субъектов и объектов взаимодействия

✓ Функционирующий доверенный УЦ для выпуска сертификатов безопасности

ОТУЦ

? Нормативное регулирование в части подписи ПО

? Обеспечение технологической независимости

Проблемы и их инструменты решения

? Единый подход при разработке отечественного ПО в части обеспечения:
- целостности и подлинности разрабатываемого ПО
- аутентификации субъектов и объектов взаимодействия

? Функционирующий доверенный УЦ для выпуска сертификатов безопасности

? Нормативное регулирование в части подписи ПО

✓ Обеспечение технологической независимости

СКЗИ, СЭП, УЦ

ОТУЦ

ОС

Проблемы и их инструменты решения

? Единый подход при разработке отечественного ПО в части обеспечения:
- целостности и подлинности разрабатываемого ПО
- аутентификации субъектов и объектов взаимодействия

? Функционирующий доверенный УЦ для выпуска сертификатов безопасности

✓ Нормативное регулирование в части подписи ПО

РБПО, +(?)

? Обеспечение технологической независимости

Цели 2-ой итерации

Первые шаги:

►Проработать процедуру обеспечения и проверки целостности и подлинности дистрибутивов ПО

►Проработать процедуры взаимодействия между организациями

При проработке учитывать необходимость в дальнейшем автоматизации!

ЕДИНОЕ
ПРОСТРАНСТВО ДОВЕРИЯ

проект
Регламента

НТЦ ЦК
КриптоПро
infotecs
КОД безопасности

Ещё на шаг ближе

1

ЕДИНОЕ
ПРОСТРАНСТВО ДОВЕРИЯ

Регламент
подписи* дистрибутива ПО
и проверки его подписи

2

ЕДИНОЕ
ПРОСТРАНСТВО ДОВЕРИЯ

Регламент
внешних взаимодействий
между организациями

Версия 1.0

Направления доработок

Доработка процессов подписи
дистрибутива ПО
в организации-разработчике

Разработка процедуры проверки подписи
дистрибутива ПО потребителем

Разработка процедур взаимодействия
между внешними участниками

Системный подход – верхнеуровневая цель

Разработка и регламентация системного подхода,
гарантирующего решение существующих проблем в части обеспечения доверия продуктов российской разработки

Задачи

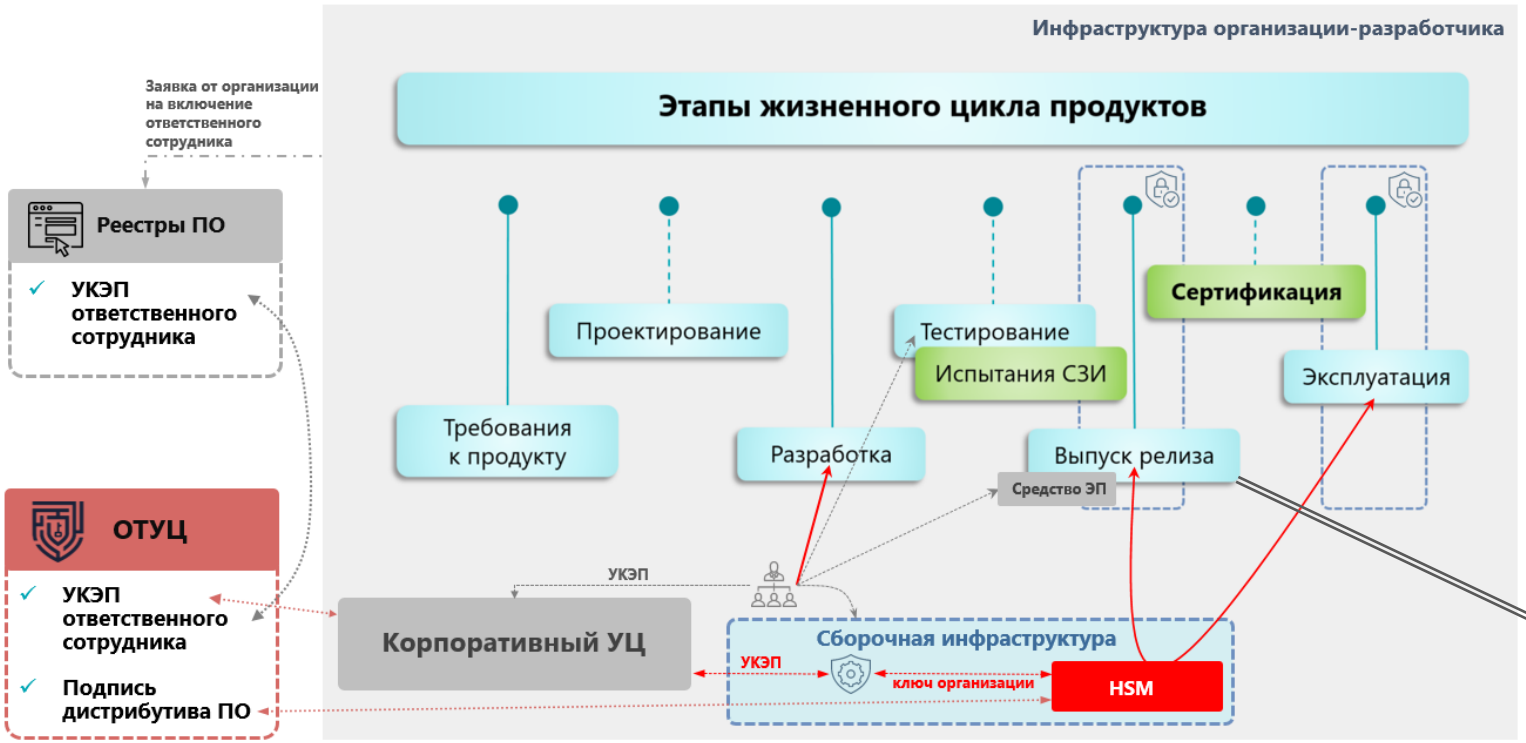
Разработка требований

- Требования к механизмам и технологиям ✓
- Типовое конфигурирование инфраструктуры ✓
- Жизненный цикл сертификатов
- Организация процессов взаимодействия (всех участников взаимодействия)

Регламентация

- Определение корневых доверенных УЦ
- Нормативное регулирование по каждому направлению

Подпись дистрибутива ПО



✓ Минимально необходимые доработки

Единое пространство доверия (ЕПД)

ЕДИНОЕ ПРОСТРАНСТВО ДОВЕРИЯ

Регламент
подписи* дистрибутива ПО и проверки его подписи

1

Версия 1.0

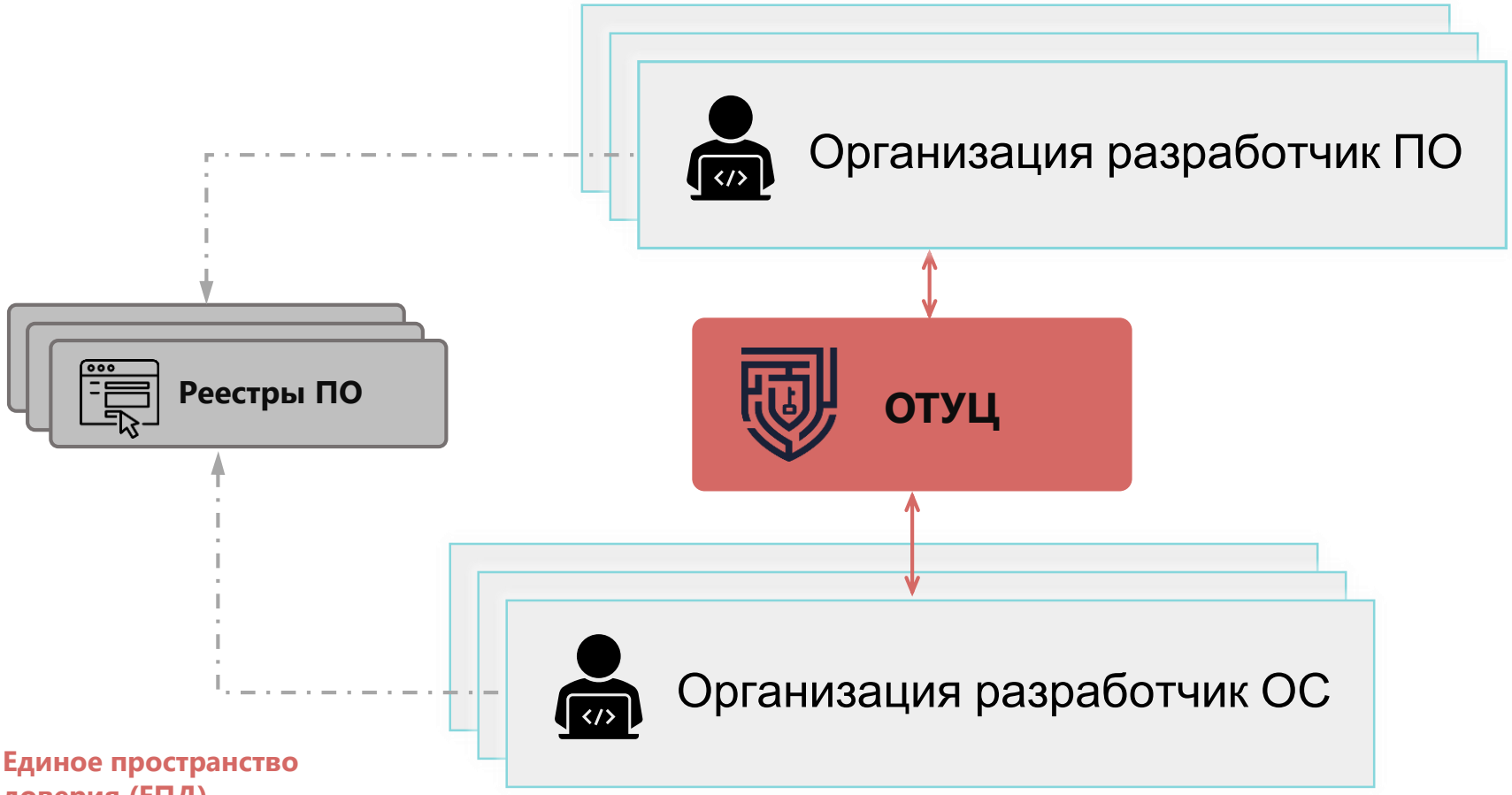
Потребитель ПО

проверка целостности и подлинности ПО

- ✓ Ручная проверка **Средство ЭП**
- ✓ Проверка при установке, обновлении и функционировании
- ✓ Проверка средствами ОС
- ✓ Аппаратный корень доверия

* Используя метку доверенного кода из системы ОТУЦ

Участники внешних взаимодействий



Единое пространство доверия (ЕПД)

ЕДИНОЕ ПРОСТРАНСТВО ДОВЕРИЯ

Регламент
внешних взаимодействий между организациями

2

Версия 1.0

Результат на текущий момент

- ✓ *(итерация 1)* Разработан проект подхода обеспечения целостности и подлинности дистрибутивов ПО
- ✓ *(итерация 1)* ОТУЦ использован в качестве корневого доверенного УЦ
- ✓ *(итерация 1)* Протестировано использование системы ОТУЦ при кросс-верификации целостности и подлинности дистрибутивов ПО
- ⚑ (текущая итерация 2) Разработаны минимальные типовые доработки процессов (внутренние и внешние взаимодействия)

✓ Текущие результаты уже можно применять в процессах организаций-разработчиков

Текущие ограничения

- Только ручная проверка
- Отсутствие полной интеграции в процессы РБПО
- Срок действия дистрибутивов ПО ограничен сроком действия сертификата подписи
- Отсутствие предустановленного корня доверия

Вопросы и ответы

РусКрипто
XXVIII НАУЧНО-ПРАКТИЧЕСКАЯ КОНФЕРЕНЦИЯ

Спасибо за внимание!

Александр Петров,
ведущий инженер-аналитик

КриптоПро

alexander@cryptopro.ru

Анастасия Калугина, руководитель направления безопасной разработки и инфраструктуры

инфотекс

akalugina@infotecs.ru