



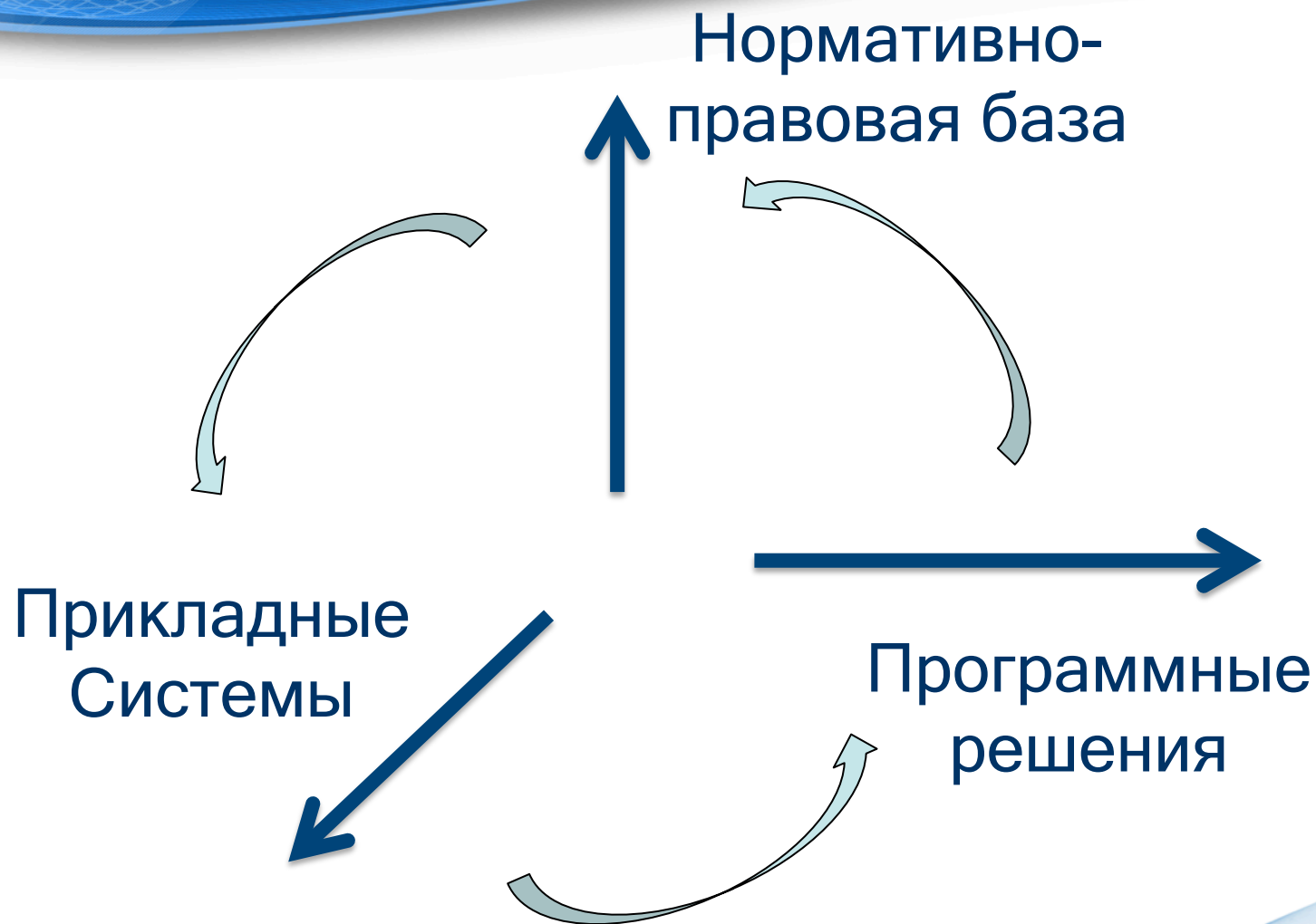
ГАЗИНФОРМСЕРВИС

Интероперабельность РКИ задачи и решения

Начальник отдела разработки средств защиты
Сергей Петров

Интероперабельность РКИ

Вектор развития



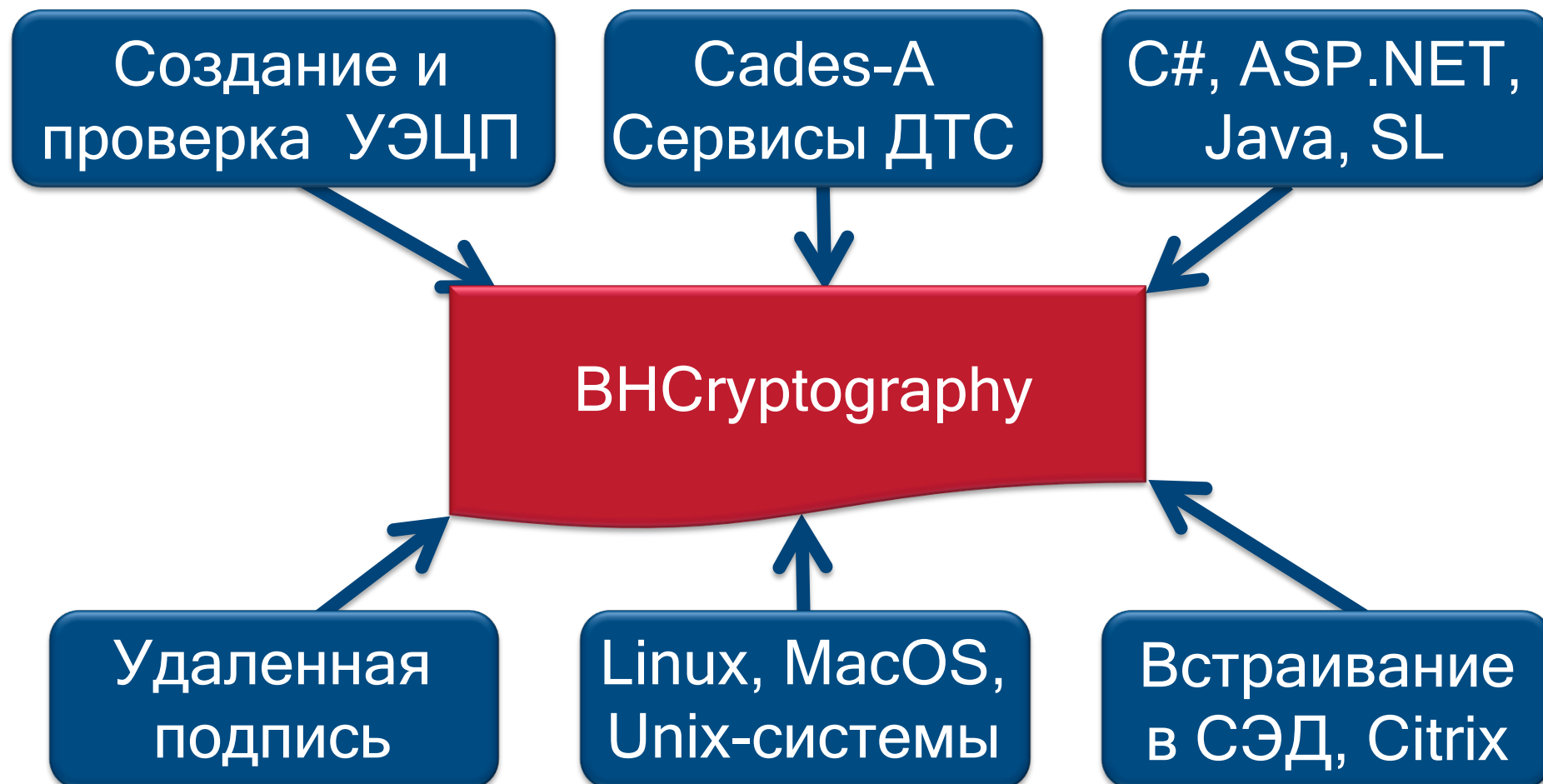
Технические проблемы РКІ

- РКІ окружение пользователя
- Трансграничность
- Парк ОС и платформ
- Парк ЭДО
- Технические ограничения
- Закон vs технологии



Интероперабельность PKI

Архитектурное решение



Интероперабельность PKI

PKI окружение пользователя

Блокхост-ЭЦП 2.0

Блокхост ЭЦП 2.0

Файл Справка

Подпись

- Подписать
- Проверить
- Добавить подпись
- Заверить подпись

Шифрование

- Зашифровать
- Расшифровать
- Удалить файлы

Подпись и Шифрование

- Подписать и зашифровать
- Расшифровать и проверить

Запросы на сертификат

- Создать запрос на сертификат
- Установить личный сертификат
- Сертификаты в контейнерах

Настройки

- Управление сертификатами
- Настройки приложения

Подпись документов

Имя файла	Размер	Пу
Описание применения.doc	1.9 M6	D:/BlockHostEDS2.0/BHCryptography/test_1/
Описание программы.doc	1.4 M6	D:/BlockHostEDS2.0/BHCryptography/test_1/
Описание применения_new.doc	1.8 M6	D:/BlockHostEDS2.0/BHCryptography/test_1/
Программные интерфейсы BHCryptography.docx	44.1 K6	D:/BlockHostEDS2.0/BHCryptography/test_1/

Добавить Удалить все Удалить

Сертификат подписчика

Идентификатор (CN)	Антон
Страна	BY
Организация	ГИС
Издатель	Test Center CRYPTO-PRO
Версия	3
Серийный номер	75:43:ab:37:00:02:00:02:81:2d
Действителен с	06.09.2012 09:45:00
Действителен до	06.12.2013 09:55:00

Выбор сертификата

Параметры подписи

- Создать отдельную подпись
- Вложить внутренний штамп времени
- Создать усовершенствованную подпись

Комментарий

Подписать

Выполнение операции

Операция выполнена успешно!

100%

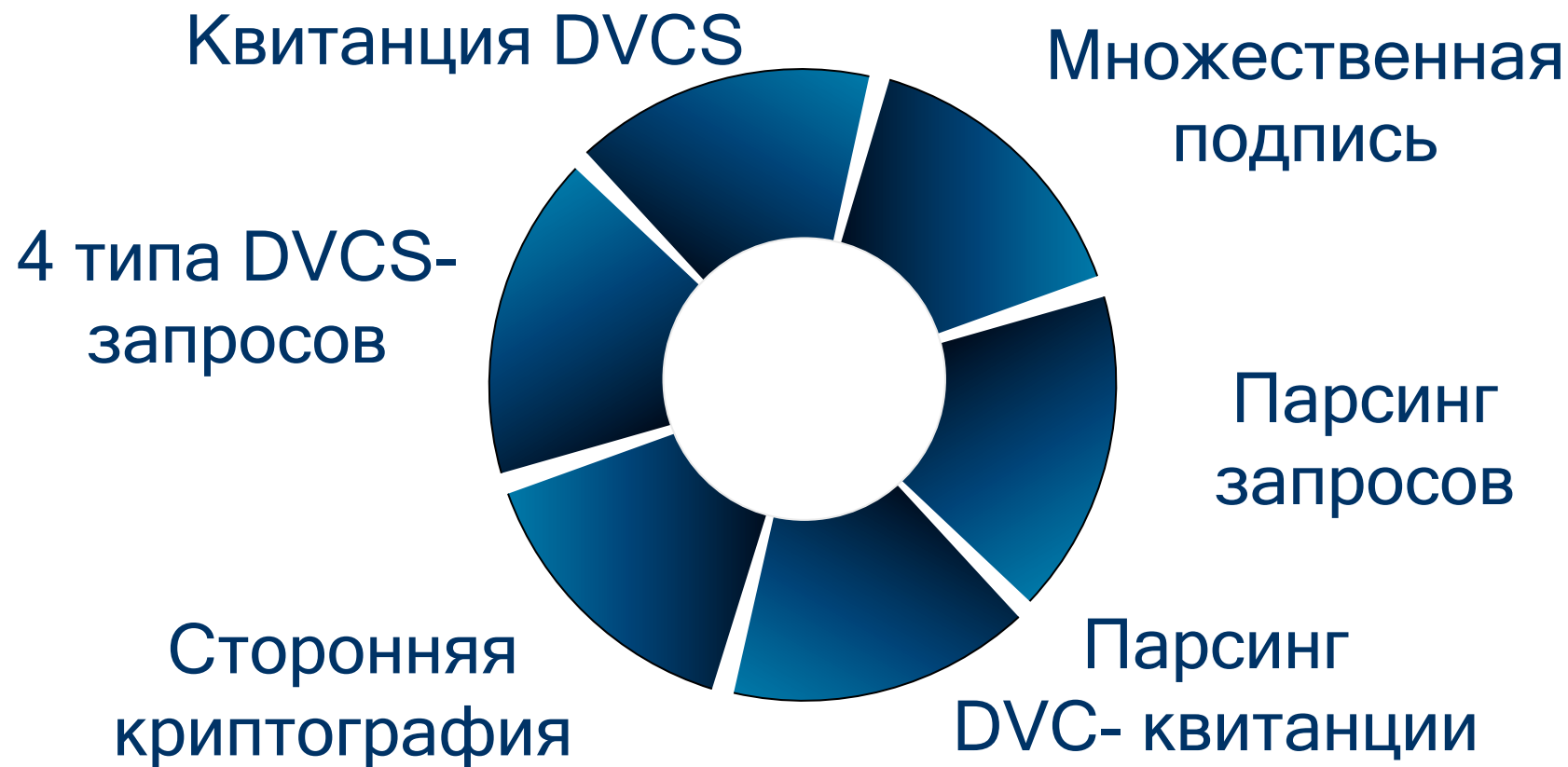
Детальный результат Закрыть

Интероперабельность PKI

Трансграничность vs CSP

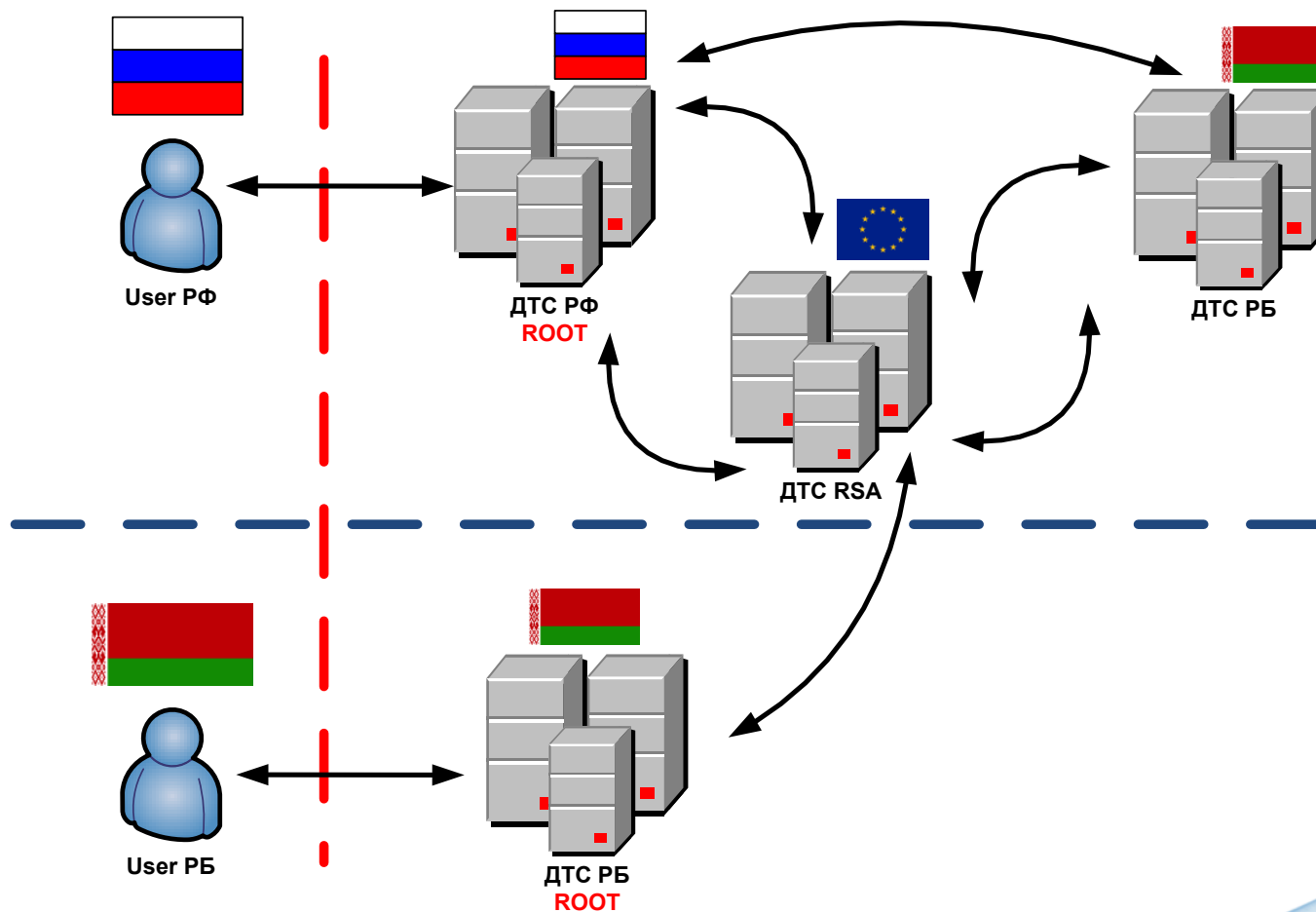


ГАЗИНФОРМСЕРВИС

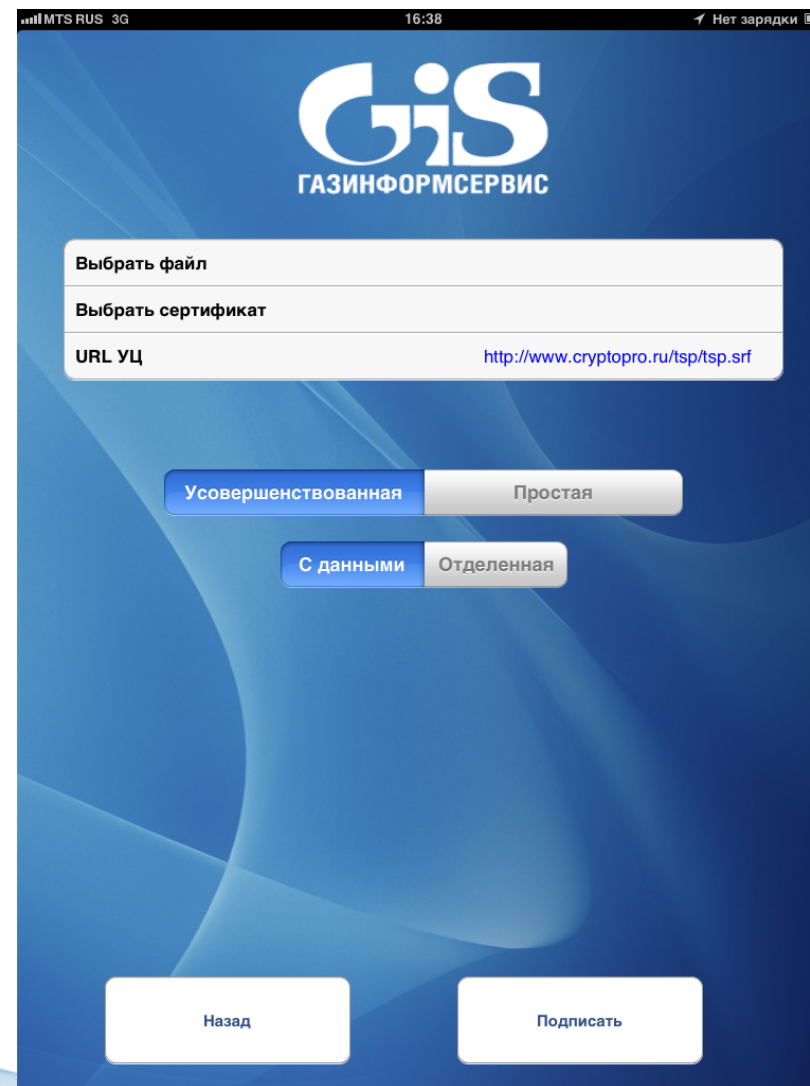


Интероперабельность PKI

Трансграничность vs CSP



Интероперабельность PKI Парк ОС и платформ



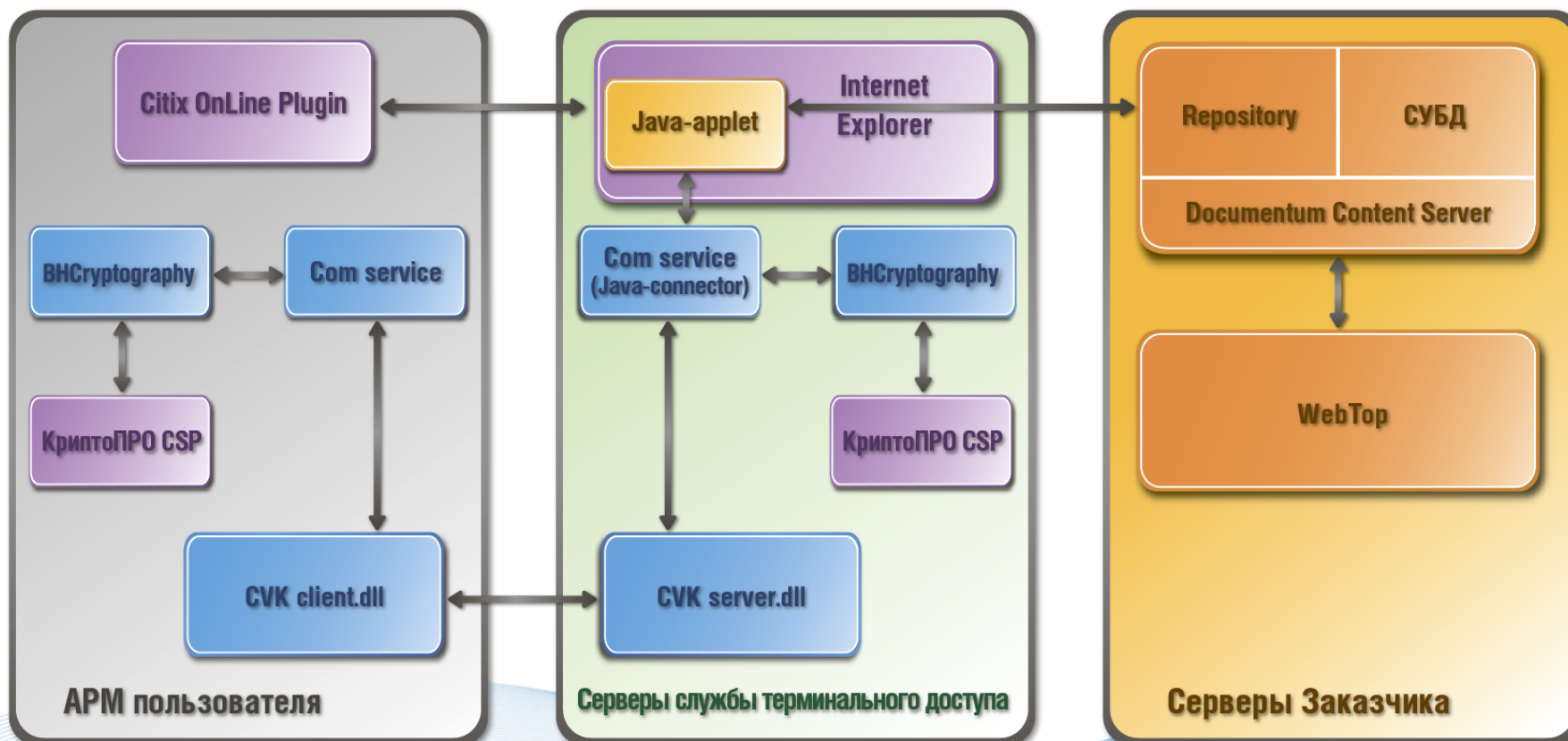
Интероперабельность РКІ

Парк ЭДО

Компоненты, разрабатываемые «Газинформсервис»

Компоненты, которые будут использоваться «Газинформсервис»

Компоненты, разрабатываемые Заказчиком



Интероперабельность PKI

Технические ограничения

Пользователь

Сервер



запрос



ИСХОДНЫЙ
ДОКУМЕНТ

ХЭШ

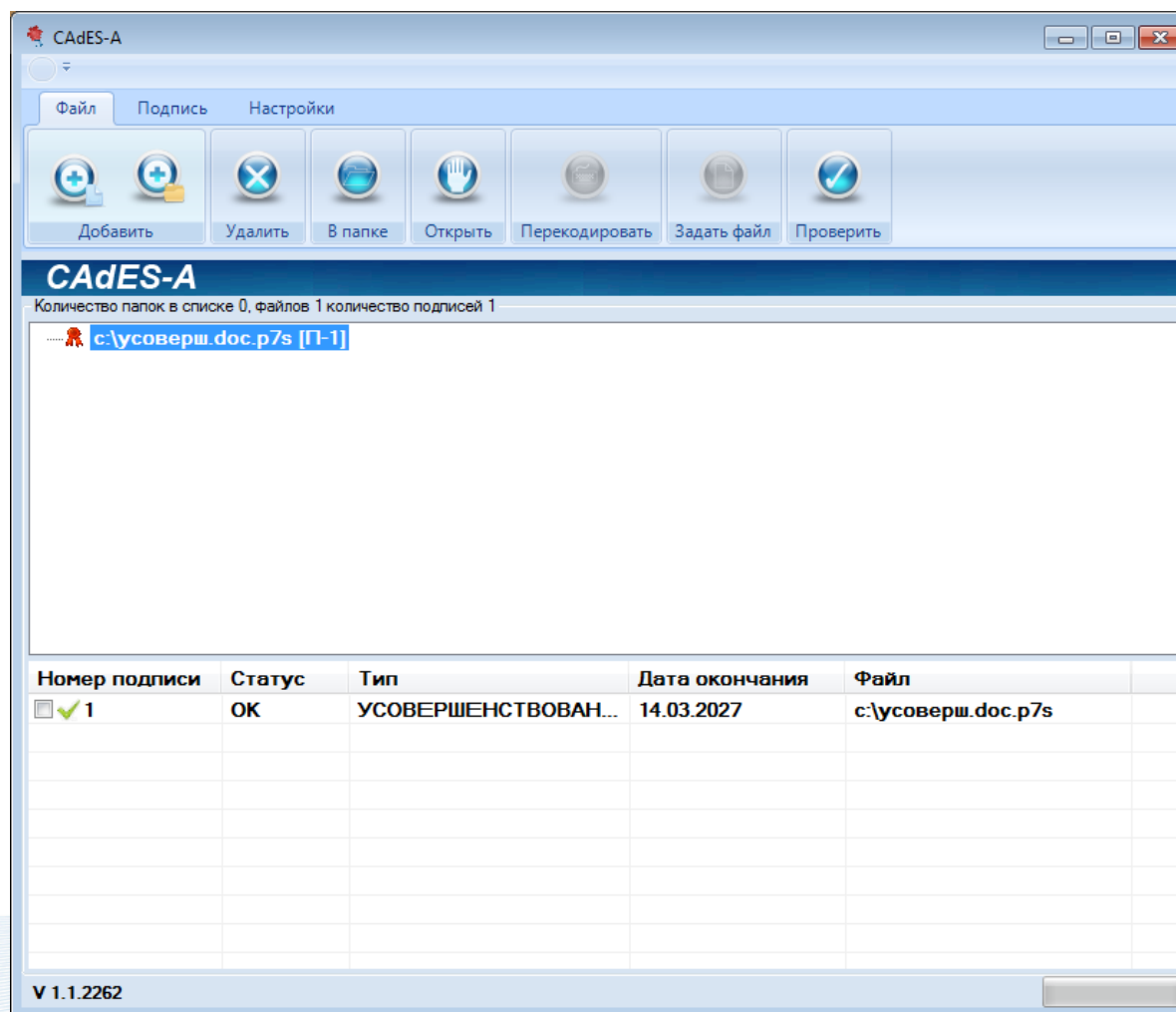


ПОДПИСАННЫЙ ХЭШ



ПОДПИСАННЫЙ
ДОКУМЕНТ

Cades-A



Библиотека «ВНСryptography»

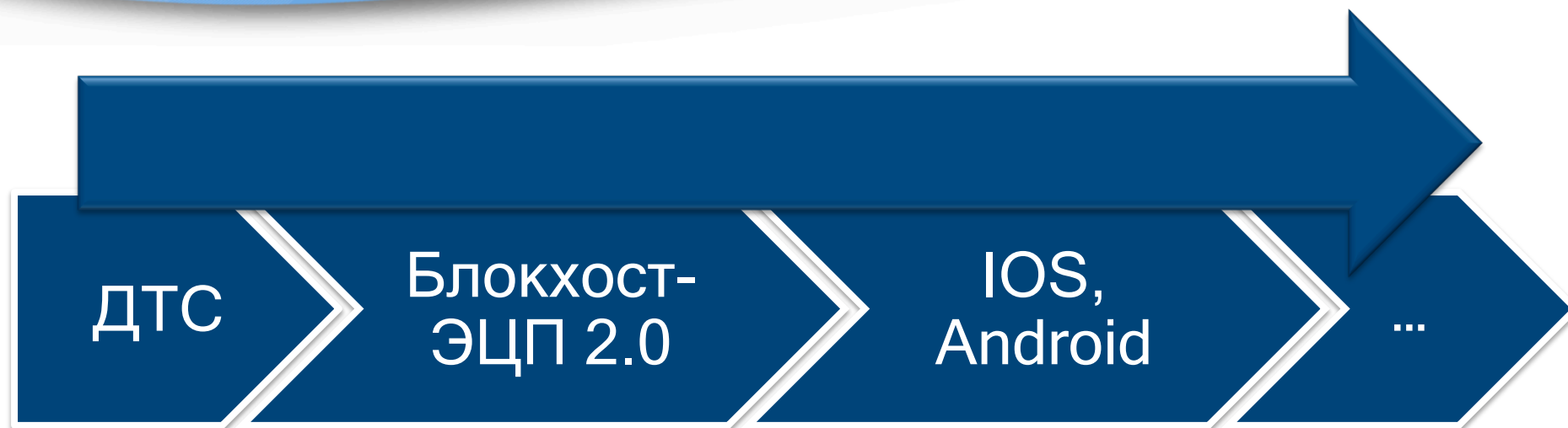
Направления развития



Направления развития

Библиотека «ВНСryptography»

Направления развития



Библиотека «ВНСryptography»

Направления развития

ДТС

Блокхост-
ЭЦП 2.0

IOS,
Android

...

Библиотека «ВНСryptography»

Направления развития

ДТС

Блокхост-
ЭЦП 2.0

IOS,
Android

...

Библиотека «ВНСryptography»

Направления развития

ДТС

Блокхост-
ЭЦП 2.0

IOS,
Android

...



ГАЗИНФОРМСЕРВИС

Спасибо за внимание!

Начальник отдела разработки средств защиты
Сергей Петров