конференция
РусКрипто

Ежегодная международная научно-практическая конференция

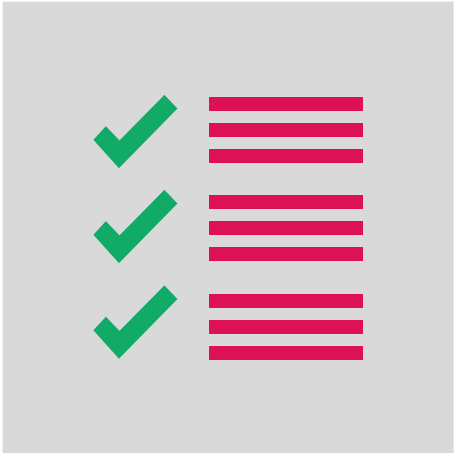
«РусКрипто'2022»

Преобразование интерфейса PKCS#11 в CryptoAPI

Сергей Агафьин,
Начальник отдела разработки ФКН, КриптоПро

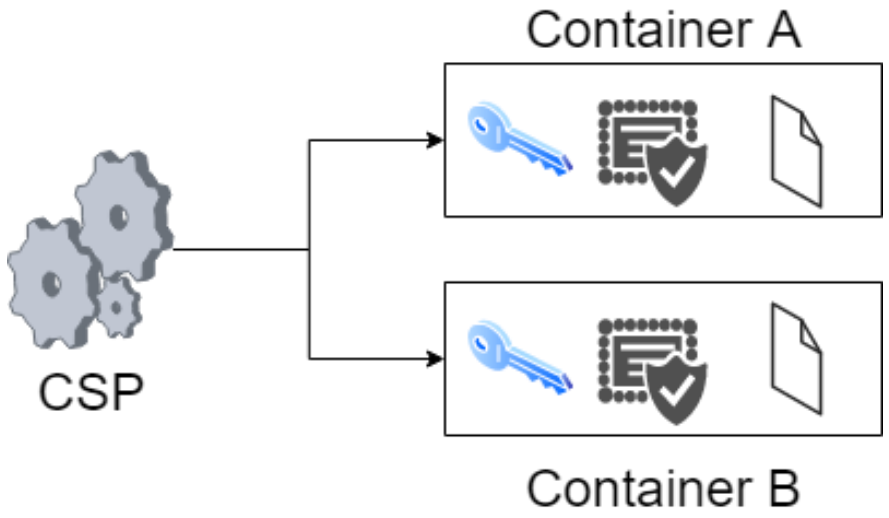
О чем доклад

- Как мы научились использовать PKCS#11 библиотеки через CryptoAPI
- Какие проблемы пришлось решить, а какие не удалось
- Результаты работы: год спустя после релиза



Немного вводных о CryptoAPI

- CryptoAPI – программный интерфейс Windows, используемый для подключения криптографических модулей (криптопровайдеров)

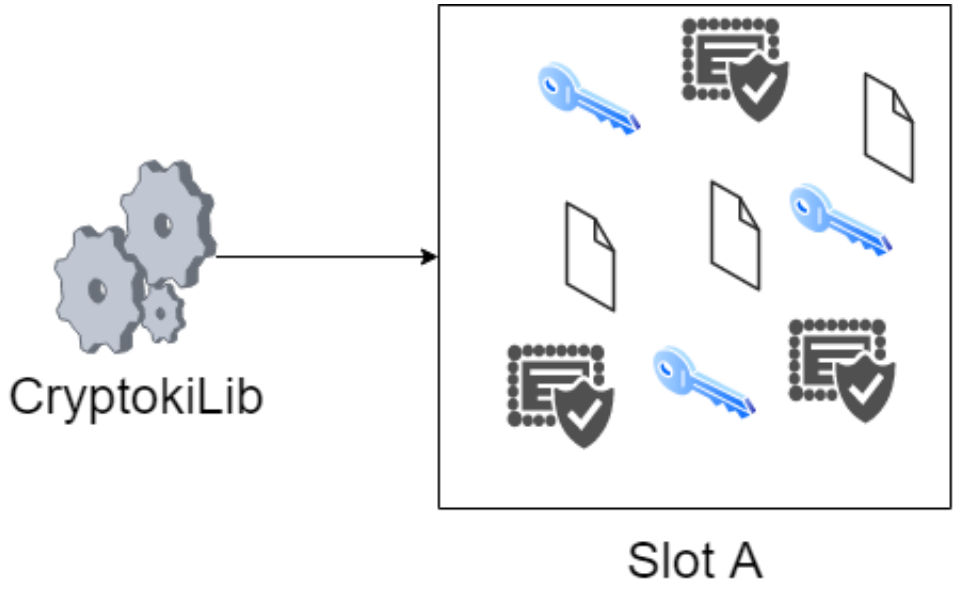


Примеры функций CryptoAPI

- CryptAcquireContext
- CryptSignHash
- CryptHashData
- CryptEncrypt
- CryptGenRandom
- CryptGenKey
- CryptSetProvParam
- …

Немного вводных о PKCS#11

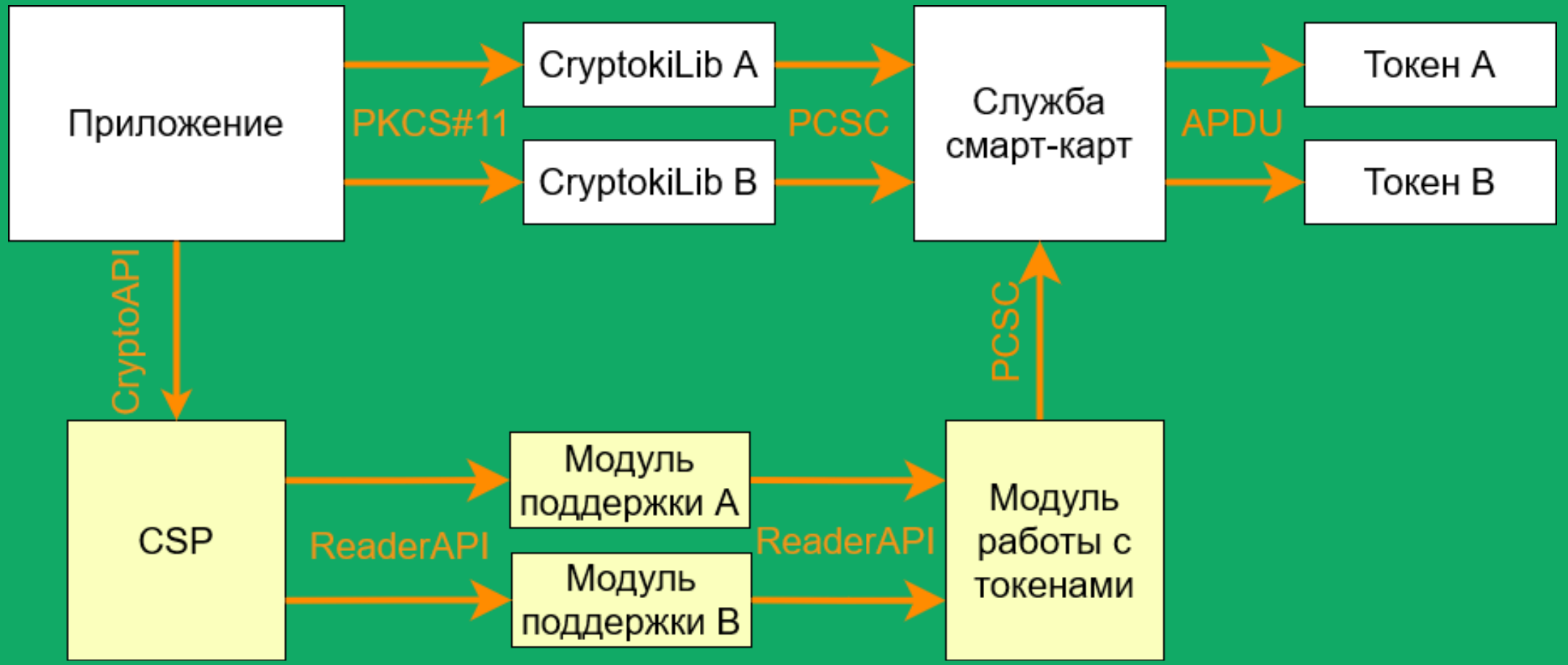
- PKCS#11 (Cryptoki) – программный интерфейс подключения библиотек криптографических объектов: токенов, HSM



Примеры функций PKCS#11

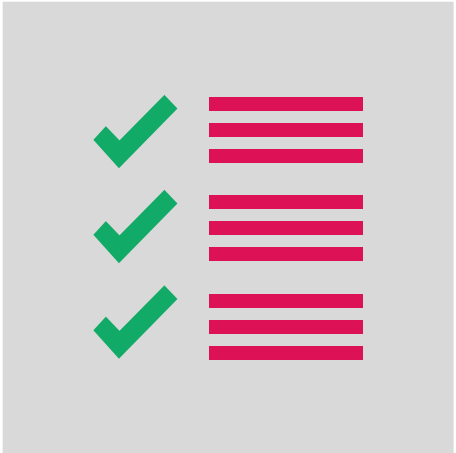
- C_Initialize
- C_GetSlotList
- C_Sign
- C_OpenSession
- C_Digest
- C_GenerateKey
- C_DeriveKey
- …

Параллельная работа

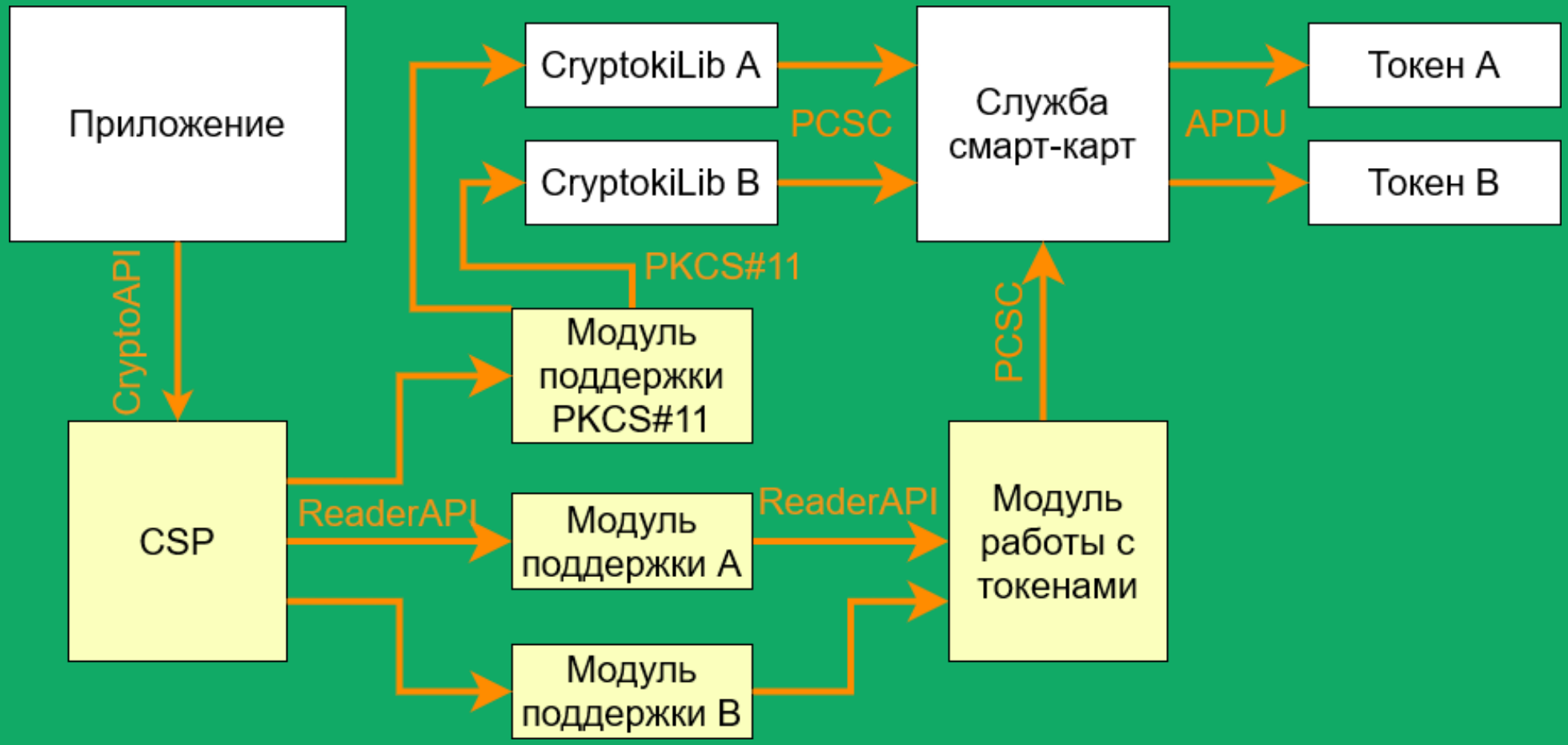


Страдают все

- Разработчик универсального приложения будет реализовывать подключение по двум интерфейсами
- Разработчики токенов должны поддерживать не менее двух библиотек синхронно: PKCS#11 свою и модуль поддержки каждого CSP
- Разработчики CSP должны поддерживать каждый новый носитель отдельно



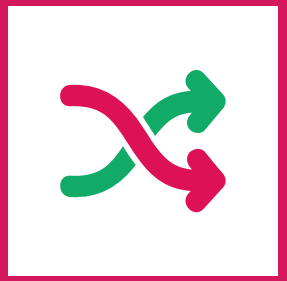
Как хотелось (и стало в итоге)



Концепция разработки модуля

- Слот PKCS#11 превращается в считыватель CSP

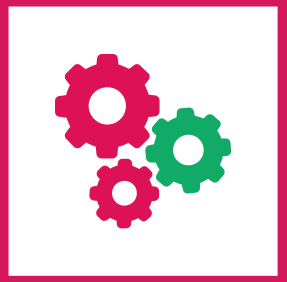
- CKA_ID сертификата, закрытого и открытого ключа одного «контейнера» должны совпадать



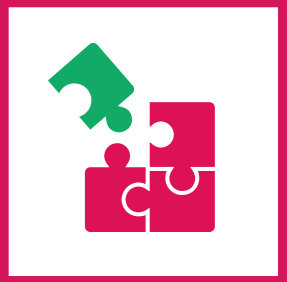
- CKA_LABEL открытого ключа превращается в имя контейнера CSP

Основные проблемы разработки

- Синхронизация доступа к носителю + тормоза
  - Пришлось ослабить ряд требований провайдера, пожертвовав стабильностью в редких случаях



- Слоты могут иметь одинаковые имена
  - Пришлось на первое время использовать имена вида «PKCS11 Reader SlotID»



- Существующие приложения, использующие PKCS#11 могут не следовать стандарту
  - Смирились ☹

Результаты работы

- Сертифицирован криптопровайдер «КриптоПро CSP 5.0 R2»
- Доработана документация и инструкции – пользователи научились и в целом довольны
- Поддержаны носители, которых никогда не было в CSP

- Проблемы производительности в общем случае не решить
- Сложная доставка продукта и контроль зависимостей
- Очень много мелких подводных камней продолжает находиться каждый день