РУТОКЕН

Интерфейсы взаимодействия с активными ключевыми носителями. Корректное использование и применимость в различных средах функционирования

Татьяна Липина,
Руководитель аналитического отдела,
Компания «Актив»

Активные ключевые носители

- Защищенная память
- Неизвлекаемые ключи
- Криптография «на борту»
- Форм-факторы:
  - токен
  - смарт-карта
  - чип
- Протоколы подключения:
  - USB
  - NFC
  - Bluetooth 2.0
  - Bluetooth LE
  - SPI
  - UART
  - …

Виды интерфейсов для работы с носителями

Высокоуровневые

- OpenSSL API
- Crypto API
- PKCS#11 API
- …

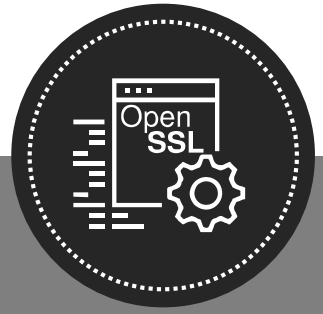
Низкоуровневые

- APDU
- PC/SC
- CT-API
- OpenCard Framework
- …

Высокоуровневые интерфейсы

Windows Crypto API

- Глубокая интеграция в Windows и прикладное программное обеспечение под Windows
- легкая портируемость программного обеспечения в пределах ОС Windows
- автоматический доступ к любому установленному криптопровайдеру



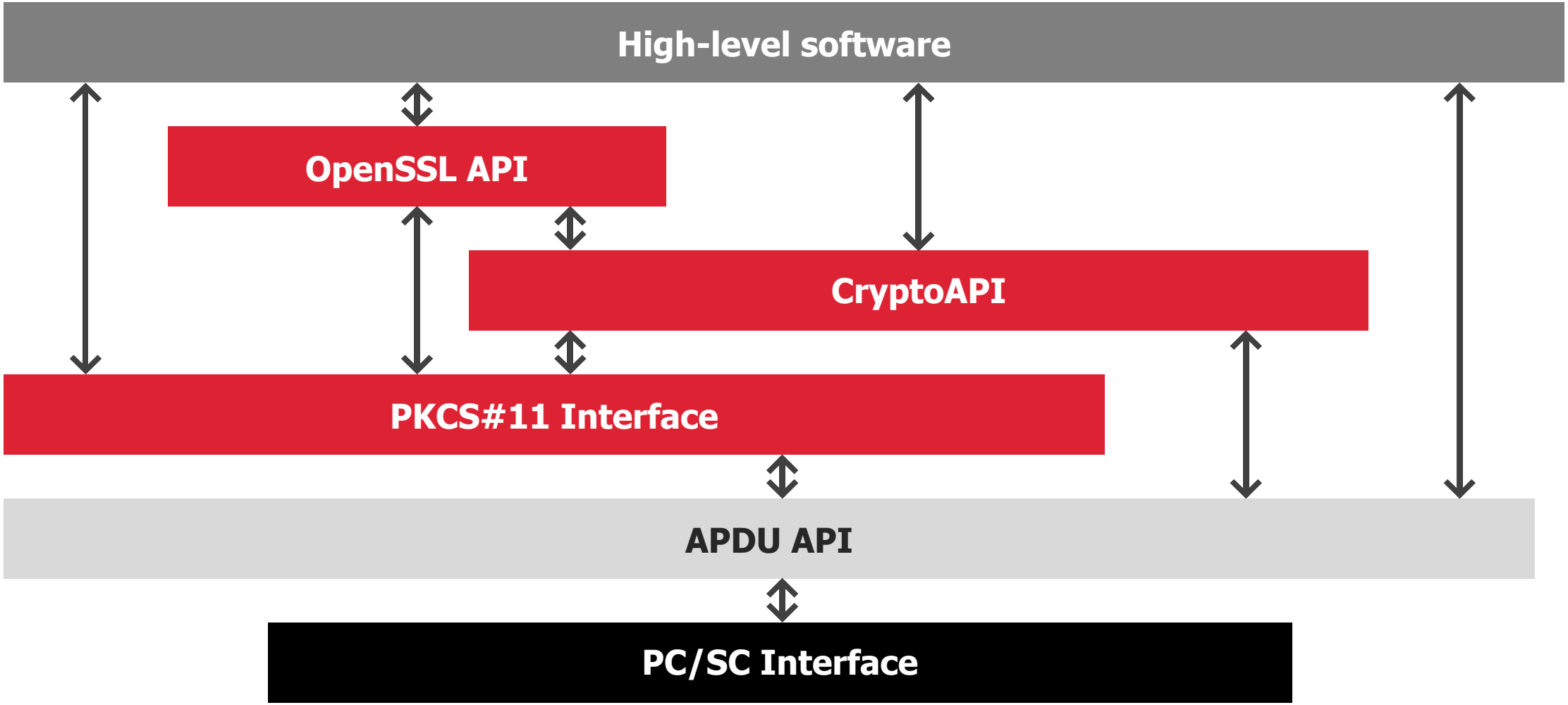
OpenSSL API

- Кроссплатформенность
- Широкий функционал
- Открытый исходный код
- Распространенность
- Может использовать «движки»

PKCS#11 API

- Кроссплатформенность
- Поддержка управления несколькими устройствами одновременно
- Наличие специальной функции ожидания подключения/отключения аппаратного токена
- Возможность расширения интерфейса

Архитектура подсистемы взаимодействия с носителями



PKCS#11

Разработан для работы с аппаратными криптографическими устройствами

Поддерживается большинством разработчиков активных ключевых носителей

Объекты:

- Произвольные данные
- Сертификаты
- Vendor-defined объекты
- Ключи:
  - закрытые ключи
  - открытые ключи
  - секретные ключи

Расширение интерфейса PKCS#11

Расширение интерфейса при помощи

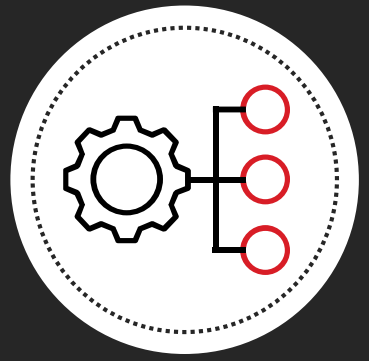
- Vendor-defined объектов
- Функций расширения

При расширении интерфейса необходимо руководствоваться:

- PKCS #11 Cryptographic Token Interface Base Specification

  Последняя версия стандарта — 3.0
- МР 26.2.007-2017 «Расширение PKCS#11 для использования российских стандартов ГОСТ Р 34.10-2012 и ГОСТ Р 34-11-2012»
- Проект МР «Расширение PKCS#11 для использования стандартов ГОСТ 34.12-2018 и ГОСТ 34.13-2018»

Встраивание носителей через интерфейс PKCS#11



При встраивании разработчик пользуется следующим набором:

- PKCS #11 Cryptographic Token Interface Base Specification
- Руководство программиста
- SDK

Примеры ошибок:

- В шаблоне ключа указано значение:

  CKA_PRIVATE=FALSE

- При работе в многопоточном режиме отсутствует флаг:

  CKF_OS_LOCKING_OK

Высокоуровневые интерфейсы.
Достоинства и недостатки

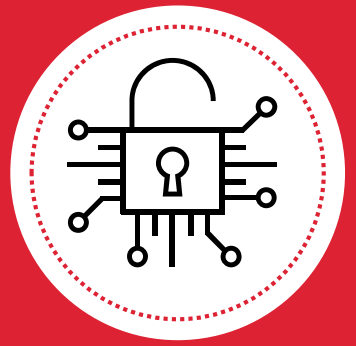
- Широко распространены
- Легки в освоении для разработчиков
- Поддерживаются стандартными семействами ОС: Windows, Linux, FreeBSD, Mac OS, Android, iOS
- Доступная документация, продуманные SDK
- И снова: широкий функционал

- Не все ОС могут работать с такими библиотеками
- Неоптимальное взаимодействие с ключевым носителем

APDU

Встраивание в прикладное ПО по интерфейсу APDU требуется в:

- M2M устройствах
  (датчики, сенсоры, малогабаритные устройства управления)
- iOT устройствах
- АПМДЗ



Особенности APDU-интерфейса:

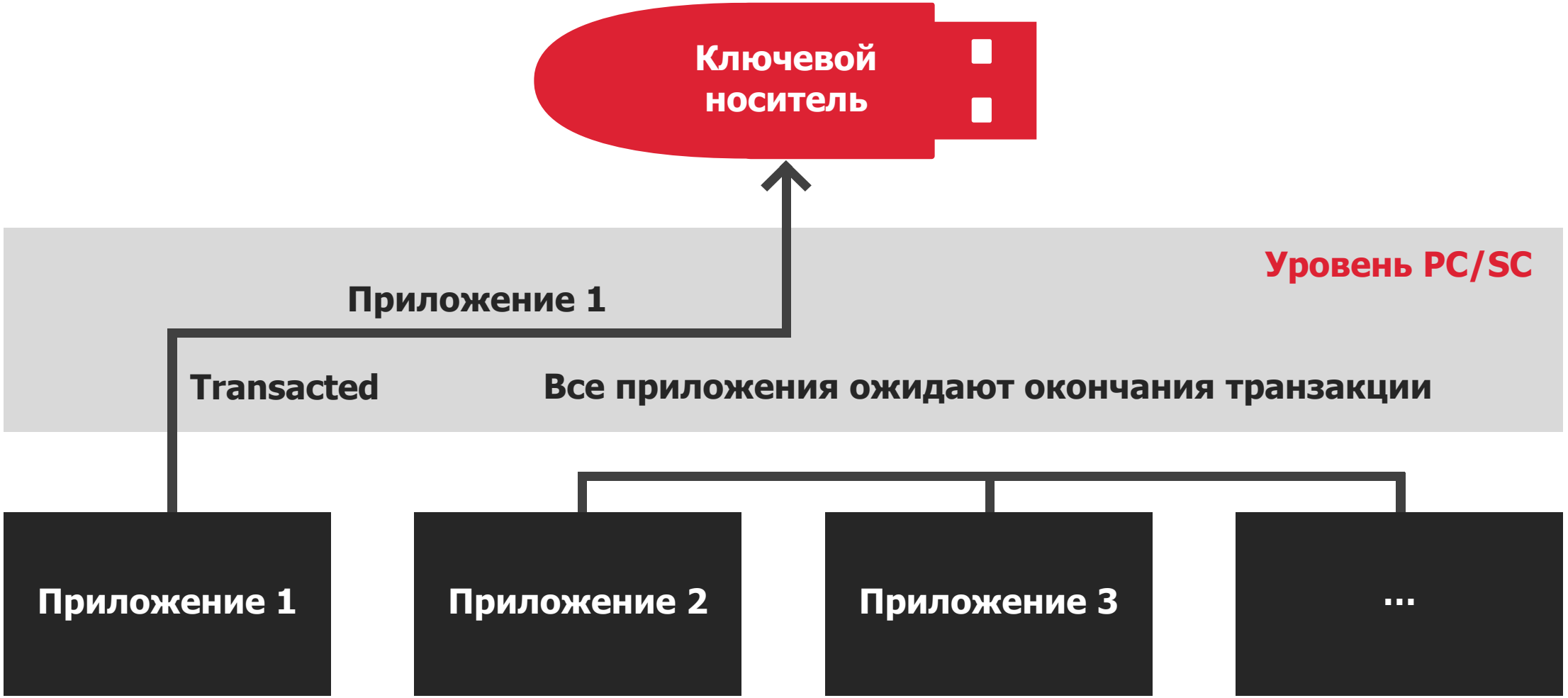
- Общение с устройствами с помощью байтовых последовательностей
- ОС ключевого носителя обрабатывает команду и посылает в ответ код возврата и, при необходимости, дополнительную информацию
- Фиксированный формат команды
- Реализован в соответствии с ISO 7816-4

APDU. Достоинства и недостатки

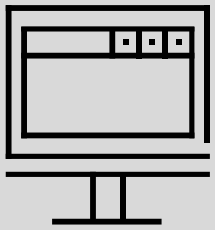
- Скоростные характеристики
- Требует меньше памяти
- Сложно сделать ошибку, ведущую к криптографически опасным последствиям
- Позволяет использовать функционал устройства, который не поддерживается высокоуровневыми интерфейсами
- Работает даже если ОС не поддерживает высокоуровневые библиотеки

- Неудобно работать с байтовыми последовательностями
- При выполнении самой простой операции надо написать множество команд
- Функционал ограничен только возможностями носителя

Механизм транзакций



Защита канала



Интерфейсная библиотека с реализацией аутентификации

Encrypted

APDU

Преобразование команд

ОС

- Технологии Global Platform
- Технология ФКН (протокол SESPAKE)
- Проприетарные протоколы Secure Messaging

Спасибо за внимание!

Контактная информация

Татьяна Липина

Lipina@aktiv-company.ru
info@rutoken.ru

www.rutoken.ru
www.aktiv-company.ru

+7 916 287-23-04