Технологии электронной подписи. Часть 1

Владимир Салыкин
Менеджер по продуктам
Компания «Актив»

https://www.youtube.com/user/AktivCompany

Сегодня мы ответим на вопросы:

- Как работают смарт-карты на низком уровне и какие там есть интерфейсы?
- Какие есть стандарты в области технологий электронной подписи?
- Какие высокоуровневые интерфейсы доступны для различных языков программирования?
- Какой интерфейс выбрать для встраивания?
- Как во всем этом не запутаться и быстро встроить поддержку подписи?

Термины

- Отечественные алгоритмы

  ГОСТ Р 34.10-2001 и ГОСТ Р 34.10-2012(256 и 512 бит)

  ГОСТ Р 34.11-94 и ГОСТ Р 34.11-2012

  ГОСТ 28147-89

  VKO GOST R 34.10-2001 (RFC 4357)

  VKO GOST R 34.10-2012 (RFC 7836)

- Иностранные алгоритмы

  RSA

  AES

Компания «Актив»

Крупнейший российский производитель аппаратных средств аутентификации и электронной подписи, разработчик и поставщик комплексных решений в сфере информационной безопасности. Основана в 1994 году.

Направления деятельности

РУТОКЕН

Продукты и решения в области аутентификации, защиты информации и электронной подписи.

Guardant

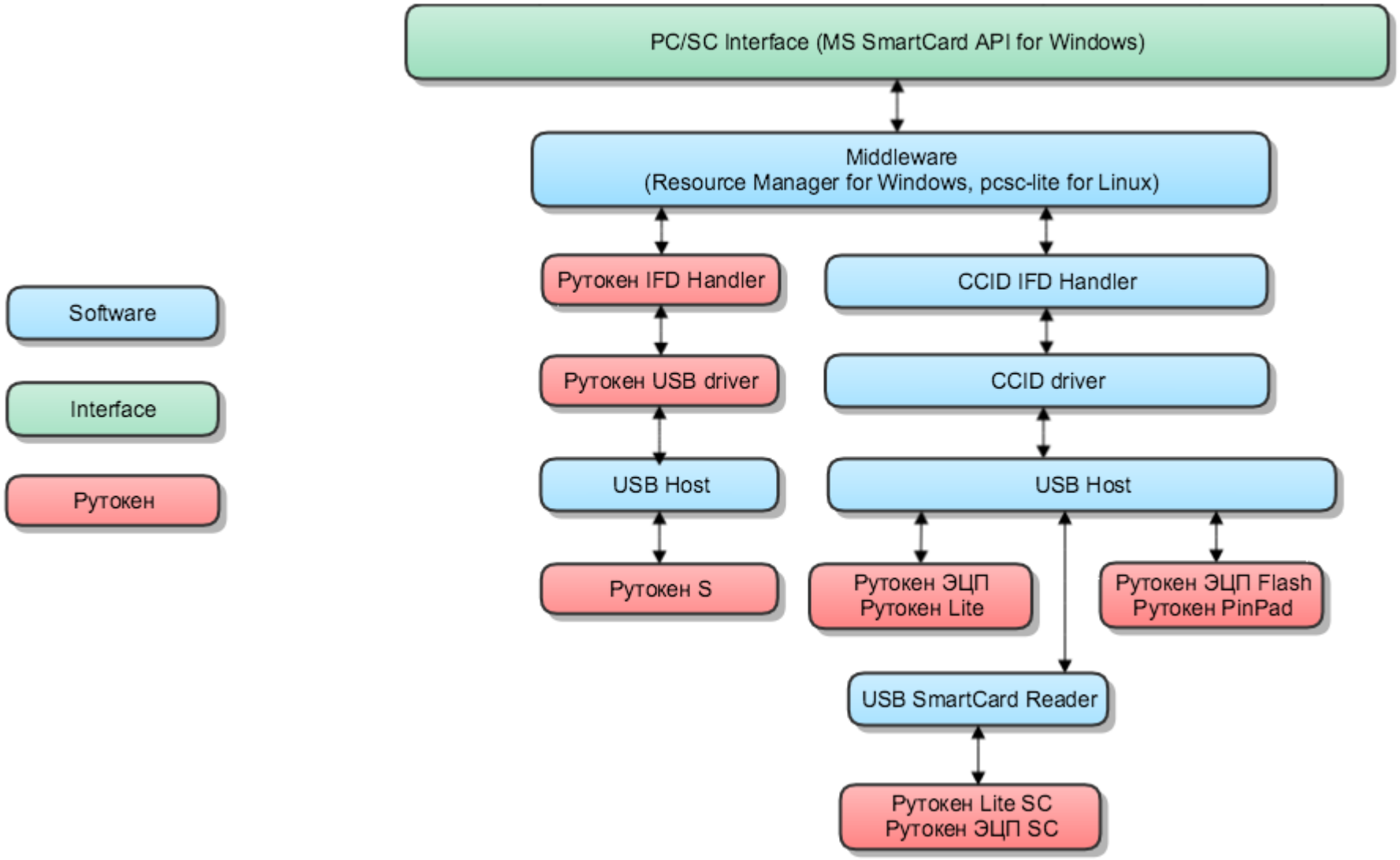
Средства защиты и лицензирования программного обеспечения.

О каких интерфейсах поговорим сегодня

- **APDU**
- **CAPI**
- **PKCS#11**
- pki-core
- Pkcs11-helper
- PKCS11Interop
- opensc
- openssl
- PyKCS11
- pyscard
- Java pkcs11Wrapper
- sunJCA
- sunPkcs11Wrapper
- Рутокен Плагин
- mobile pkcs

Низкоуровневые интерфейсы

Программная архитектура низкого уровня



PC\SC или Microsoft SmartCard API

- Разработана под Windows 200x/XP,
  затем спортирована под Windows NT/9x
- Windows
  Microsoft Resource Manager + Smart Card Service
  (winscard.dll)
- Linux и Mac
  PCSC lite
  (libpcsc.so + pcscd)
- Основной интерфейс – APDU команды
- Иностранные и отечественные алгоритмы

APDU интерфейс

- Определен в ISO/IEC 7816-4 Organization, security and commands for interchange
- Работает в формате запрос-ответ
- Запрос

  Заголовок **[CLA INS P1 P2]** + Тело запроса **[Lc] [Data] [Le]**

CLA	Метаданные команды	Lc	Длина элемента Data в байтах
INS	Код инструкции	Data	Данные команды
P1 и P2	Параметры команды	Le	Ожидаемая длина данных ответа

- Ответ

  Тело ответа **[Data]** + Trailer **[SW1 SW2]**

Data	Данные ответа	SW	Статусные слова

- 90 00 - ОК

  61XX - ОК, но есть еще XX байтов данных

Как попробовать

- APDU Trace – посмотреть какие ходят команды
- SPRINGCARD NETPCSC – послать команду\получить ответ
- APDU команды Рутокен – NDA
- SCardTransmit example – link

APDU демо

Достоинства и недостатки APDU интерфейса

- Максимум возможностей
- Не требует дополнительных библиотек
- Доступен бесплатно

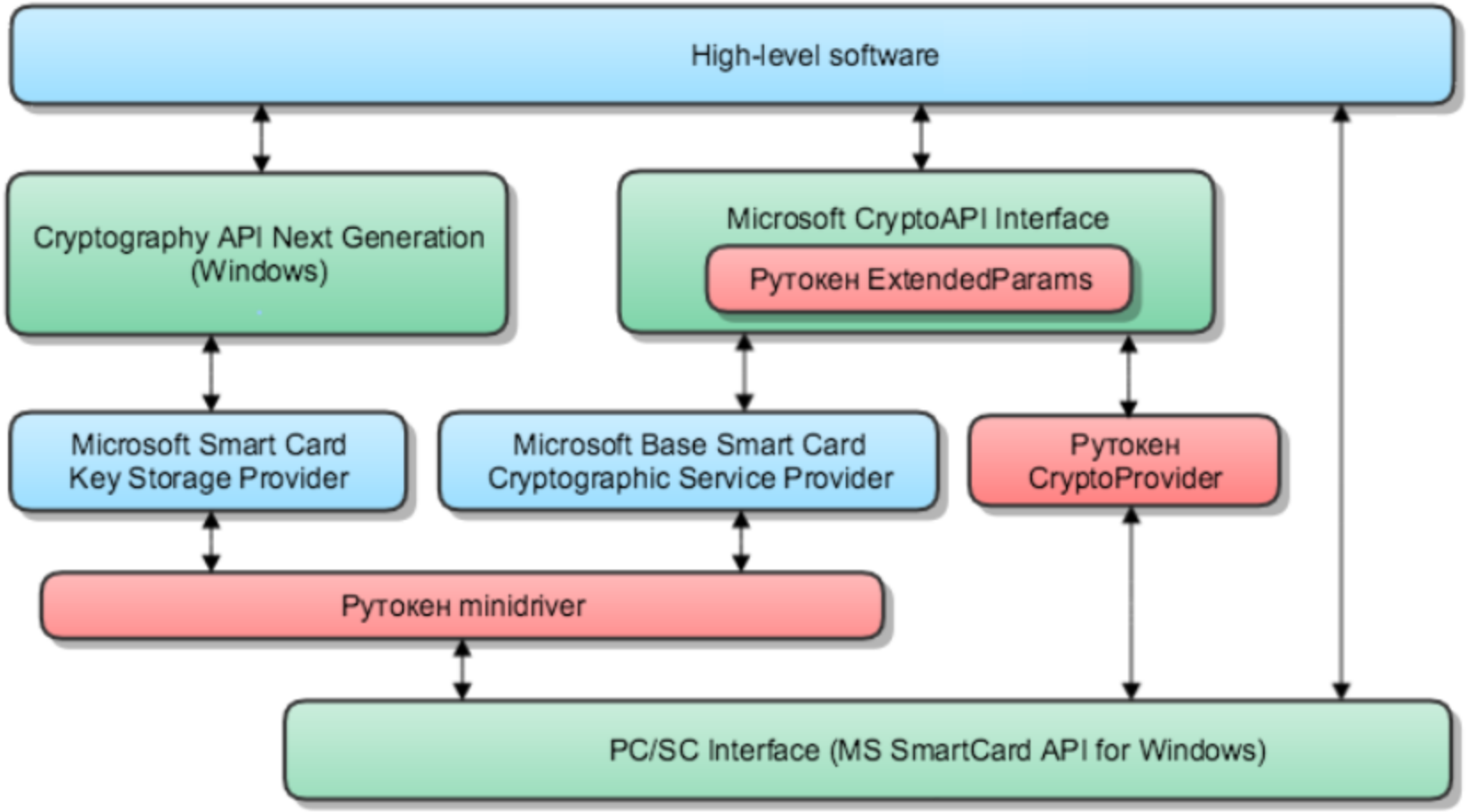
- Работа на уровне байтовых массивов
- Необходимо знать внутренние структуры и форматы хранения
- Может значительно отличаться от производителя к производителю

Высокоуровневые интерфейсы

CAPI или CSP

- CAPI или CryptoAPI или Cryptographic Application Programming Interface
- Представлен в Windows NT 4.0
- Большинство функций поддерживается, начиная с Windows 2000
- Вторая версия Cryptography API: Next Generation (CNG) с Windows Vista
- Работает с установленными Cryptographic Service Providers
- Криптопровайдер - независимый модуль, позволяющий осуществлять криптографические операции
- Приложения не работают напрямую с криптопровайдером
  Они вызывают функции CryptoAPI из библиотек Advapi32.dll и Crypt32.dll
- Документация на MSDN и сайтах разработчиков CSP

Программная архитектура CAPI



Особенности работы с CAPI

- Начинается с выбора криптопровайдера
  CryptAcquireContext или BCryptEnumRegisteredProviders
- Работа ведется не с устройством, а с объектами провайдера
- Поддерживает CMS и другие форматы
- Работает с хранилищем сертификатов
  (место хранения сертификатов, CRL и CTL)

CAPI демо

Достоинства CAPI

- Глубокая интеграция в Windows
- Работа с сертификатами из коробки
- Хранилище сертификатов
- Одинаково работает для всех поддерживаемых устройств

Недостатки CAPI

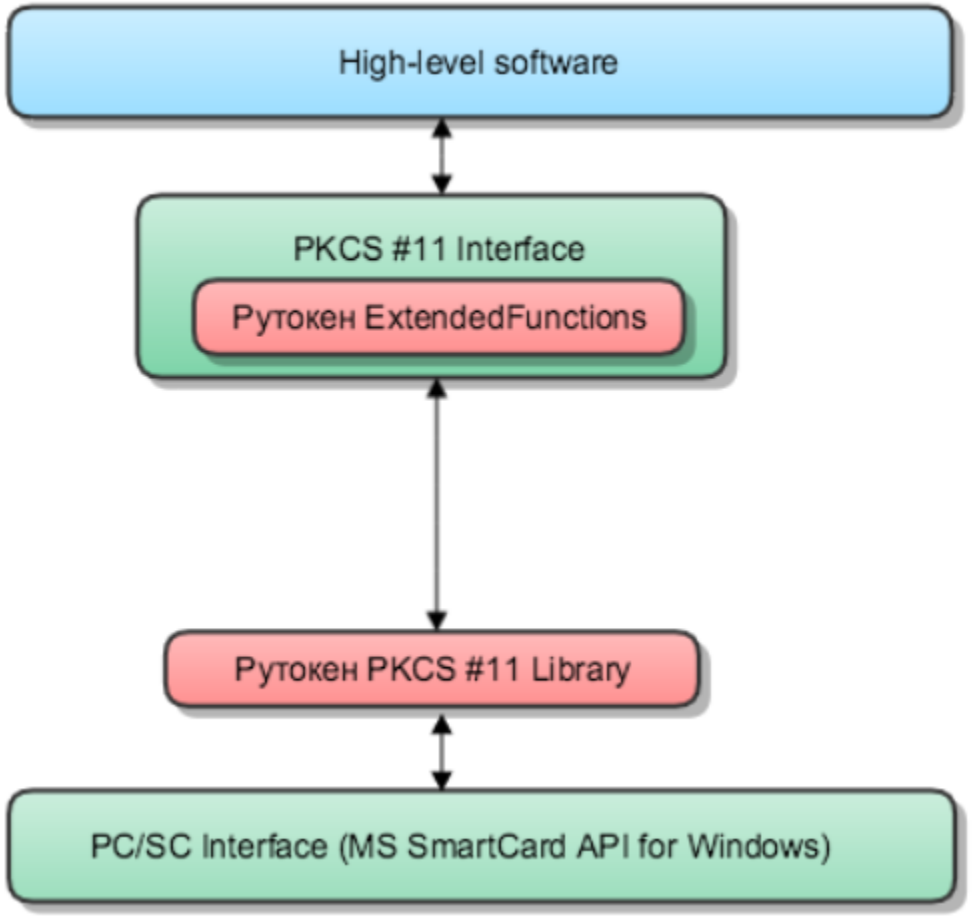
- Windows only
- Глубокая интеграция в Windows
- Спроектировано только для иностранных алгоритмов
- Для работы с ГОСТ алгоритмами требует обязательной установки сторонних, возможно платных криптопровайдеров
- Поддержка устройств ограничена разработчиками криптопровайдеров
- Требует прав администратора для установки
- Работа может отличаться для различных CSP

PKCS#11

PKCS#11 или Cryptoki

- Public Key Cryptography Standards
  (Стандарты криптографии с открытым ключом)
- Первая версия вышла в апреле 1995 года
- Текущая версия v2.40 вышла в мае 2016 года
- Поддержка отечественных алгоритмов включена в стандарт
- Работает непосредственно с устройствами, нужна только библиотека

Программная архитектура PKCS#11



Особенности работы с PKCS#11

- Начинается с загрузки PKCS#11 библиотеки и перечисления устройств
- Поддерживает CMS
- Нет глубокой интеграции в Windows
- C style интерфейс, без классов
- Работает с устройствами и объектами на них

PKCS#11 демо

Достоинства PKCS#11

- 100% кроссплатформенность
- Доступность для множества архитектур (ARM, Эльбрус, Байкал…)
- Простота
- Бесплатность
- Нативная поддержка отечественных алгоритмов
- Может быть вызван практически из любого языка программирования
- Не требует прав администратора для установки

Недостатки PKCS#11

- Требует самостоятельной реализации работы с сертификатами
- Может иметь отличия от вендора к вендору в части дополнительных функций

Где найти больше информации?

- Портал документации Рутокен
  https://dev.rutoken.ru
- Комплект разработчика Рутокен https://www.rutoken.ru/developers/sdk/
- Github компании Актив
  https://github.com/AktivCo/
- Стандарт PKCS#11
  http://docs.oasis-open.org/pkcs11/pkcs11-curr/v2.40/
- Пишите на
  sv@rutoken.ru
  mk@rutoken.ru

Контактная информация

Электронная почта:

Личная – sv@rutoken.ru

Отдел продаж – sales@rutoken.ru

Тех. поддержка – hotline@rutoken.ru

Facebook:

facebook.com/vladimir.salykin

Сайты:

www.rutoken.ru

www.aktiv-company.ru

Телефон:

+7 495 925-77-90