Конференция ИнфоТеКС PKI Day 2

«Криптография для разработчиков»

Криптобиблиотеки, токены и как все это работает в реальной жизни

Арина Эм



infotecs

AGENDA

1. Обзор средств встраиваемой криптографии
2. ViPNet OSSL: архитектура, принцип работы
3. Работа с криптотокенами
4. Живая демонстрация

Обзор средств встраиваемой криптографии

Криптобиблиотеки Инфотекс



ViPNet **CSP**

Для разработки ПО под Windows



ViPNet **OSSL**

Для разработки мобильных
и серверных решений



ViPNet JCrypto SDK

Для разработки ПО на Java



ViPNet CryptoSmart

Для тех, кому нужен ГОСТ в блокчейне

Функциональность криптобиблиотек

infotecs

Работа с ЭП

- ГОСТ Р 34.10-2012

Хэширование

- ГОСТ Р 34.11-2012

Шифрование

- ГОСТ Р 34.12-2015
- ГОСТ Р 34.13-2015

Защищенные соединения

- TLS 1.2
- TLS 1.3

Работа с ключами на внешних устройствах

- Rutoken
- JaCarta
- и др…

Поддержка ОС



Библиотеки Инфотекс

ViPNet CSP

Платформы



Интерфейсы

MS CryptoAPI

Класс защиты

КС1-КС3

Сертификат ФСБ

да

ViPNet OSSL

Платформы



Интерфейсы

PKCS#11
OpenSSL

Класс защиты

КС1, КС2

Сертификат ФСБ

почти да

ViPNet JCrypto SDK

Платформы



Интерфейсы

JNI/JCA
PKCS#11

Класс защиты

КС1

Сертификат ФСБ

еще нет

ViPNet CryptoSmart

Платформы



Интерфейсы

MSP
NetCSP
BCCSP Lite

Класс защиты

КС1, КС2

Сертификат ФСБ

почти да

ViPNet OSSL

Для тех, кто разрабатывает мобильные и серверные решения

для клиентов



- функции подписи и шифрования на клиентских устройствах
- нужна оценка влияния

для серверов

- гибкость в выборе места установки
- распараллеливание процессов

Не нужна оценка влияния!

Архитектуры и операционные системы

infotecs

Архитектуры

- x86
- x86-64
- ARM
  - Android
  - Байкал-М
  - Аврора
  - macOS, iOS
- Эльбрус
- M1

Linux

CentOS
Debian
Red Hat Enterprise Linux
Ubuntu, Ubuntu Server
SUSE Linux Enterprise Server
Альт 8 СП, 9, 10
ГосЛинукс ИК6
AlterOS
РЕД ОС
РОСА «КОБАЛЬТ»
Astra Linux (SE, CE)
ROSA Enterprise Linux Server
Лотос
Атлант ОС
Аврора

Windows

Windows 7, 8.1, 10, 11
Windows Server 2008 R2, 2012, 2012 R2, 2016, 2019, 2022

Мобильные ОС

Android 7.x – 12.x.
iOS 12.x – 15.x.
iPadOS 14, 15.

macOS

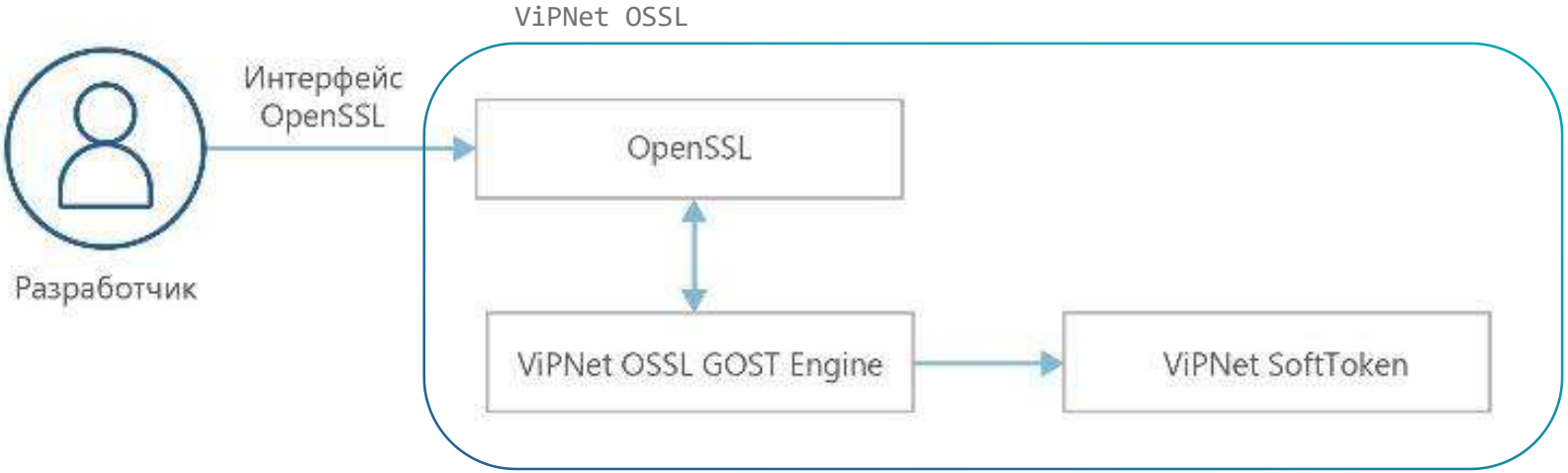
macOS 10.13, 10.14, 10.15, macOS 11, macOS 12

Работа с криптотокенами

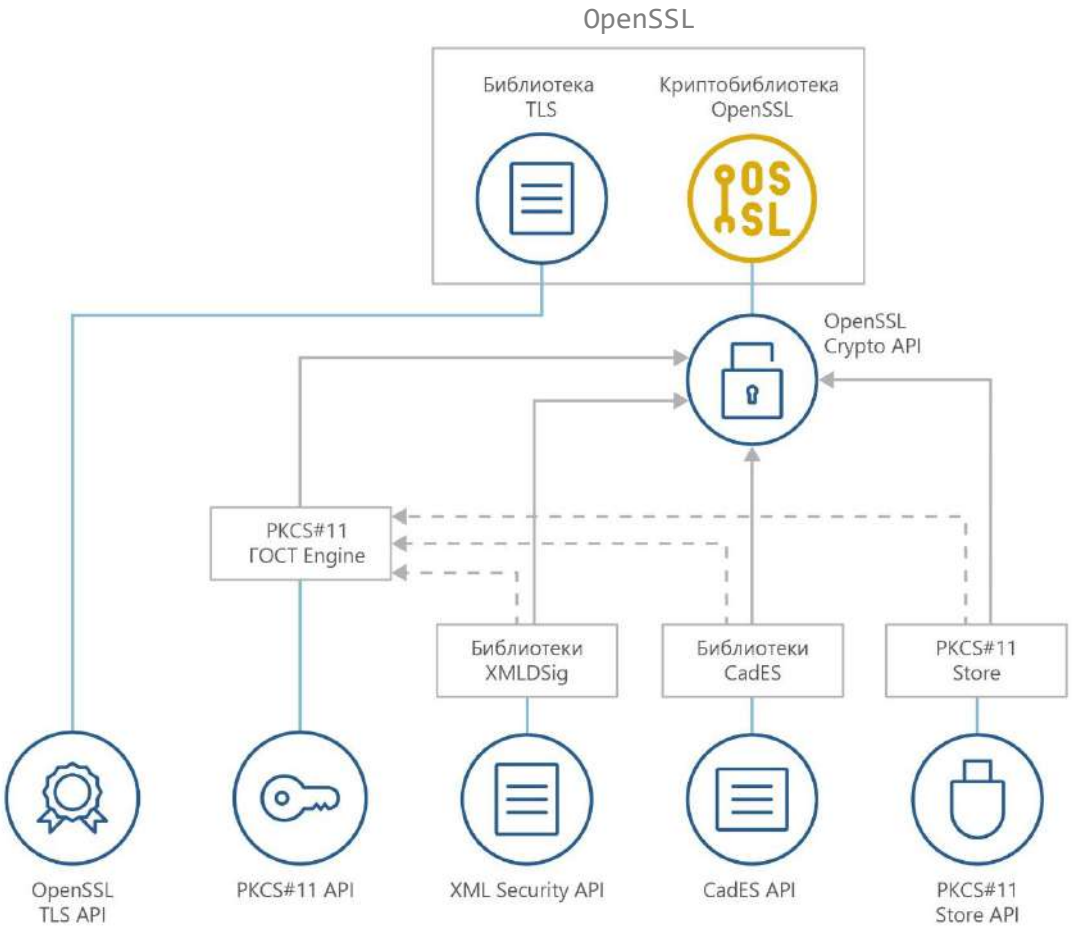
Рутокен ЭЦП 2.0 Touch
Рутокен ЭЦП Bluetooth
Рутокен Lite
Рутокен ЭЦП 2.0, 2.0 Flash
Rutoken S (только под Windows)
Рутокен ЭЦП 2.0 3000
Рутокен ЭЦП PKI
Рутокен ЭЦП 2.0 2100
Рутокен 2151
Рутокен ЭЦП 3.0 NFC

ViPNet HSM
ViPNet SoftToken
JaCarta

Структура ViPNet OSSL



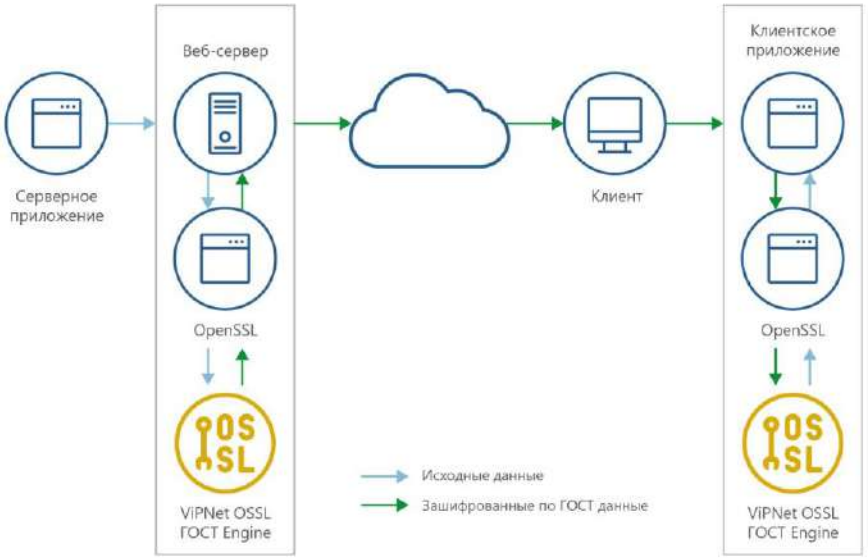
Общая архитектура



OpenSSL vs. ViPNet OSSL



Шифрование с «чистым» OpenSSL



Шифрование с ViPNet OSSL

Как встроить ViPNet OSSL

Что понадобится для разработки

- пакеты ViPNet OSSL для разработчика
- g++ (GNU C++)
- утилита make
- CMake ДЛЯ СБОРКИ ПРИМЕРОВ
- библиотеки C++ Boost ДЛЯ СБОРКИ ПРИМЕРОВ

Есть дистрибутив – что дальше?

Шаг 1: Регистрация движка

Шаг 2: Подключение и инициализация движка

Шаг 3: Конфигурация интерфейса PKCS#11

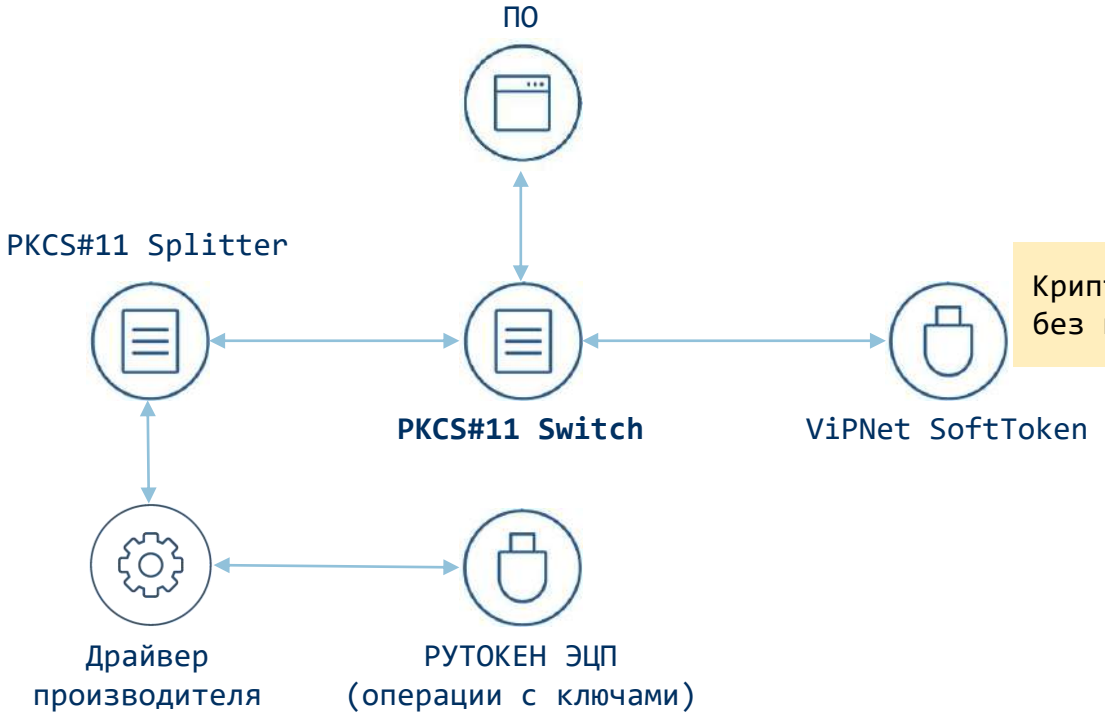
Шаг 4: Инициализация хранилища ключевой информации ДЛЯ РУТОКЕН УЖЕ НАСТРОЕНО

Шаг 5: Организация TLS-соединения

Шаг 6: Реализация бизнес-логики работы с ключами и данными

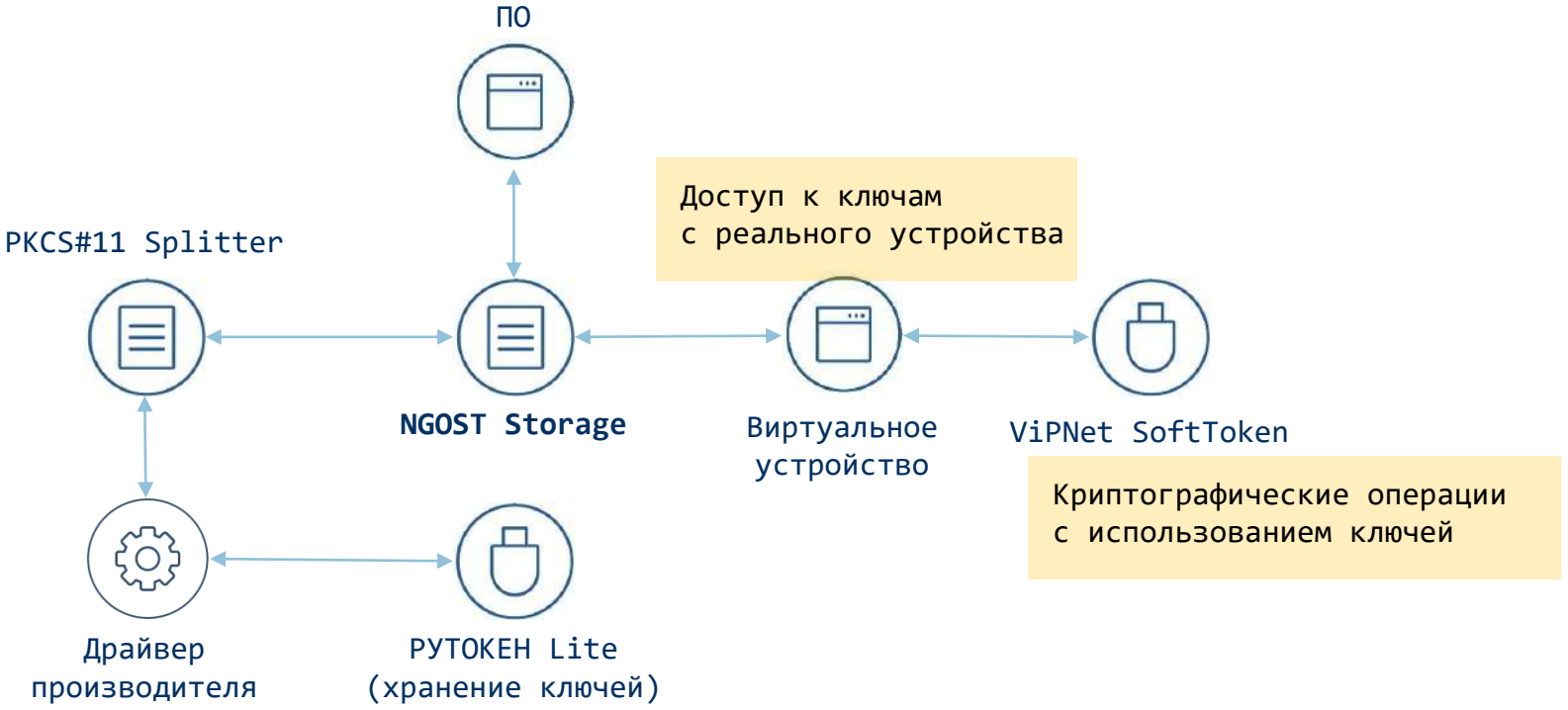
Работа с токенами

Токен поддерживает криптооперации



Работа с токенами

Токен в роли хранилища ключей



Встраивание в приложение

infotecs

Остаемся на связи!

Арина Эм

Arina.Em@infotecs.ru

Подписывайтесь на наши соцсети

https://vk.com/infotecs_news

https://t.me/infotecs_news