Криптографические библиотеки для встраивания. Состав, сертификация, ценовая политика

Елена Выходцева, заместитель начальника отдела по работе с партнерами
Сергей Петренко, руководитель продуктового направления криптографических библиотек для встраивания

Введение

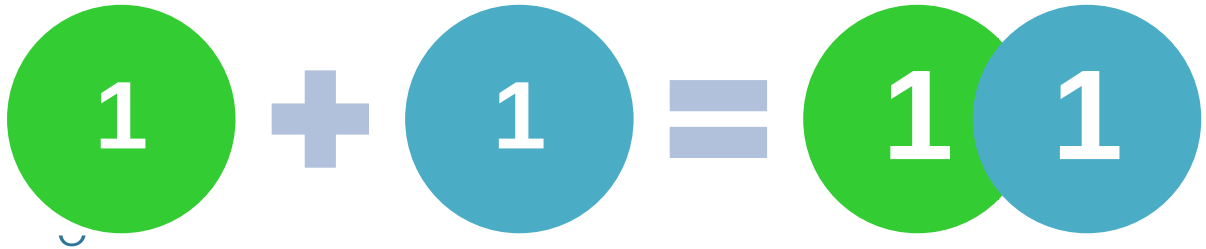
В 2017 году по сравнению с 2015-2016 наблюдается значительное возрастание спроса на криптографические библиотеки с различными интерфейсами и под различные платформы

Происходит некое качественное изменение рынка и наша с вами задача не упустить это окно возможностей

Для этого ИнфоТеКС открывает новое продуктовое направление «Криптографические библиотеки для встраивания»

Зачем?

- Синергия с лидерами рынка
- Рост собственной экспертизы
- Выход на смежные рынки
- Оптимизация стоимости решений
- Новые продукты в портфеле



Что происходит на рынке?

- Рынок далек от насыщения и будет расти еще несколько лет
- Тренд импортозамещения усиливается
- Растет информированность граждан в вопросах ИБ (ЭП, токены, https)
- Растет объем электронного взаимодействия (СЭД, СМЭВ, ККТ), активно развиваются мобильные решения
- С подачи государства регуляторы расширяют сферы влияния (НСПК, КИИ, Пр.-1380, Постановление 1104)

Что происходит у нас?

Спрос:
за 2017 г. зафиксировано >25 запросов на криптокомпоненты от технологических партнеров

Окно возможностей

Предложение:
криптографические компоненты разной степени зрелости (P11, OSSL, CSP, JCrypto)

Что мы с этим будем делать?

- Разрабатывать и поставлять **технологическим партнерам** криптобиблиотеки ViPNet OEM Crypto (VOC), предназначенные для встраивания сторонними разработчиками

Осуществлять

- Продажи
- *Сертификацию / контроль встраивания СКЗИ*
- *Анализ уязвимостей решений партнеров*

Как и кто может стать ТП?

- Выгода для двух сторон очевидна
- Перспектива монетизации
- Желание вкладываться ресурсами
- Формализация требований к желаемому результату
- Четкое представление конечного результата
- Активные совместные действия
- Готовность к долгосрочным отношениям

Необходимые действия

- Обосновать почему это выгодно
- Заполнить опросники

  Детально и подробно(!)
- Подписать NDA
- Подписать Соглашение о ТП
- Готовность к передаче или обмену техно
- Назначить ответственных

Почему мы считаем, что можем это делать?

- Практика безопасной разработки SDL
- Устранение ошибок/предупреждений статических анализаторов
- Четыре типа тестирования
- Регулярные замеры производительности (Google Benchmark)
- Unit Tests в режиме непрерывной интеграции. Покрытие тестами свыше 95% кода

ViPNet CryptoUnderground – *алгоритмическое криптоядро: криптомеханизмы на языке C/C++. Максимальная оптимизация и независимость*

Платформы: Win, Lin, UEFI, Байкал, Android, ~~Тайзен~~, Sailfish, iOS, macOS, Эльбрус, STM32

Архитектуры: x86, x86-64, ARM, MIPS, elbrus, RISC

ViPNet CryptoUnderground

Реализовано (небольшая часть, для примера):

- Реализация шифраторов на различных инструкциях:
  a. ГОСТ 28147-89 на SIMD инструкциях процессора ARMv7-A
  b. ГОСТ 28147-89, 34.12-2015, ГОСТ 34.11-2012 на SIMD инструкциях процессора Intel
  c. ГОСТ 28147-89, 34.12-2015 на инструкциях AVX2
  d. Шифратор AES256 на инструкциях AESNI
- Реализация утилиты измерения производительности (google benchmark)
- Сборка под платформы Байкал, Эльбрус, STM32
- Реализация тестов соответствия (datafit) для FIPS криптографии в CU

Не СКЗИ

ViPNet P11 (SoftToken) - *группа компонентов, реализующих стандартный криптографический интерфейс PKCS #11*

Платформы: Windows, Linux, Байкал, Эльбрус, ~~Тайзен~~, Sailfish, iOS

- Базовое криптоядро
- Соответствие мировому стандарту PKCS#11
- Библиотека с алгоритмами + защищенное хранилище

Не СКЗИ

ViPNet OSSL - *движок (engine), позволяющий выполнять криптографические операции по алгоритмам ГОСТ при взаимодействии с пакетом OpenSSL.*

Платформы: Windows, Linux, Байкал, Тайзен, Sailfish

Функциональность (дополнительно к SoftToken):

- Организация TLS-соединений по алгоритмам ГОСТ
- Выполнение функций УЦ (поддержка PKI на базе стандарта X.509)
- Поддержка CMS с использованием алгоритмов ГОСТ
- Поддержка алгоритмов экспорта и импорта ключей, в т.ч. PKCS#12 (PFX)

Многократно сертифицировано в составе ПАКов

Есть согласованное ТЗ. Идет подготовка к получению заключения

ViPNet CSP Win - *криптопровайдер для приложений Microsoft и другого ПО с интерфейсом CryptoAPI 2.0*

Функциональность (основная):

- Создание ключей ЭП, формирование и проверка ЭП по ГОСТ Р 34.10-2001, ГОСТ Р 34.10-2012
- Хэширование данных по ГОСТ Р 34.11-94 и ГОСТ Р 34.11-2012
- Шифрование и имитозащита данных по ГОСТ 28147-89
- Создание СЧ и ПСЧ, сессионных ключей шифрования
- Работа с электронными ключами на внешних устройствах
- Аутентификация и выработка сессионного ключа SSL/TLS
- Создание/проверку ЭП (CAdES-T, CAdES-BES, XML-DSig, XAdES-BES)

Сертифицированное СКЗИ

ViPNet CSP Lin - *криптопровайдер для ОС Linux с интерфейсом ViPNet CryptoAPI for Linux*

Платформы: Linux, Байкал, Эльбрус

Функциональность (основная):

- Создание ключей ЭП, формирование и проверка ЭП по ГОСТ Р 34.10-2001, ГОСТ Р 34.10-2012
- Хэширование данных по ГОСТ Р 34.11-94 и ГОСТ Р 34.11-2012
- Шифрование и имитозащита данных по ГОСТ 28147-89
- Создание СЧ и ПСЧ, сессионных ключей шифрования
- Работа с электронными ключами на внешних устройствах
- Создание и проверку ЭП в форматах CAdES-T, CAdES-BES

Сертифицированное СКЗИ

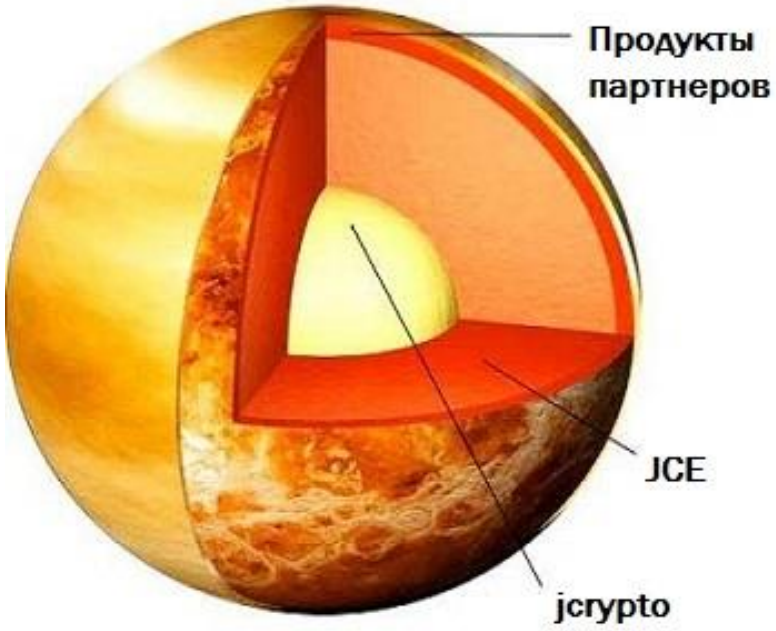
ViPNet JCrypto SDK – *криптопровайдер для Java-машин Dalvik (Android) и Oracle JDK (Windows, Linux, macOS) с интерфейсом JCA*

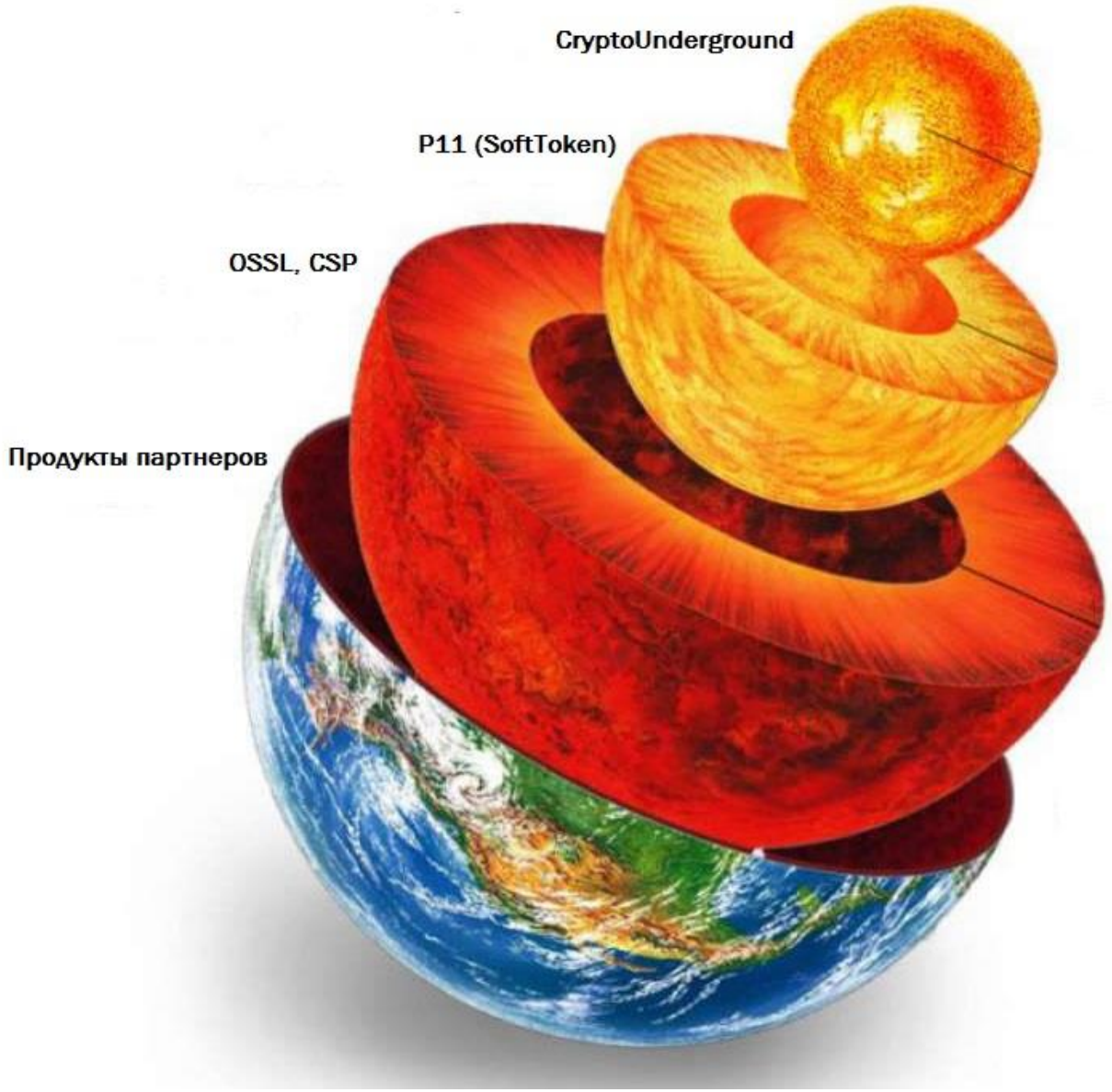
Функциональность (основная):

- Генерация ключей ЭП и шифрования в по ГОСТ Р 34.10-2001, ГОСТ Р 34.10-2012
- Вычисление хэш-функции по ГОСТ Р 34.11-94, ГОСТ Р 34.11-2012
- Вычисление и проверка ЭП по ГОСТ Р 34.10-2001, ГОСТ Р 34.10-2012
- Выработка ПСЧ, сессионных ключей шифрования
- Шифрование и имитозащита данных по ГОСТ 28147-89
- Создание запроса PKCS#10, работа с токенами по PKCS#11
- Аутентификация и шифрование по протоколам TLS 1.2
- Операции с сертификатами открытых ключей X.509 v3
- PKCS#7 (CMS, CAdES-BES), S/MIME, XMLDSig, SOAP. OCSP-запросы и ответы

Согласовано ТЗ на КС1 (заключение), идут тематические исследования.

Строение ~~планеты~~ криптографических компонент





«Почем опиум для народа»?

Лицензирование

- Ограничение срока действия лицензии
- Ограничение функциональности
- Ограничение производительность

Ценовая политика

- «Гибкая»
- Поштучная продажа
- Безлимитные лицензии

infotecs

Спасибо за внимание!

Обращайтесь!
E-mail - **techpartners@infotecs.ru**

Сергей Петренко
Sergey.Petrenko@infotecs.ru
+7 (495) 737-61-92 (5240)

Елена Выходцева
Elena.Vykhodtseva@infotecs.ru
+7 495 737-61-92 (доб. 5275)