РусКрипто XXVIII НАУЧНО-ПРАКТИЧЕСКАЯ КОНФЕРЕНЦИЯ

Развитие интерфейсов криптографических библиотек для решения прикладных задач

Арина Эм, ИнфоТеКС

МЫ КАК ВЕНДОР СТАЛКИВАЕМСЯ С НЕКОТОРЫМИ ВЫЗОВАМИ ПРИ РАЗВИТИИ БИБЛИОТЕК

Технологии развиваются, и от нас ожидают

- использование новых интерфейсов
- обеспечение удобства работы с библиотеками
- использование и реализация актуальных технологий и форматов
- новые сценарии использования

О ЧЕМ СЕГОДНЯ ПОГОВОРИМ

ViPNet CSP

ViPNet OSSL

XMLdsig

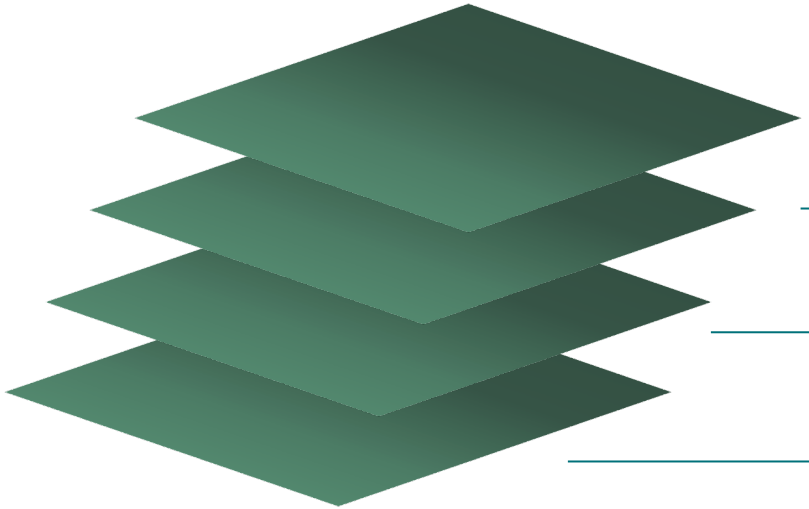
SQLite

JOSE (OpenID Connect)

ViPNet JCrypto SDK

ViPNet CryptoSmart

КАК МЫ СТРОИМ АРХИТЕКТУРУ СКЗИ



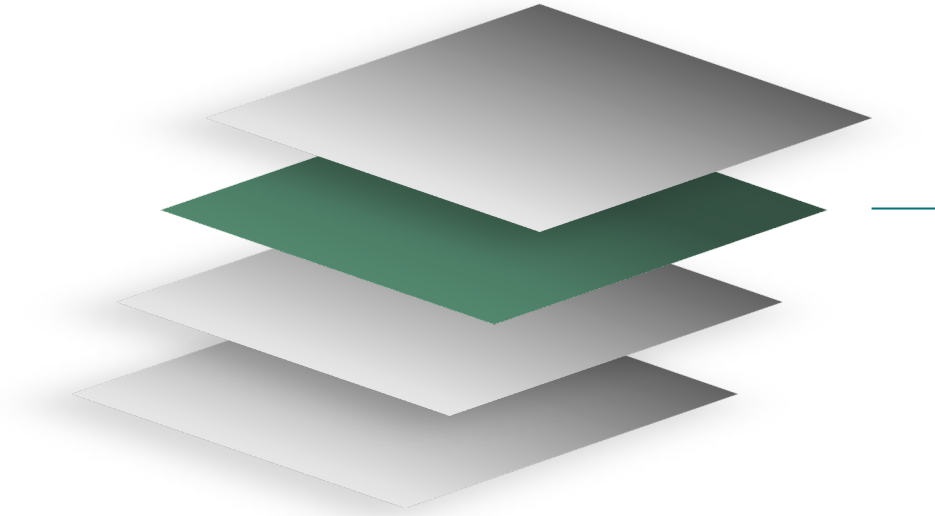
4 уровень
Прикладное ПО

3 уровень
Крипто форматы и протоколы

2 уровень
Стандартный интерфейс PKCS#11

1 уровень
Криптопримитивы

КРИПТОГРАФИЧЕСКИЕ ФОРМАТЫ И ПРОТОКОЛЫ



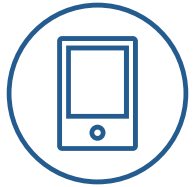
3 уровень

ViPNet OSSL - КРИПТОЯДРО

ViPNet OSSL - библиотека для встраивания на базе OpenSSL, используется для разработки приложений и сервисов

Важные особенности

- Стандартные интерфейсы OpenSSL и PKCS#11
- Возможность развертывания на серверной и клиентской стороне



Для мобильных и планшетов

Для десктопов

Для серверов

ViPNet XMLdsig

Модуль ViPNet OSSL

- Работа с электронной подписью в формате XML
- Алгоритмы подписи и хэширования по алгоритмам ГОСТ
- Расширенные форматы XML-подписи (XAdES)
- Электронная XML-подпись в формате СМЭВ 3
- Электронная XML-подпись в формате WS-Security

ViPNet SQLite

Модуль ViPNet OSSL

Перед нами стояли задачи

- шифрование данных приложений без влияния на производительность
- сделать так, чтобы конечный продукт не требовал проведения ТИ

Компонент предоставляет API для шифрования страниц,
которые вызывает SEE (SQLite Encryption Extension)

ViPNet JOSE

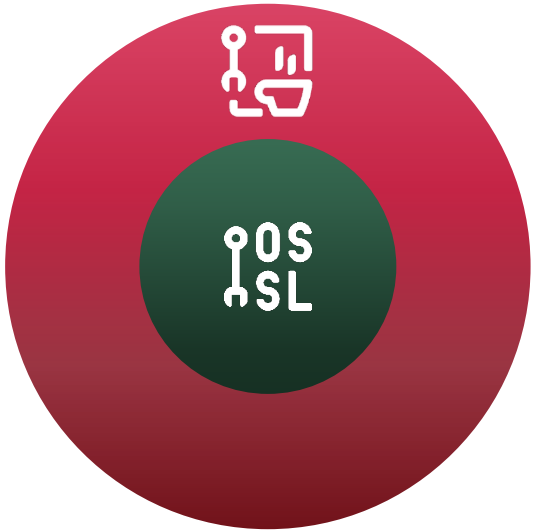
Модуль ViPNet OSSL

JOSE (JSON Object Signing and Encryption) - набор стандартов, определяющих способы защиты данных и их обмена в формате JSON, используя подпись и шифрование.

- Включает в себя несколько спецификаций (JWT, JWS, JWE, JWK и JWA), которые позволяют безопасно передавать и проверять информацию между различными системами
- Цель – создание SDK для работы со структурами JOSE, в том числе с использованием ГОСТ алгоритмов

ViPNet JCrypto SDK

Обертка ViPNet OSSL



Криптографическая библиотека на языке Java
Реализует интерфейс для работы с криптофункциями при помощи обращений к ViPNet OSSL

ViPNet JCrypto SDK – это надстройка на Java поверх ViPNet OSSL

Криптографические java-стандарты

JCE | JSSE | Java XMLDsig

ViPNet CryptoSmart

Обертка ViPNet OSSL

Криптобиблиотека для встраивания
Для ПО на базе Hyperledger Fabric

- интеграции российских криптоалгоритмов в блокчейн-платформы
- формирования, проверки и защиты цепочки блоков
- аутентификации пользователей
- управления правами доступа
- защиты данных
- защиты каналов связи по протоколу TLS

РусКрипто
XXVIII НАУЧНО-ПРАКТИЧЕСКАЯ КОНФЕРЕНЦИЯ

Спасибо за внимание!

Арина ЭМ
arina.em@infotecs.ru
@cryptografinya