

Криптография для разработчиков прикладных систем

Арина Эм

техно infotecs
2022 Фест

ТЕХНИЧЕСКАЯ
КОНФЕРЕНЦИЯ

Прикладные системы: какие бывают

Офисные приложения Документооборот
Сервисы доставки Шифрование данных в облаке
Мобильные приложения
Финтех Логистика Интернет вещей
Банкинг Мессенджеры Умный дом

СКЗИ: какое выбрать?

Прикладные

Серверные
Мобильные

ViPNet OSSL
ViPNet CSP

Самостоятельные

Серверные

TLS Gateway
PKI Service

Мобильные

PKI Client

Зачем использовать криптобиблиотеки



Для разработки собственных программ и создания расширений

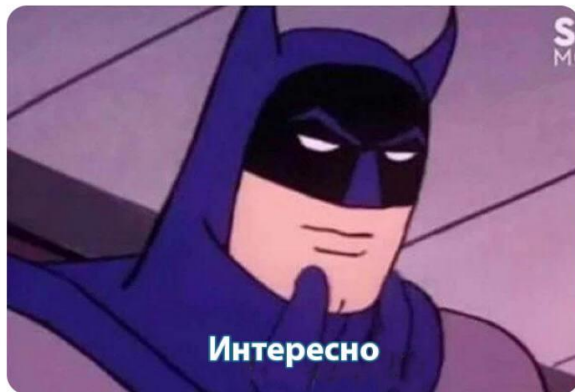
Зачем использовать криптобиблиотеки



Это проще и дешевле,
чем писать самостоятельно

Когда потратил 4 часа на
создание функции, а потом
нашёл библиотеку, в которой она
реализована проще и лучше:

работке



Зачем использовать криптобиблиотеки



Они помогают разработчикам

- Берегут время разработки
- Сложно неправильно использовать
- Реализуют сильную криптографию
- Кроссплатформенные
- Используют стандартные интерфейсы

Криптобиблиотеки Инфотекс



ViPNet CSP



ViPNet OSSSL



ViPNet
JCrypto SDK



ViPNet
CryptoSmart

Какой есть функционал

Работа с ЭП

- ГОСТ Р 34.10-2001*
- ГОСТ Р 34.10-2012

Хэширование

- ГОСТ Р 34.11-94*
- ГОСТ Р 34.11-2012

Шифрование

- ГОСТ 28147-89*
- 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



Какой есть функционал



Форматы

- CMS
- PFX
- XMLDsig
- CAdES
- XAdES
- X.509



Интерфейсы

- OpenSSL
- PKCS#11
- Microsoft CryptoAPI
- JNI/JCA



Протоколы

- TSP
- OCSP
- TLS

CSP ViPNet CSP

Для тех, кто разрабатывает ПО под Windows

ViPNet CSP

криптография для граждан и для
встраивания



Для физических лиц



Для разработчиков

Новое в версии 4.4.2

Доработали ViPNet CSP в соответствии с
приказом ФСБ №795

Сертификаты ГУЦ и Минкомсвязи
устанавливаются автоматически

Поддержка TLS включена по умолчанию



ФЕДЕРАЛЬНАЯ СЛУЖБА БЕЗОПАСНОСТИ
РОССИЙСКОЙ ФЕДЕРАЦИИ

Система сертификации РОСС RU.0001.030001

СЕРТИФИКАТ СООТВЕТСТВИЯ

Регистрационный номер СФ/124-4103 от "10" августа 2021 г.

Действителен до "10" августа 2024 г.

Выдан Акционерному обществу «Информационные технологии и коммуникационные системы».

Настоящий сертификат удостоверяет, что средство криптографической защиты информации (СКЗИ) VIPNet CSP 4.4 (Версия 4.4.2) (исполнения 1, 2, 3, 4, 5, 6) в комплектации согласно формуляру ФРКЕ.00106-07 30 01 ФО

соответствует Требованиям к средствам криптографической защиты информации, предназначенным для защиты информации, не содержащей сведений, составляющих государственную тайну, класса КС1 (для исполнений 1, 4), класса КС2 (для исполнений 2, 5), класса КС3 (для исполнений 3, 6), Требованиям к средствам электронной подписи, утверждённым приказом ФСБ России от 27 декабря 2011 г. № 796, установленным для класса КС1 (для исполнений 1, 4), класса КС2 (для исполнений 2, 5), класса КС3 (для исполнений 3, 6) и может использоваться для криптографической защиты (создание и управление ключевой информацией, шифрование файлов и данных, содержащихся в областях оперативной памяти, вычисление имитовставки для файлов и данных, содержащихся в областях оперативной памяти, вычисление значения хэш-функции для файлов и данных, содержащихся в областях оперативной памяти, защита TLS-соединений, реализация функций электронной подписи в соответствии с Федеральным законом от 6 апреля 2011 г. № 63-ФЗ «Об электронной подписи»: создание электронной подписи, проверка электронной подписи, создание ключа электронной подписи, создание ключа проверки электронной подписи) информации, не содержащей сведений, составляющих государственную тайну.

Сертификат выдан на основании результатов проведенных Обществом с ограниченной ответственностью «СФБ Лаборатория»

сертификационных испытаний образцов продукции №№ 637Д-000506, 637Д-000507, 637Д-000508, 637Д-000509, 637Д-000510, 637Д-000511.

Безопасность информации обеспечивается при использовании СКЗИ в соответствии с требованиями эксплуатационной документации согласно формуляру ФРКЕ.00106-07 30 01 ФО.

Заместитель руководителя Научно-технической
службы – начальник Центра защиты информации
и специальной связи ФСБ России



О.В. Скрибин

VIPNet CSP 4.4.2 сертифицирован ФСБ России

По классам КС1, КС2, КС3
До 10 августа 2024 года

OS
SSL

VIPNet OSSSL

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!

ViPNet OSSSL 5.0: TLS

цифры

| | Односторонний TLS | Двусторонний TLS |
|----------------------------------|-------------------|------------------|
| Скорость передачи данных | 8300 Мбит/с | 8200 Мбит/с |
| Скорость установления соединений | 8425 соедин/с | 5 260 соедин/с |
| Время установления соединения | 11 мс | 17 мс |

Условия:

Debian 9.12.0

nginx 1.14.0

ViPNet OSSSL 5.0

ViPNet Coordinator HW 5000 Q1

12 ядер, HyperThreading ON

GOST2012-GOST8912-GOST8912

Длина ключа 256

TLS 1.2

VIPNet OSSSL 5.0: Подпись цифры

| Потоки | Подпись, шт/с | Проверка подписи, шт/с |
|--------|---------------|------------------------|
| 1 | 23,1k | 3,5k |
| 24 | 255,1k | 35,9k |

Условия:

Алгоритм ГОСТ 34.10-2012 (256)

Лицензирование ViPNet OSSL

Для серверов



1 лицензия –
1 устройство

Для клиентов



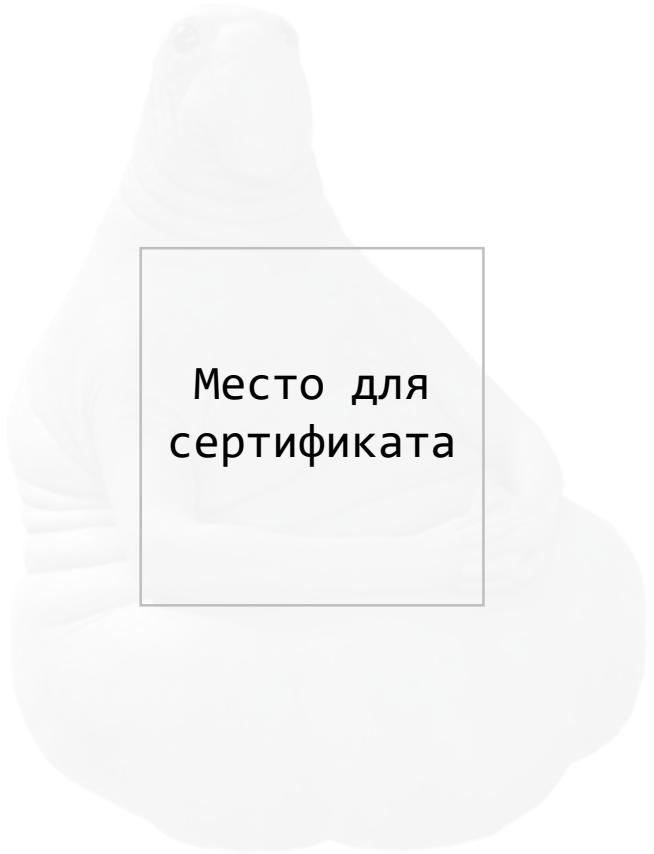
Десктоп

1 лицензия –
1 устройство



Мобильные

1 лицензия –
100 устройств



Место для
сертификата

Сертификация

Заключение ФСБ:

II кв. 2022



ViPNet JCrypto SDK

Для тех, кто разрабатывает ПО на Java

ViPNet JCrypto SDK

Криптопровайдер на Java



Использует ViPNet OSSL
как криптоядро

- Криптографические функции
- Лицензирование

В процессе сертификации



ViPNet CryptoSmart

Для тех, кому нужен ГОСТ в блокчейне

ViPNet CryptoSmart

СКЗИ для блокчейн-платформ
на базе Hyperledger Fabric

Обеспечивает

- Защиту конфиденциальных данных
- Юридическую значимость транзакций
- Интеграцию с отечественной РКІ
- Соответствие требованиям ПКЗ-2005

В процессе сертификации



HYPERLEDGER
FABRIC

Библиотеки Инфотекс

ViPNet CSP

Платформы



Интерфейсы

MS CryptoAPI

Класс защиты

KC1-KC3

Сертификат ФСБ

да

ViPNet OSSL

Платформы



Интерфейсы

PKCS#11
OpenSSL

Класс защиты

KC1-KC3

Сертификат ФСБ

почти да

ViPNet JCrypto SDK

Платформы



Интерфейсы

JNI/JCA
PKCS#11

Класс защиты

KC1

Сертификат ФСБ

еще нет

ViPNet CryptoSmart

Платформы



Интерфейсы

MSP
NetCSP
BCCSP Lite

Класс защиты

KC1, KC2

Сертификат ФСБ

почти да

Подробная документация и примеры кода

Руководство администратора

Информация об установке и настройке
для работы со сторонним ПО

Справочник функций

Описание функций и их параметров

Руководство разработчика

Сведения о разработке с помощью
библиотек

Примеры

Примеры кода с обращением к
перечисленным функциям
+ Приложения для тестирования
возможностей

Как выбрать API

CryptoAPI

- предназначен для разработчиков приложений на основе Windows
- Позволяет интегрироваться с приложениями Microsoft, встроиться в механизмы ОС



OpenSSL

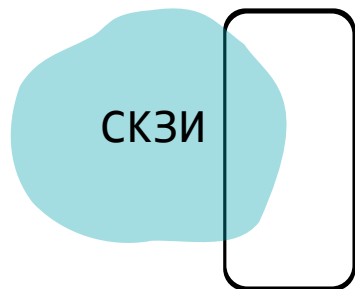
- используется практически всеми сетевыми серверами для защиты передаваемой информации
- можно использовать на различных языках программирования
- кроссплатформенность



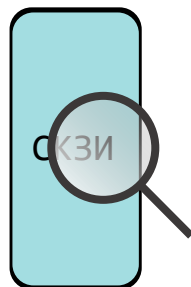
Особенности сертификации

Особенности сертификации

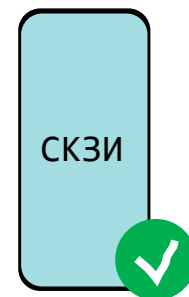
1 Встраивание



2 Оценка влияния



3 Заключение



К нам обращаются по вопросам

Использование в связке
с nginx или apache

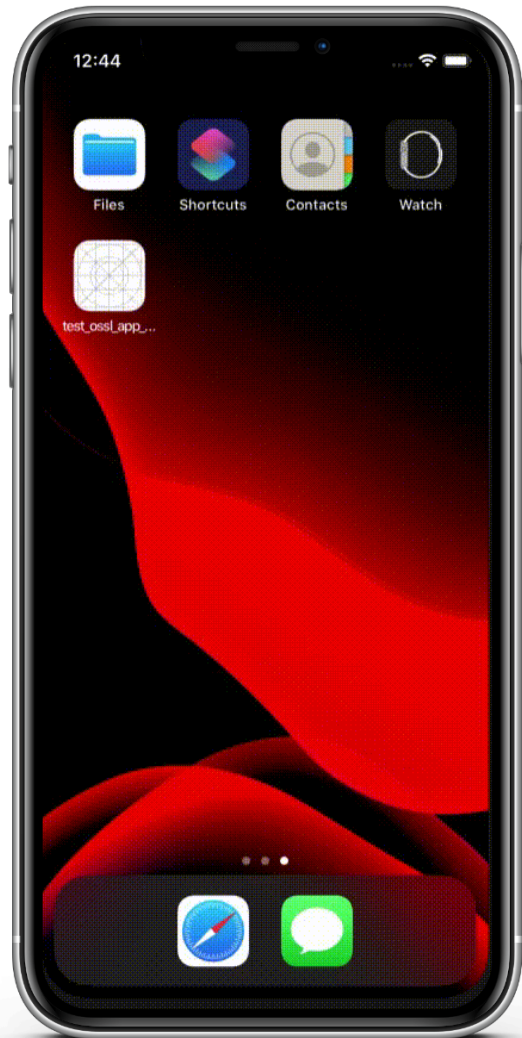
Защита канала между клиентом
и сервером

Встраивание в пользовательское
приложение для шифрования
файлов и электронной подписи

Как можно попробовать

- 1 Подключиться к сайту ИнфоТеКС по TLS ГОСТ
- 2 Протестировать TLS 1.2 и 1.3 на нашем стенде
- 3 Купить или взять на тесты: soft@infotecs.ru

**Если осталось
время**



Приложение с VipNet OSSL



Приложение с VipNet OSSL

ТЕХНО infotecs
2022 Фест

Остаемся на связи!

Арина Эм

Arina.Em@infotecs.ru

Подписывайтесь на наши соцсети



https://vk.com/infotecs_news



https://t.me/infotecs_news