Криптография для разработчиков прикладных систем

Арина Эм
Ведущий менеджер продуктов

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	ViPNet OSSL
	Мобильные	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:

зработке

Зачем использовать криптобиблиотеки

Они помогают разработчикам

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

Криптобиблиотеки Инфотекс

ViPNet **CSP**

ViPNet **OSSL**

ViPNet
JCrypto SDK

ViPNet
CryptoSmart

Какой есть функционал

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

Какой есть функционал

Форматы

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

Интерфейсы

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

Протоколы

- TSP
- OCSP
- TLS

ТехноФест infotecs 2023

ViPNet CSP

Для тех, кто разрабатывает ПО под Windows

ViPNet CSP

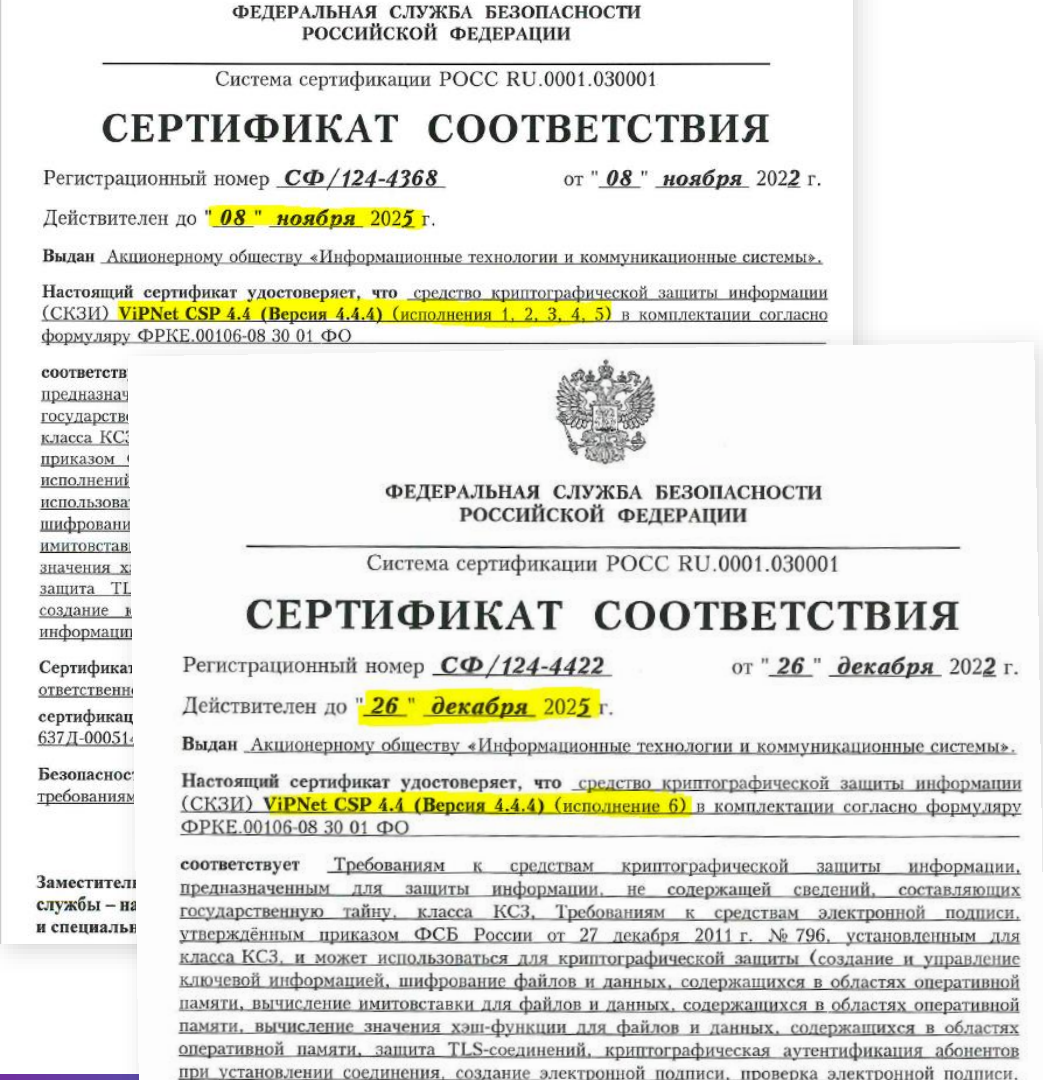
криптография для граждан
и для встраивания

Для физических лиц

Для разработчиков

Новое в версии 4.4.4 Win

- Поддержка Windows 11
- Поддержка обновлений Windows 10
- Совместимость с КриптоПро ЭЦП Browser plug-in
- Поддержка драйверов ESMART PKI Client 4.7



ФЕДЕРАЛЬНАЯ СЛУЖБА БЕЗОПАСНОСТИ
РОССИЙСКОЙ ФЕДЕРАЦИИ

Система сертификации РОСС RU.0001.030001

СЕРТИФИКАТ СООТВЕТСТВИЯ

Регистрационный номер СФ/124-4368 от "08" ноября 2022 г.

Действителен до "08" ноября 2025 г.

Выдан Акционерному обществу «Информационные технологии и коммуникационные системы».

Настоящий сертификат удостоверяет, что средство криптографической защиты информации (СКЗИ) ViPNet CSP 4.4 (Версия 4.4.4) (исполнения 1, 2, 3, 4, 5) в комплектации согласно формуляру ФРКЕ.00106-08 30 01 ФО

ФЕДЕРАЛЬНАЯ СЛУЖБА БЕЗОПАСНОСТИ
РОССИЙСКОЙ ФЕДЕРАЦИИ

Система сертификации РОСС RU.0001.030001

СЕРТИФИКАТ СООТВЕТСТВИЯ

Регистрационный номер СФ/124-4422 от "26" декабря 2022 г.

Действителен до "26" декабря 2025 г.

Выдан Акционерному обществу «Информационные технологии и коммуникационные системы».

Настоящий сертификат удостоверяет, что средство криптографической защиты информации (СКЗИ) ViPNet CSP 4.4 (Версия 4.4.4) (исполнение 6) в комплектации согласно формуляру ФРКЕ.00106-08 30 01 ФО

соответствует Требованиям к средствам криптографической защиты информации, предназначенным для защиты информации, не содержащей сведений, составляющих государственную тайну, класса КС3, Требованиям к средствам электронной подписи, утверждённым приказом ФСБ России от 27 декабря 2011 г. № 796, установленным для класса КС3, 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, криптографическая аутентификация абонентов при установлении соединения, создание электронной подписи, проверка электронной подписи,

ViPNet CSP 4.4.4

сертифицирован ФСБ России по классам КС1, КС2, КС3

до 8 ноября 2025 года

ТехноФест infotecs 2023

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

Лицензирование ViPNet OSSL

Для серверов

1 лицензия –
1 устройство

Для клиентов

Десктоп

1 лицензия –
1 устройство

Мобильные

1 лицензия –
100 устройств

Место для сертификата

ViPNet OSSL 5.0

получил заключение по классам КС1, КС2

до 10 ноября 2027 года

ТехноФест infotecs 2023

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

ТехноФест 2023 infotecs

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 PKI
- Соответствие требованиям ПКЗ-2005

В процессе сертификации

Библиотеки Инфотекс

ТЕХНО infotecs 2023 ФЕСТ

ViPNet CSP

Платформы

Интерфейсы

MS CryptoAPI

Класс защиты

КС1-КС3

Сертификат ФСБ

да

ViPNet OSSL

Платформы

Интерфейсы

PKCS#11
OpenSSL

Класс защиты

КС1-КС3

Сертификат ФСБ

да

ViPNet JCrypto SDK

Платформы

Интерфейсы

JNI/JCA
PKCS#11

Класс защиты

КС1

Сертификат ФСБ

ожидаем во II кв.

ViPNet CryptoSmart

Платформы

Интерфейсы

MSP
NetCSP
BCCSP Lite

Класс защиты

КС1, КС2

Сертификат ФСБ

ожидаем во II кв.

Подробная документация и примеры кода

Руководство администратора

Информация об установке и настройке для работы со сторонним ПО

Руководство разработчика

Сведения о разработке с помощью библиотек

Справочник функций

Описание функций и их параметров

Примеры

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

ТехноФест 2023 infotecs

Как выбрать API

CryptoAPI

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

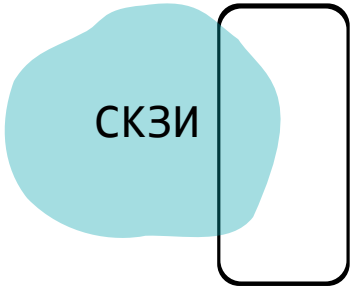
OpenSSL

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

Особенности сертификации

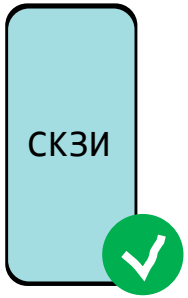
Особенности сертификации

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. Забрать на сайте все, что выложено в открытый доступ

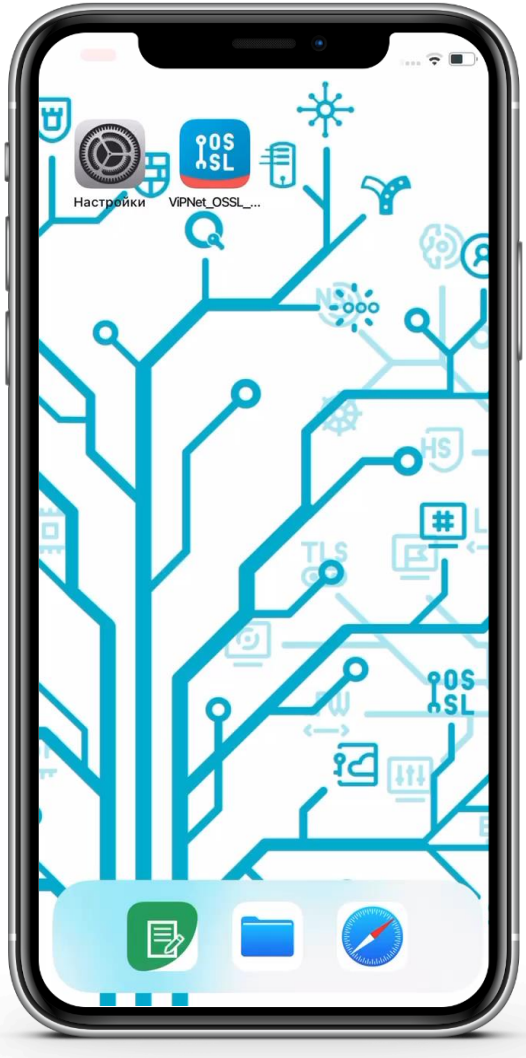
   ViPNet CSP (Windows)

   ViPNet OSSL (Windows, Linux)

2. Купить или взять на тесты: soft@infotecs.ru

Или можно писать лично мне Arina.Em@infotecs.ru

Если осталось время



Приложение с ViPNet OSSL

Подробнее – на нашем стенде

ТЕХНО 2023 infotecs ФЕСТ

Спасибо за внимание!

Подписывайтесь на наши соцсети

vk.com/infotecs_news

https://t.me/infotecs_official

rutube.ru/channel/24686363