Криптография для разработчиков прикладных систем

Арина Эм
Ведущий менеджер продуктов

О чем сегодня будем говорить

1. Зачем использовать криптобиблиотеки
2. Криптобиблиотеки Инфотекс
3. Как встроить криптографию в свое ПО
4. Как выбрать API
5. Особенности сертификации

Зачем использовать криптобиблиотеки

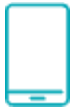
Криптографические библиотеки используют для разработки собственных программ и создания расширений

Криптография в прикладных системах

Офисные приложения

Документооборот

Логистика



Мобильные приложения

Шифрование данных в облаке

Здравоохранение

Банкинг

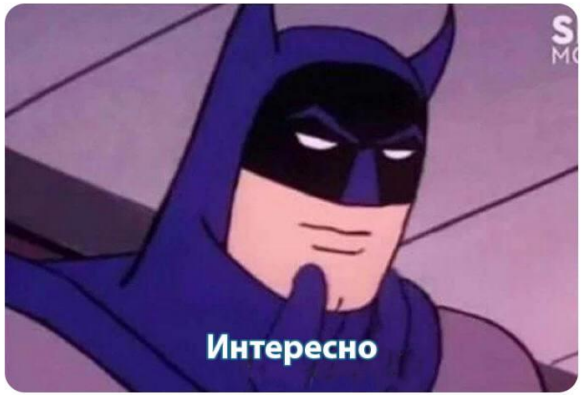
Мессенджеры

Интернет вещей

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:



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

Характеристики и функциональность

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

Поддержка ОС

Форматы

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

Протоколы

- TLS 1.2
- TLS 1.3
- TSP
- OCSP

Работа с ключами на токенах

- Rutoken
- JaCarta
- HSM
- и др..

Интерфейсы

- CryptoAPI
- OpenSSL
- Java SDK
- GO

К нам обращаются по вопросам

- Защита канала между клиентом и сервером
- Организация удаленных защищенных соединений
- Реализация шифрования файлов и электронной подписи в пользовательских приложениях

Криптобиблиотеки Инфотекс

ViPNet CSP

Криптопровайдер для граждан и разработчиков

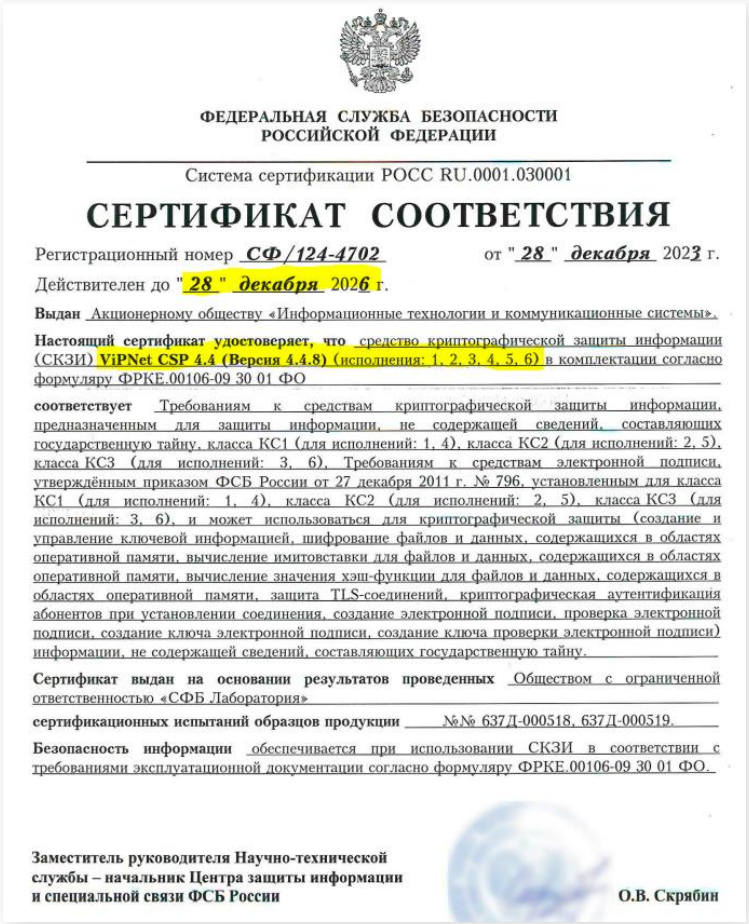
Сертификат ФСБ России: КС1, КС2, КС3

Упрощенная интеграция на Windows

Бесплатно под Windows

Особенности

- Интерфейс MS CryptoAPI
- Поддержка различных форматов подписи
- Актуальные алгоритмы и протоколы
- Совместим с токенами и смарт-картами
- Возможность экспортировать ключи с других машин и криптопровайдеров



ФЕДЕРАЛЬНАЯ СЛУЖБА БЕЗОПАСНОСТИ
РОССИЙСКОЙ ФЕДЕРАЦИИ

Система сертификации РОСС RU.0001.030001

СЕРТИФИКАТ СООТВЕТСТВИЯ

Регистрационный номер **СФ/124-4702** от "**28**" **декабря** 2023 г.

Действителен до "**28**" **декабря** 2026 г.

Выдан Акционерному обществу «Информационные технологии и коммуникационные системы».

Настоящий сертификат удостоверяет, что средство криптографической защиты информации (СКЗИ) **ViPNet CSP 4.4 (Версия 4.4.8)** (исполнения: 1, 2, 3, 4, 5, 6) в комплектации согласно формуляру ФРКЕ.00106-09 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, криптографическая аутентификация абонентов при установлении соединения, 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-000518, 637Д-000519.

Безопасность информации обеспечивается при использовании СКЗИ в соответствии с требованиями эксплуатационной документации согласно формуляру ФРКЕ.00106-09 30 01 ФО.

Заместитель руководителя Научно-технической службы – начальник Центра защиты информации и специальной связи ФСБ России **О.В. Скрябин**

ViPNet CSP 4.4.8

сертифицирован ФСБ России по классам КС1, КС2, КС3

до 28 декабря 2026 года

ViPNet OSSL

Криптобиблиотека для разработки мобильных и серверных решений

Сертификат ФСБ России: КС1, КС2, КС3

Клиентское и серверное исполнение

Поддержка мобильных ОС

Особенности

- Стандартные интерфейсы OpenSSL и PKCS#11
- Поддержка различных форматов подписи
- Актуальные алгоритмы и протоколы
- Содержит программный токен
- Совместим с токенами и смарт-картами
- Возможность экспортировать ключи с других машин и криптопровайдеров

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

Лицензирование ViPNet OSSL

Для серверов

1 лицензия –
1 устройство

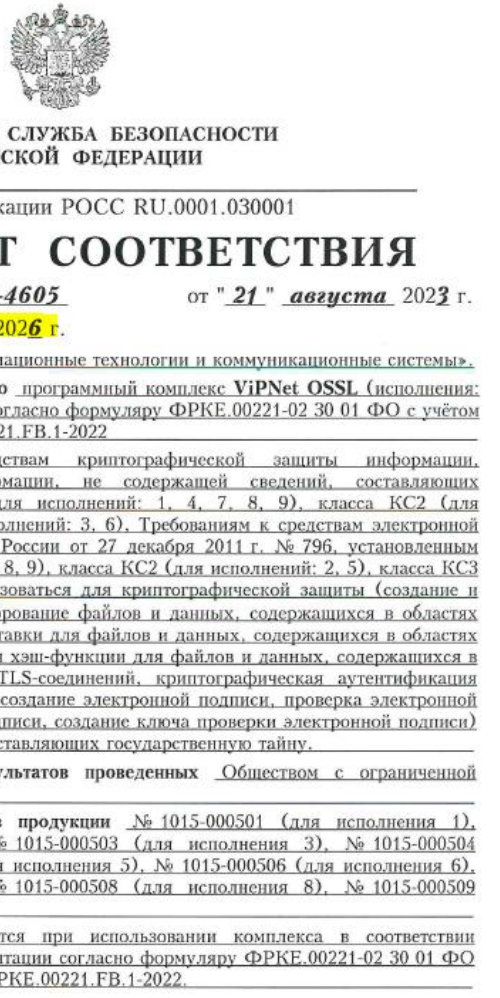
Для клиентов

Десктоп

1 лицензия –
1 устройство

Мобильные

1 лицензия –
100 устройств



ФЕДЕРАЛЬНАЯ СЛУЖБА БЕЗОПАСНОСТИ
РОССИЙСКОЙ ФЕДЕРАЦИИ

Система сертификации РОСС RU.0001.030001

СЕРТИФИКАТ СООТВЕТСТВИЯ

Регистрационный номер *СФ/124-4605* от "*21*" *августа* 2023 г.

Действителен до "*21*" *августа* 2026 г.

Выдан Акционерному обществу «Информационные технологии и коммуникационные системы».

Настоящий сертификат удостоверяет, что программный комплекс **ViPNet OSSL** (исполнения: 1, 2, 3, 4, 5, 6, 7, 8, 9) в комплектации согласно формуляру ФРКЕ.00221-02 30 01 ФО с учётом извещения об изменении № 1 ФРКЕ.00221.ФВ.1-2022

соответствует Требованиям к средствам криптографической защиты информации, предназначенным для защиты информации, не содержащей сведений, составляющих государственную тайну, класса КС1 (для исполнений: 1, 4, 7, 8, 9), 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, 7, 8, 9), 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, криптографическая аутентификация абонентов при установлении соединения, 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 № 1015-000501 (для исполнения 1), № 1015-000502 (для исполнения 2), № 1015-000503 (для исполнения 3), № 1015-000504 (для исполнения 4), № 1015-000505 (для исполнения 5), № 1015-000506 (для исполнения 6), № 1015-000507 (для исполнения 7), № 1015-000508 (для исполнения 8), № 1015-000509 (для исполнения 9).

Безопасность информации обеспечивается при использовании комплекса в соответствии с требованиями эксплуатационной документации согласно формуляру ФРКЕ.00221-02 30 01 ФО с учётом извещения об изменении № 1 ФРКЕ.00221.ФВ.1-2022.

ТЕХНО 2024 infotecs ФЕСТ

ViPNet OSSL 5.4 сертифицирован ФСБ России по классам КС1, КС2, КС3

До 21 августа 2026 года

ViPNet JCrypto SDK

В процессе сертификации

Криптоядро ViPNet OSSL

Криптобиблиотека для разработки на Java-машинах

Особенности

- Стандартные интерфейсы JNI/JCA и PKCS#11
- Поддержка различных форматов подписи
- Актуальные алгоритмы и протоколы
- Содержит программный токен
- Совместим с токенами и смарт-картами

ViPNet CryptoSmart

В процессе сертификации

Криптоядро ViPNet OSSL

Криптобиблиотека для реализации ГОСТ в блокчейне

Особенности

- Поддержка различных форматов подписи
- Актуальные алгоритмы и протоколы
- Содержит программный токен
- Совместим с токенами и смарт-картами

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-КС3

Сертификат ФСБ

да

ViPNet JCrypto SDK

Платформы

Интерфейсы

JNI/JCA
PKCS#11

Класс защиты

КС1

Сертификат ФСБ

в процессе

ViPNet CryptoSmart

Платформы

Интерфейсы

MSP
NetCSP
BCCSP Lite

Класс защиты

КС1, КС2

Сертификат ФСБ

в процессе

С чего начать разработку

Что нужно для старта работ?

Лицензия на разработку защищенных с использованием шифровальных (криптографических) средств информационных систем

Криптографический модуль

- ViPNet OSSL
- ViPNet JCrypto SDK
- ViPNet CSP
- ViPNet CryptoSmarT

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

ТЕХНО 2024 infotecs ФЕСТ

Как выбрать API

CryptoAPI

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

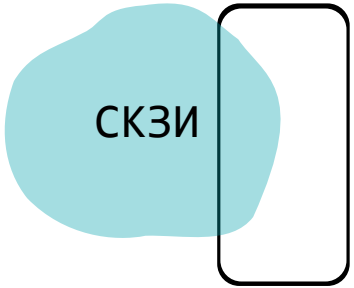
OpenSSL

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

Особенности сертификации

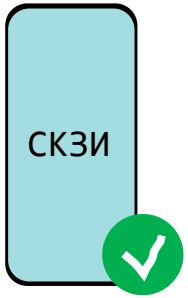
Особенности сертификации

1 Встраивание



2 Оценка влияния

3 Заключение



Когда встроили – пройдите оценку влияния

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

ТЕХНО 2024 infotecs ФЕСТ

Легкого встраивания!

Арина Эм
Arina.Em@infotecs.ru

Подписывайтесь на наши соцсети