# ViPNet JCrypto SDK: о продукте

Арина Эм

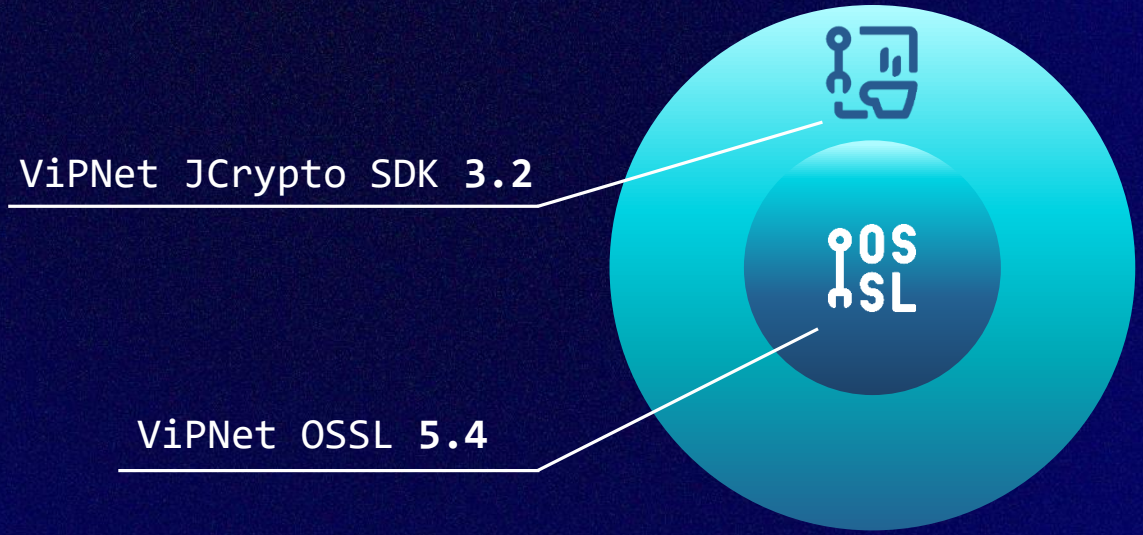
infotecs

# Что такое ViPNet JCrypto SDK

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

Используется для создания приложений,
в которых криптографические операции
выполняются по ГОСТ-алгоритмам

# Актуальная версия



# Функциональность ViPNet JCrypto SDK

infotecs

## 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

## Форматы

CMS
PFX
XMLDsig
X.509

## Защищенные соединения

TLS 1.2
TLS 1.3

## Работа с ключами на токенах

ViPNet HSM
Rutoken
JaCarta

## Интерфейсы

PKCS#11
Java SDK
JNI

## Поддержка ОС

# Криптоядро: 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

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.FB.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.FB.1-2022.

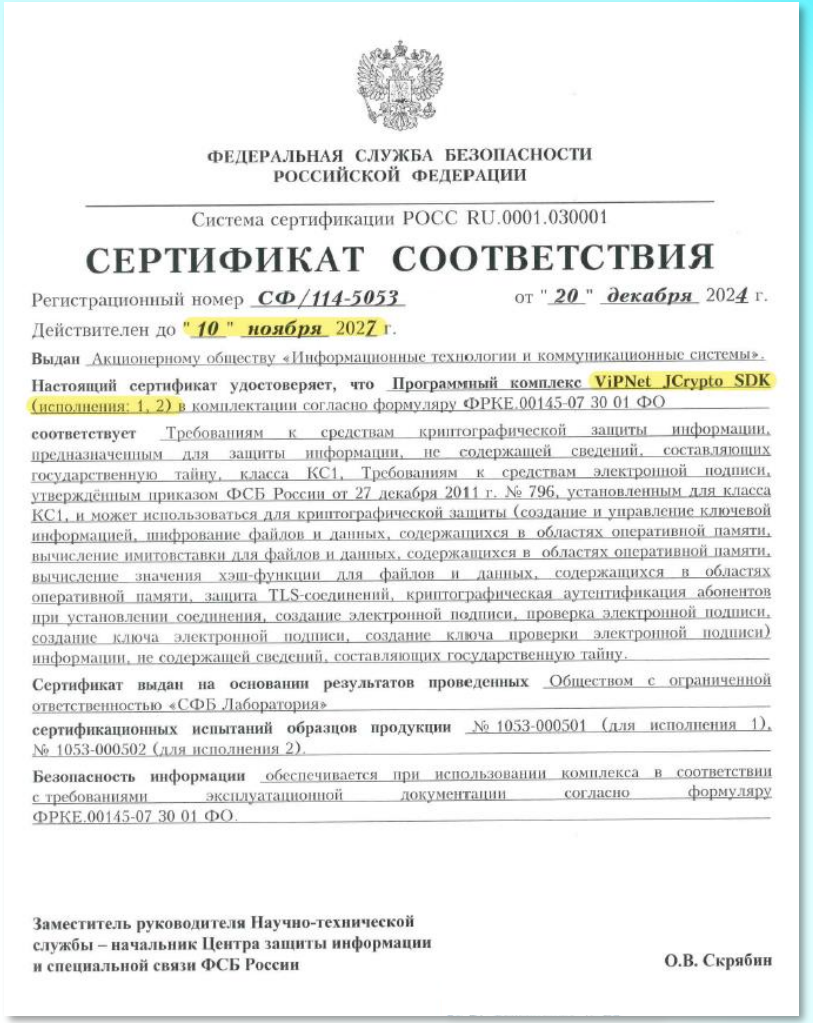
infotecs

# ViPNet OSSL 5.4

## сертифицирован ФСБ России

по классам КС1, КС2, КС3

**до 21 августа 2026 года**



ФЕДЕРАЛЬНАЯ СЛУЖБА БЕЗОПАСНОСТИ
РОССИЙСКОЙ ФЕДЕРАЦИИ

Система сертификации РОСС RU.0001.030001

# СЕРТИФИКАТ СООТВЕТСТВИЯ

Регистрационный номер СФ/114-5053 от "20" декабря 2024 г.

Действителен до "10" ноября 2027 г.

**Выдан** Акционерному обществу «Информационные технологии и коммуникационные системы».

**Настоящий сертификат удостоверяет, что** Программный комплекс ViPNet JCrypto SDK (исполнения: 1, 2) в комплектации согласно формуляру ФРКЕ.00145-07 30 01 ФО

**соответствует** Требованиям к средствам криптографической защиты информации, предназначенным для защиты информации, не содержащей сведений, составляющих государственную тайну, класса КС1, Требованиям к средствам электронной подписи, утверждённым приказом ФСБ России от 27 декабря 2011 г. № 796, установленным для класса КС1, 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** № 1053-000501 (для исполнения 1), № 1053-000502 (для исполнения 2).

**Безопасность информации** обеспечивается при использовании комплекса в соответствии с требованиями эксплуатационной документации согласно формуляру ФРКЕ.00145-07 30 01 ФО.

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

infotecs

# ViPNet JCrypto SDK

## сертифицирован ФСБ России

по классу КС1

До 10.11.2027

# Исполнения ViPNet JCrypto SDK

**Исполнение 1**

Работа на десктоп-ОС

- Windows
- Linux

**Исполнение 2**

Работа на Android

# Архитектуры и операционные системы

## Архитектуры

- x64
- ARM

## Операционные системы

### Linux

CentOS
Debian
Red Hat Enterprise Linux
Ubuntu
Ubuntu Server
SUSE Linux Enterprise Server
Альт
AlterOS
РЕД ОС
РОСА «КОБАЛЬТ»
Astra Linux
Лотос

### Windows

Windows 8.1, 10, 11
Windows Server 2012, 2012 R2
Windows Server 2016, 2019, 2022

### Мобильные ОС

Android 8-12

# Среды функционирования

### Десктоп

- Oracle Java Runtime Environment
- OpenJDK
- Axiom JDK

### Android

ART 8 и выше

# Архитектура

ViPNet JCrypto SDK – это надстройка на Java поверх ViPNet OSSL


Криптографические java-стандарты

JCE | JSSE | Java XMLDsig

# Модули ViPNet JCrypto SDK

**jcrypto-jca**

реализует общие классы, использующие API JCA

**jcrypto-xmldsig**

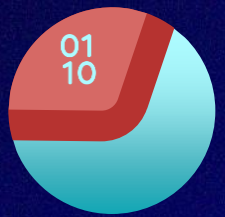
поддержка Java XMLDSig с использованием ГОСТ-алгоритмов

**jcrypto-pkcs11**

работа с внешними устройствами, через PKCS#11

**jcrypto-pkcs7**

работа с подписанными и зашифрованными сообщениями по PKCS#7




**jcrypto-ossl**

поддержка JCA и JSSE с использованием API ViPNet OSSL

# Выбор провайдера для вызова криптографических функций

- ViPNetOSSLProvider
- ViPNetPKCS11Provider
- ViPNetXMLDSigProvider

# Работа с токенами

Работать с криптографическими устройствами стандарта PKCS#11 можете средствами стандартного **API JCA** через **провайдер ViPNetPKCS11Provider**, реализованный в **модуле jcrypto-pkcs11**

**Поддерживаем**

- ViPNet SoftToken
- ViPNet HSM
- JaCarta
  - JaCarta-2 PKI/ГОСТ
  - JaCarta-2 ГОСТ
- Rutoken
  - Рутокен ЭЦП Bluetooth
  - Рутокен ЭЦП 2.0, 2.0 Flash
  - Рутокен ЭЦП 3.0 (NFC) 3100

# Комплект поставки

- ViPNet JCrypto SDK
- ViPNet OSSL
- ViPNet HashCalc

\+ документация

примеры

# Есть дистрибутив – что дальше?

1 Развернуть ViPNet JCrypto SDK

2 Конфигурирование ViPNet OSSL

3 Зарегистрировать продукт

4 * Использование био-рулетки

* только для Android

5 Инициализация провайдеров

ViPNetOSSLProvider
ViPNetPKCS11Provider
ViPNetXMLDSigProvider

6 Инициализация ключевого хранилища (KeyStore)

# Что понадобится для разработки

- Пакеты ViPNet OSSL для разработчика
- Комплекты разработчика JDK или Android SDK
- Фреймворки для автоматизации сборки проектов Gradle или Maven
- Сторонние библиотеки (поставляются вместе с SDK)
- Интегрированная среда разработки (IntelliJ IDEA, Android Studio)

# Что нужно для старта работ?

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

Криптографический модуль

ViPNet OSSL

ViPNet JCrypto SDK

# Важно!

Встроили –
пройдите оценку влияния

# Оценка влияния или сертификация?

## Оценка влияния*

Вызываются функции, описанные в правилах пользования **И**
само встраиваемое СКЗИ сертифицировано

**Какая лицензия нужна разработчику**

Лицензия на разработку защищенных с использованием шифровальных (криптографических) средств ИС

**Результат**

Заключение по оценке влияния

## Создание нового СКЗИ*

Вызываются функции, **не** описанные в правилах пользования, **или**
встраиваемое СКЗИ не сертифицировано

**Какая лицензия нужна разработчику**

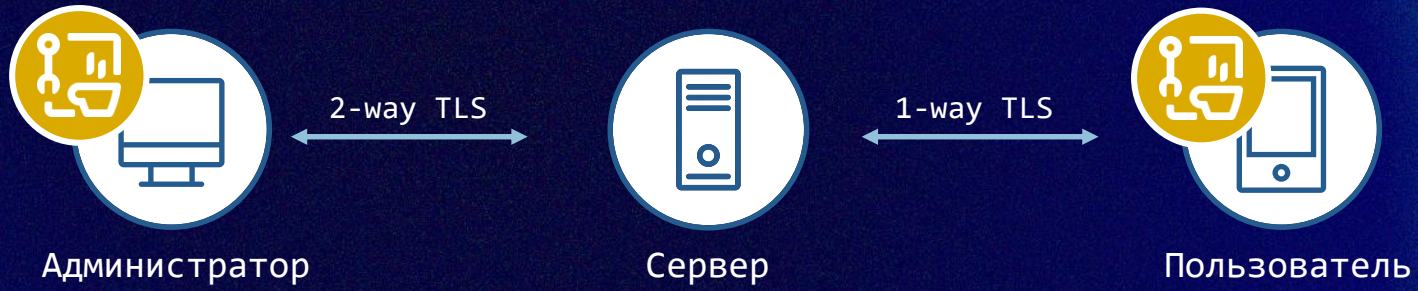
Лицензия на разработку шифровальных (криптографических) средств

**Результат**

Сертификат соответствия

* Постановление Правительства Российской Федерации от 16 апреля 2012 г. №313

# Частые сценарии использования



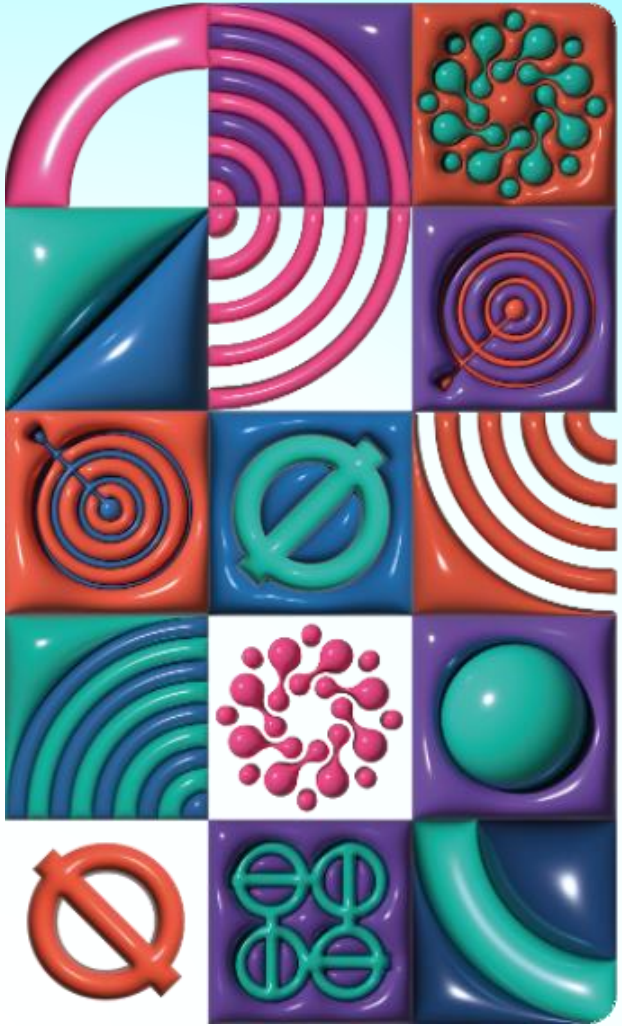

- Защита канала между клиентом и сервером
- Организация удаленных защищенных соединений
- Встраивание в пользовательское приложение для шифрования файлов и электронной подписи

# Как с нами связаться

Купить или взять на тесты:
soft@infotecs.ru

Есть идея реализации совместного решения на базе ViPNet JCrypto SDK:
techpartners@infotecs.ru

Или пишите мне!



# Приходите на Технофест!

13 марта 2025 года

Екатеринбург

## Телеграм-канал
# Криптографиня

@cryptografinya

Подписывайтесь
на наши соцсети,
там много интересного

Арина Эм
Arina.Em@infotecs.ru