Как разрабатывать ПО с криптографией внутри

Арина Эм

План на сегодня

- Как разрабатывать ПО с криптографией внутри
- Какие библиотеки выбрать

Криптография в прикладных системах

Офисные приложения

Документооборот

Логистика

Мобильные приложения

Шифрование данных в облаке

Здравоохранение

Банкинг

Мессенджеры

Интернет вещей

Криптография как основная приправа хорошей прикладной системы

Без криптографии

С криптографией

Что нужно для старта работ?

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

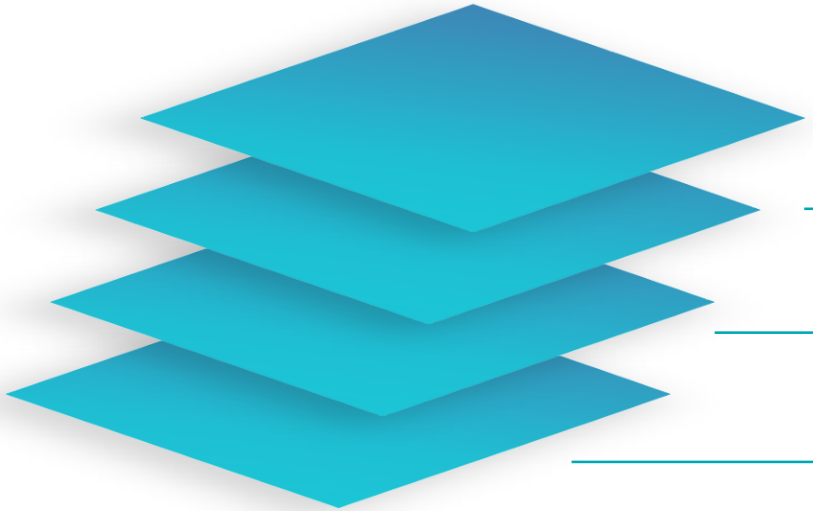
Криптографический модуль

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

- Проработать архитектуру решения
- Определить путь сертификации
- Написать ТЗ
- Сформировать бизнес-логику
- Проработать процесс активации криптофункций в ПО

До старта разработки нужно сделать кое-что еще

Переходим к встраиванию



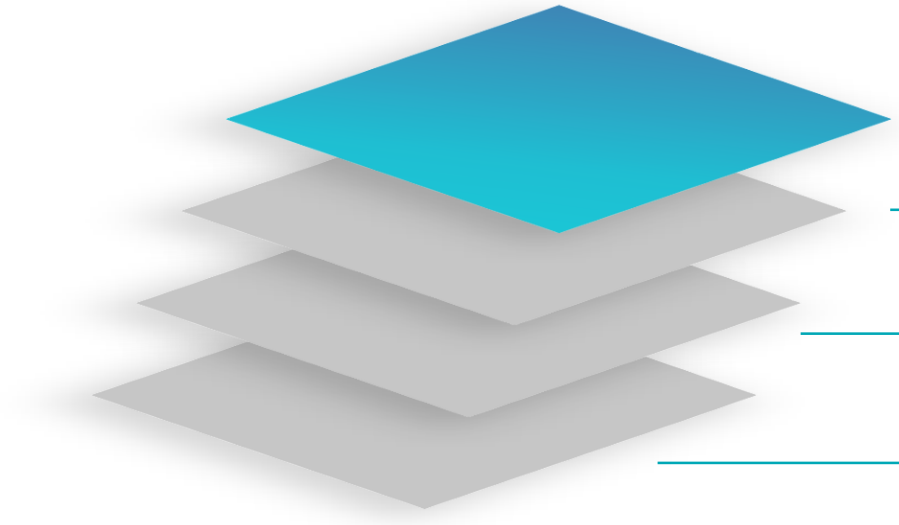
4 уровень
Прикладное ПО

3 уровень
Крипто форматы и протоколы

2 уровень
Стандартный интерфейс PKCS#11

1 уровень
Криптопримитивы

Переходим к встраиванию



4 уровень
Прикладное ПО

3 уровень
Крипто форматы и протоколы

2 уровень
Стандартный интерфейс PKCS#11

1 уровень
Криптопримитивы

ТЕХНО infotecs 2023 ФЕСТ

Когда 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 информационных систем

Что в итоге?

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

Что в итоге?

Сертификат соответствия

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

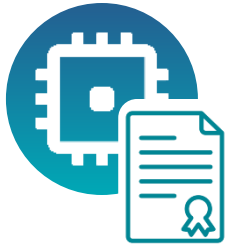
Положение ПКЗ-2005

Приказ ФСБ России от 9 февраля 2005 г. №66 об утверждении положения о разработке, производстве, реализации и эксплуатации шифровальных (криптографических) средств защиты информации

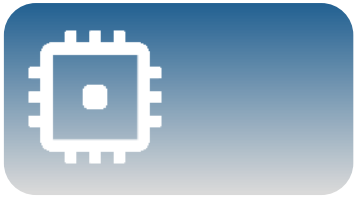
35 **Оценка влияния** аппаратных, программно-аппаратных и программных средств сети (системы) конфиденциальной связи, совместно с которыми предполагается штатное функционирование СКЗИ, на выполнение предъявленных к ним требований **осуществляется разработчиком СКЗИ совместно со специализированной организацией.**

36 **Результаты тематических исследований и оценки влияния** аппаратных, программно-аппаратных и программных средств сети (системы) конфиденциальной связи, совместно с которыми предполагается штатное функционирование СКЗИ, на выполнение предъявленных к ним требований, а также опытные образцы СКЗИ и аппаратные, программно-аппаратные и программные средства, необходимые для штатного функционирования СКЗИ, **передаются в ФСБ России для проведения экспертизы.**

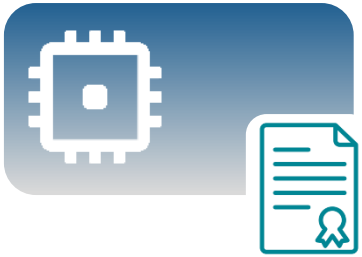
Весь процесс сводится к трем шагам



1 Найти сертифицированное СКЗИ



2 Встроить СКЗИ в ПО или ПАК



3 Провести оценку влияния

Для оценки влияния потребуется пакет материалов

Согласовывается с 8 Центром ФСБ России

- ТЗ на проведение оценки влияния
- Дистрибутивы ПО (СПО)
- Тест-план

Умная мысль

> Мало иметь библиотеку, нужно суметь правильно ее использовать

ТЕХНО infotecs 2023 ФЕСТ

Как избежать ошибок при встраивании

Как избежать ошибок при встраивании

1. Использовать «белые» функции
2. Выделять модуль для работы с криптографией
3. Использовать инструменты, с которыми вендор уже провел исследования
4. *Использовать сертифицированные ОС

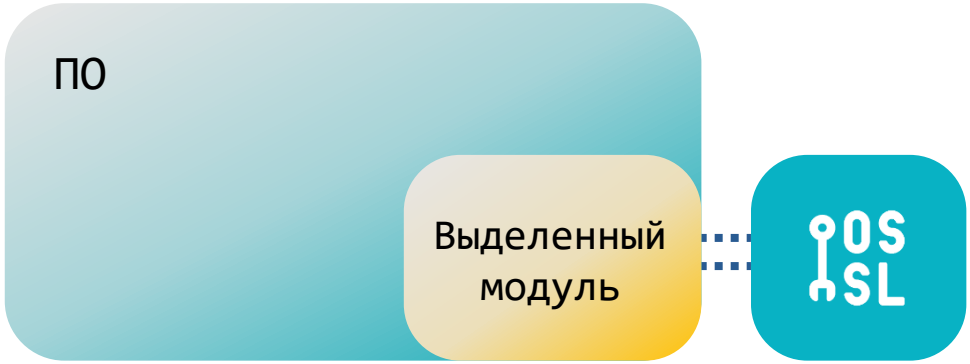
«Белые» функции –
список разрешённых команд и функций, которыми можно безопасно пользоваться из прикладного ПО

Прописаны в Правилах Пользования

Использование функций из этого списка позволяет ограничиться оценкой влияния при встраивании

Как избежать ошибок при встраивании

1. Использовать «белые» функции
2. Выделять модуль для работы с криптографией
3. Использовать инструменты, с которыми вендор уже провел исследования
4. *Использовать сертифицированные ОС



И как следствие…

Не пересобирать этот модуль без необходимости, а использовать его в бинарном виде

Как избежать ошибок при встраивании

1. Использовать «белые» функции
2. Выделять модуль для работы с криптографией
3. Использовать инструменты, с которыми вендор уже провел исследования
4. *Использовать сертифицированные ОС

Мы проводим оценку влияния популярных веб-серверов на СКЗИ

- Быстрый запуск в эксплуатацию
- Хорошая альтернатива коробочным решениям

Как избежать ошибок при встраивании

1. Использовать «белые» функции
2. Выделять модуль для работы с криптографией
3. Использовать инструменты, с которыми вендор уже провел исследования
4. Использовать сертифицированные ОС

Операционные системы:

- Astra Linux
- Альт СП
- РЕД ОС
- ROSA
- Аврора

Теперь о продуктах

Библиотеки Инфотекс

ViPNet CSP	ViPNet OSSL	ViPNet JCrypto SDK	ViPNet CryptoSmart
Платформы	Платформы	Платформы	Платформы
			
Интерфейсы	Интерфейсы	Интерфейсы	Интерфейсы
MS CryptoAPI	PKCS#11 OpenSSL	JNI/JCA PKCS#11	MSP, NetCSP BCCSP Lite
Класс защиты	Класс защиты	Класс защиты	Класс защиты
КС1-КС3	КС1-КС3	КС1	КС1, КС2
Сертификат ФСБ	Сертификат ФСБ	Сертификат ФСБ	Сертификат ФСБ
да	да	В процессе	В процессе

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
- GOM

ViPNet CSP

Криптопровайдер для граждан и разработчиков

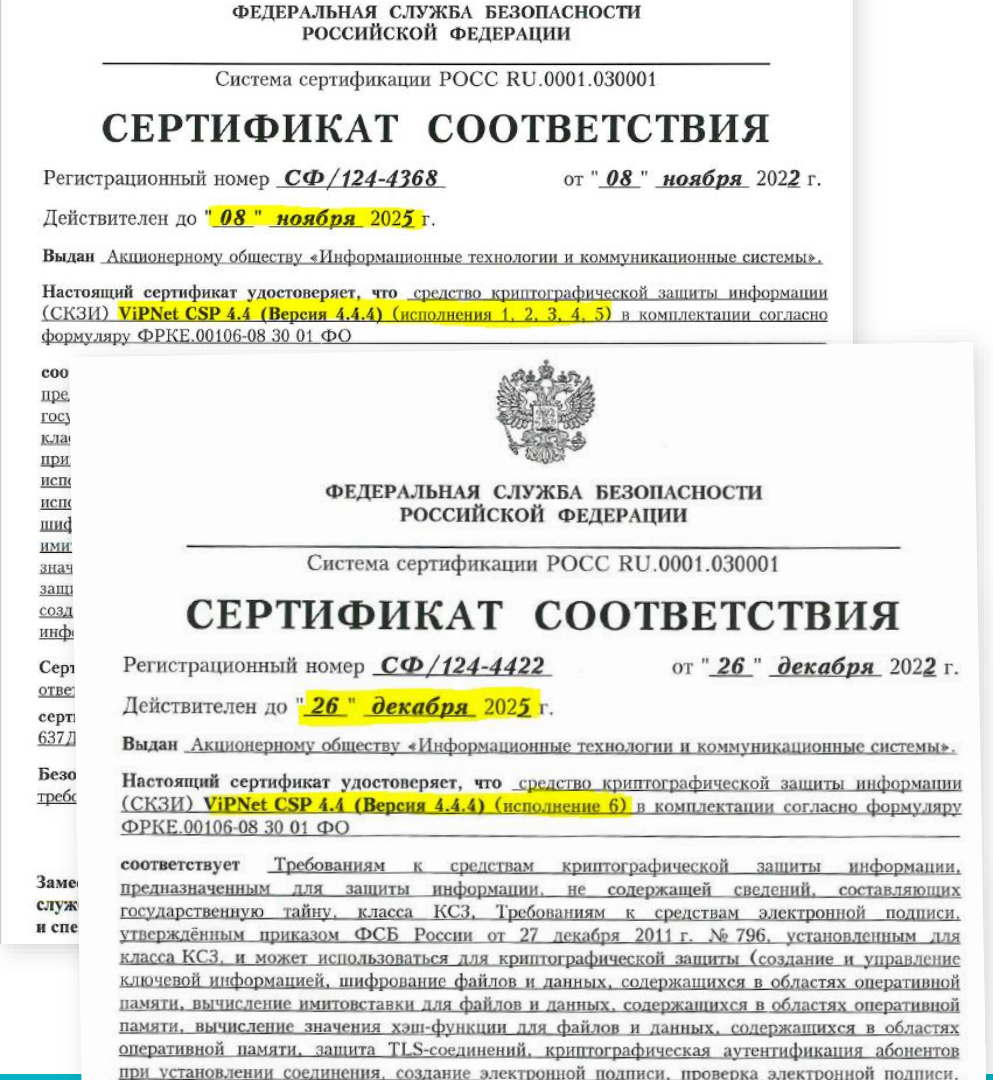
Сертификат ФСБ России: КС1, КС2, КС3

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/124-4368 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

ViPNet OSSL

Криптобиблиотека для разработки мобильных и серверных решений

Сертификат ФСБ России: КС1, КС2, КС3

Клиентское и серверное исполнение

Поддержка мобильных ОС

Особенности

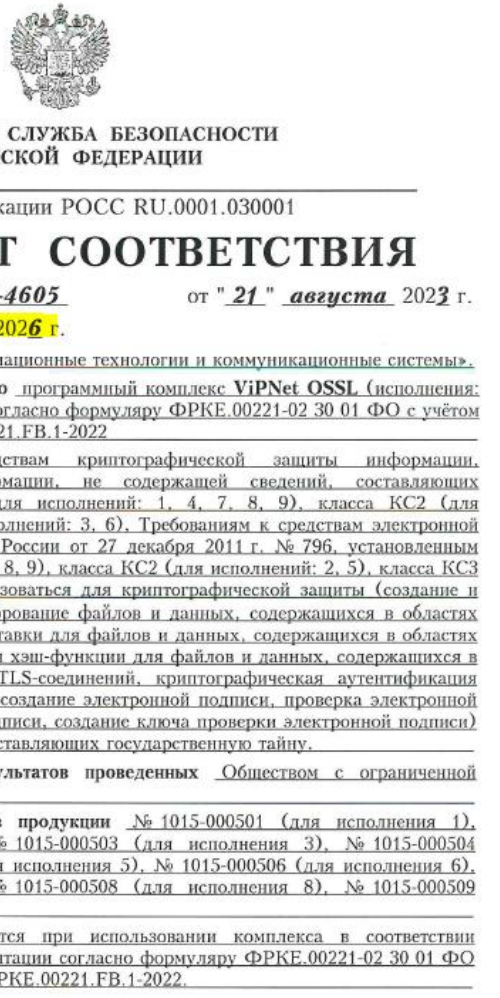
- Стандартные интерфейсы OpenSSL и PKCS#11
- Поддержка различных форматов подписи
- Актуальные алгоритмы и протоколы
- Содержит программный токен
- Совместим с токенами и смарт-картами
- Возможность экспортировать ключи с других машин и криптопровайдеров

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



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 2023 infotecs ФЕСТ

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

До 21 августа 2026 года

ViPNet JCrypto SDK

Криптобиблиотека для разработки на Java-машинах

В процессе сертификации

Криптоядро ViPNet OSSL

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

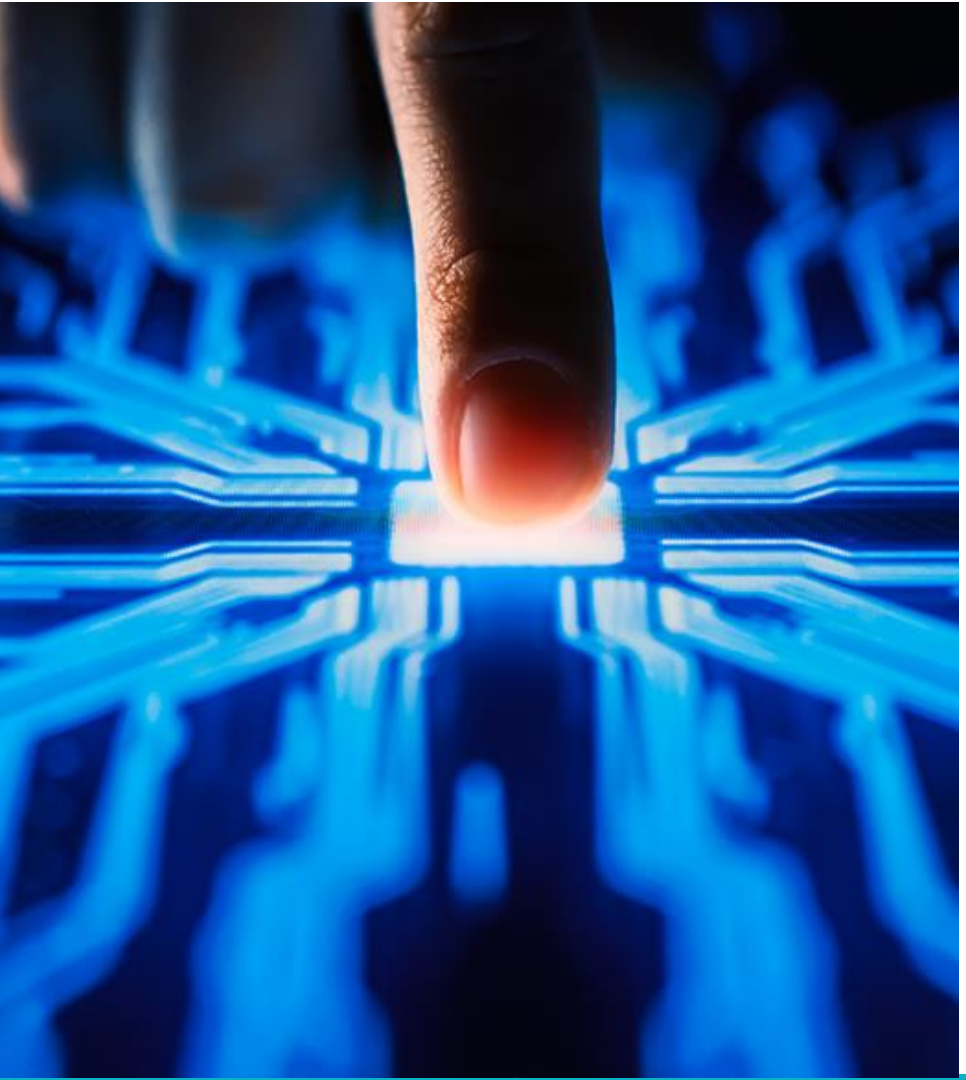
В процессе сертификации

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



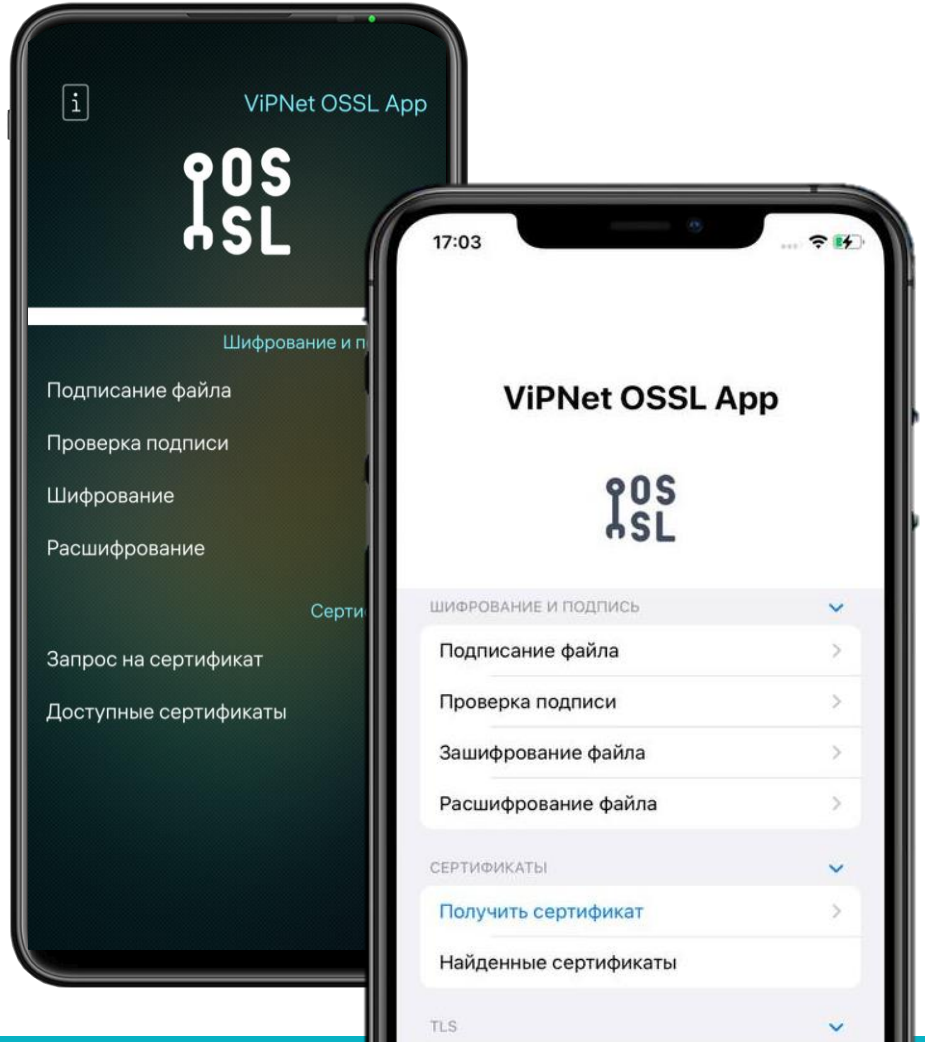
ТЕХНО 2023 infotecs ФЕСТ

Жду вас на мастер-классе!

Где
Красный поток

Когда
11:46

Мастер-класс
Прикладная криптография наглядно



Приходите на стенд!

В зону **Crypto & PKI**

Посмотреть на возможную **реализацию встраивания криптобиблиотек** в пользовательские приложения

ТЕХНО 2023 infotecs ФЕСТ

Задавайте вопросы в приложении!

Подписывайтесь на наши соцсети

vk.com/infotecs_news

https://t.me/infotecs_official

rutube.ru/channel/24686363