

Криптография для прикладных систем

Арина Эм
Ведущий менеджер продуктов



Криптография в прикладных системах



Офисные
приложения



Документооборот



Логистика



Мобильные
приложения



Шифрование данных
в облаке



Здравоохранение



Банкинг



Мессенджеры



Интернет
вещей

Продукты

Криптобиблиотеки ИнфоТеКС



ViPNet OSSL

Для разработки мобильных
и серверных решений



ViPNet CSP

Для разработки ПО
под Windows



ViPNet JCrypto SDK

Для разработки ПО на Java



ViPNet CryptoSmart

Для тех, кому нужен ГОСТ
в блокчейне

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



Форматы

CMS	CAdES
PFX	XAdES
XMLDsig	X.509



Протоколы

TLS 1.2	TSP
TLS 1.3	OCSP



Работа с ключами на токенах

ViPNet HSM
Rutoken
JaCarta



Интерфейсы

CryptoAPI	Java SDK
OpenSSL	GO



Поддержка ОС





Криптопровайдер
для граждан
и разработчиков



Сертификат ФСБ
России:
KC1, KC2, KC3



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, утвержденным 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.

VipNet CSP 4.4.8 сертифицирован ФСБ России по классам КС1, КС2, КС3

До 28 декабря 2026 года





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

VIPNet OSSL: лицензирование

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/124-5052

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 OSSSL (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 № 4 ФРКЕ.00221.FB.4-2024

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 № 4 ФРКЕ.00221.FB.4-2024.

ViPNet OSSSL 5.4 сертифицирован ФСБ России

по классам КС1, КС2, КС3

До 10 ноября 2027 года



VipNet JCrypto SDK



Криптобиблиотека
для разработки
на Java-машинах



Сертификат ФСБ
России:
KC1, KC2, KC3



Криптоядро
VipNet OSSL



Поддержка
мобильных ОС

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



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 iCrypto 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, утвержденным 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. Скрыбин

ViPNet iCrypto SDK сертифицирован ФСБ России

по классу КС1

До 10.11.2027



ViPNet CryptoSmart



**Криптобиблиотека
для реализации ГОСТ
в блокчейне**



В процессе
сертификации



Криптоядро
ViPNet OSSL

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

KC1-KC3

Сертификат ФСБ
да

ViPNet OSSL

Платформы



Интерфейсы

PKCS#11
OpenSSL

Класс защиты

KC1-KC3

Сертификат ФСБ
да

ViPNet JCrypto SDK

Платформы



Интерфейсы

JNI/JCA
PKCS#11

Класс защиты

KC1

Сертификат ФСБ
да

ViPNet CryptoSmart

Платформы



Интерфейсы

MSP, NetCSP
BCCSP Lite

Класс защиты

KC1, KC2

Сертификат ФСБ
да



Особенности встраивания

Что нужно для старта работ?



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



Криптографический модуль



ViPNet OSSSL



ViPNet
JCrypto SDK

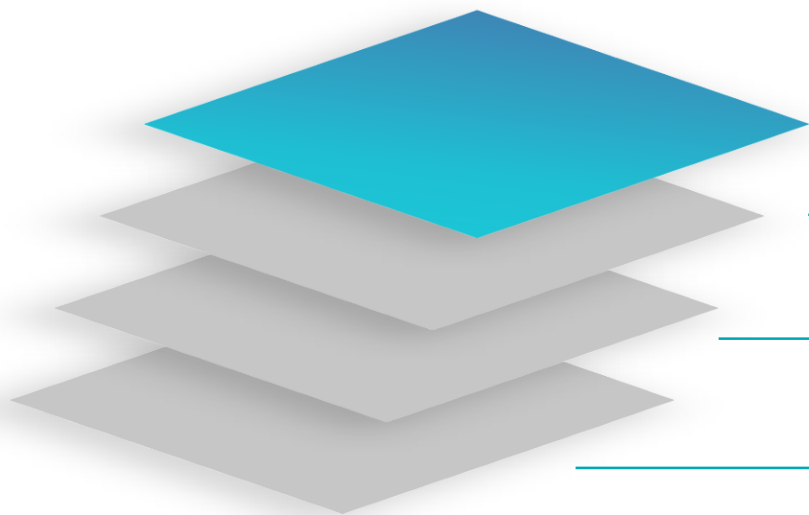


ViPNet CSP



ViPNet
CryptoSmarT

Переходим к встраиванию



4 уровень

Прикладное ПО

3 уровень

Крипто форматы и протоколы

2 уровень

Стандартный интерфейс PKCS#11

1 уровень

Криптопримитивы



Важно!



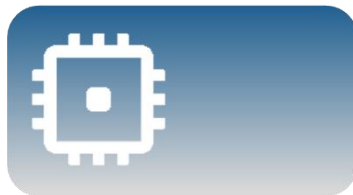
Встроили –
пройдите оценку влияния



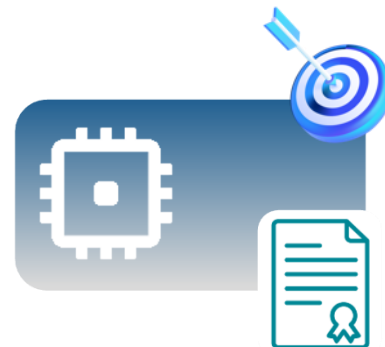
Весь процесс сводится к трем шагам



1 Найти
сертифицированное
СКЗИ



2 Встроить СКЗИ в
ПО или ПАК



3 Провести **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

Как мы можем помочь

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

Как это выглядит на практике

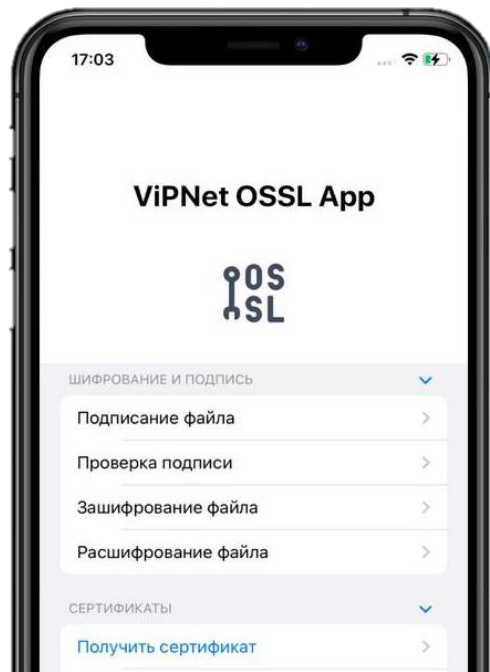
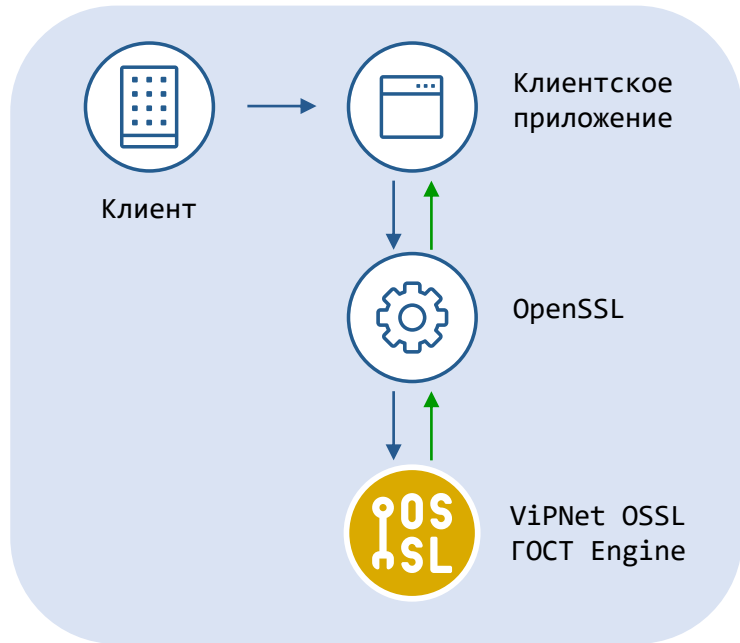
Мы написали приложение со своей криптографией

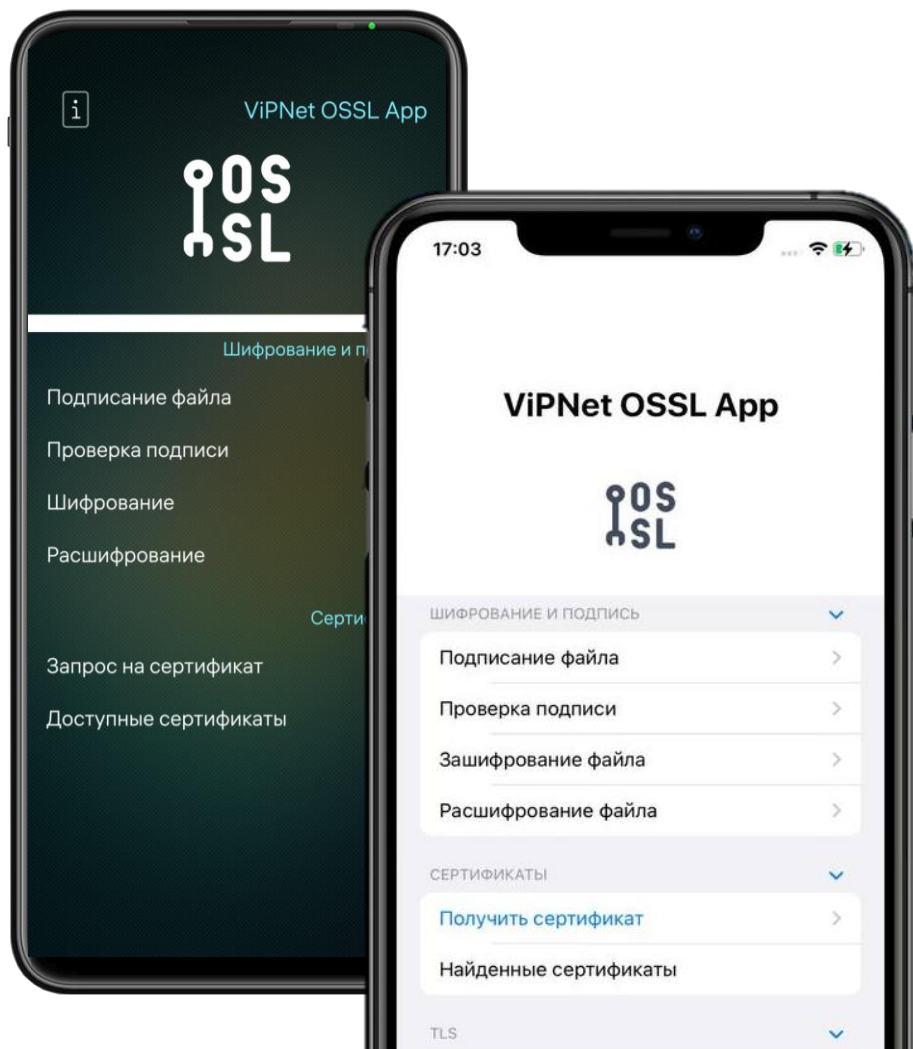
- Пример интеграции криптобиблиотеки
- Демонстрация пользовательского сценария

Демо-приложение с ViPNet OSSL

С точки зрения разработчика

С точки зрения пользователя





Приходите на стенд!

Вживую посмотреть на возможную
реализацию встраивания
криптобиблиотек
в пользовательские приложения
на мобильных ОС



Подытожим

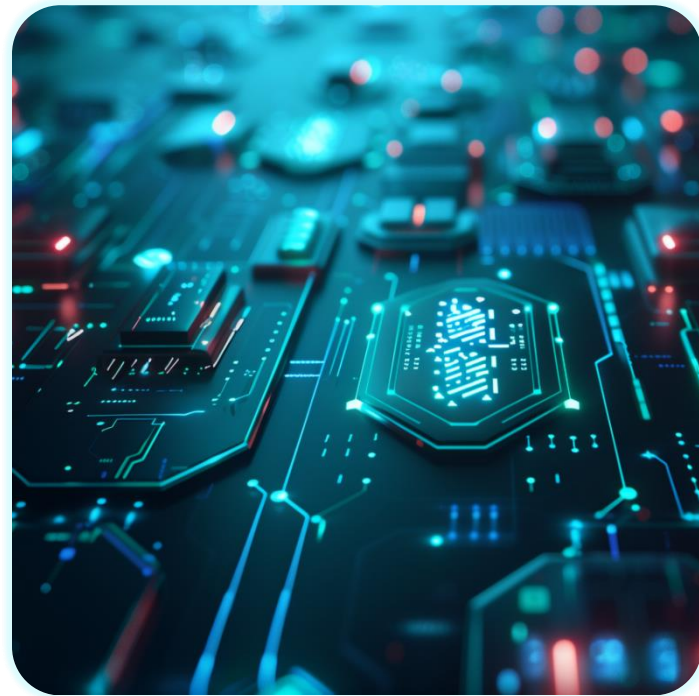
Криптобиблиотеки удобны



Для встраивания
в различные типы приложений



Для использования криптофункций
без необходимости понимания
математических деталей их работы



Подытожим

Криптобиблиотеки ИнфоТеКС – это



Разработка ПО на спектре языков разработки



Подробная документация с примерами



Реализация криптографических функций и интерфейсов согласно стандартам



Как с нами связаться

Купить или взять на тесты:

soft@infotecs.ru



Есть идея реализации совместного решения:

techpartners@infotecs.ru



Или пишите мне!





Телеграм-канал
Криптография

@cryptografinya



ТЕХНО infotecs Фест

Арина Эм
Ведущий менеджер продуктов

Подписывайтесь
на наши соцсети,
там много интересного

