ViPNet OSSL: что нового

Арина Эм
Менеджер продукта

infotecs

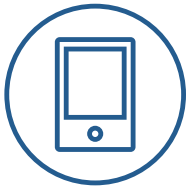
Вспоминаем, что такое ViPNet OSSL

Библиотека для встраивания

ViPNet OSSL - библиотека для встраивания на базе OpenSSL, используется для разработки приложений и сервисов

Для серверов

Для десктопов



Для мобильных и планшетов

Нужна для реализации криптографических функций

- Создание ключей ЭП
- Создание ключей проверки ЭП
- Формирование ЭП
- Проверка ЭП
  - ГОСТ Р 34.10-2012
- Хеширование данных
  - ГОСТ Р 34.11-2012
- Шифрование данных
  - ГОСТ Р 34.12-2015
  - ГОСТ Р 34.13-2015

- Организация TLS-соединений
- Работа с ключами на внешних устройствах
- Аутентификация и выработка сессионного ключа при передаче данных по протоколу TLS
- Формирование CMS сообщений
- Формирование PFX - транспортных контейнеров ключей
- Формирование запроса на сертификат (PKCS#10)

Отвечает потребностям прикладных систем

Защита персональных данных

Передача данных по защищенному каналу

Работа с электронной подписью

Соответствие требованиям регуляторов

Шифрование данных

Форматы усовершенствованной подписи

infotecs

CAdES

- CAdES-BES
- CAdES-T
- CAdES-C
- CAdES-X
- CAdES-XL
- CAdES-XLT1
- CAdES-XLT2
- CAdES-XT1
- CAdES-XT2

XAdES

- XAdES-BES
- XAdES-T
- XAdES-C
- XAdES-XLT1
- XAdES-XLT2
- XAdES-XT1
- XAdES-XT2
- XAdES-A

Важные особенности

- Стандартные интерфейсы OpenSSL и PKCS#11
- Содержит программный токен
- Совместим с токенами и смарт-картами
- Возможность развертывания на серверной и клиентской стороне

ViPNet OSSL для клиентов

Ключевые преимущества

- Интеграция в приложения для десктопных и мобильных ОС
- Реализация функций подписи и шифрования на клиентских устройствах
- Распространение через магазины приложений

Лицензирование для клиентов

Десктоп

1 лицензия – 1 устройство

Мобильные

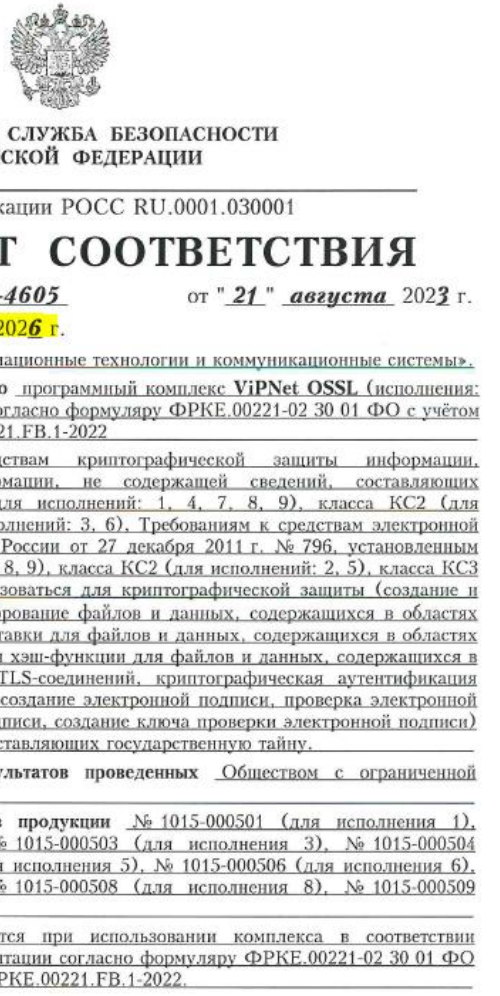
1 лицензия – 100 устройств

ViPNet OSSL для серверов

- Интерфейс OpenSSL используется популярными веб-серверами
- Обеспечивает гибкость в выборе места установки
- Обеспечивает распараллеливание процессов
- Не нужна оценка влияния

Лицензирование для серверов

1 лицензия –
1 устройство



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.

infotecs

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

До 21 августа 2026 года

Что нового в версии ViPNet OSSL 5.6

Актуализировали версии

- OpenSSL 1.1.1w
- Без оценки влияния обеспечивается работа с

  nginx 1.22, 1.24 | apache 2.4.58 | stunnel 5.71

- Расширили список поддерживаемых сред виртуализации
  - «Брест»
  - «РЕД Виртуализация»
- Актуализировали список поддерживаемых токенов
- Актуализировали версии поддерживаемых ОС

Архитектуры и операционные системы

Архитектуры

- x86
- x86-64
- ARM
- Байкал-М

Linux

CentOS
Debian
Red Hat Enterprise Linux
Ubuntu
Ubuntu Server
SUSE Linux Enterprise Server
Альт СП, 9, 10
AlterOS
РЕД ОС
РОСА «КОБАЛЬТ»
Astra Linux (SE, CE)
ROSA Enterprise Linux Server
Лотос
СинтезМ-Клиент
EMIAS OS

Windows

Windows 10, 11
Windows Server 2016, 2019, 2022

Мобильные ОС

Аврора 4
Android 8-13
iOS 11-16
iPadOS 14, 15, 16

macOS

macOS 10.15, 11, 12, 13

Поддерживаемые устройства

ViPNet HSM

Рутокен ЭЦП 2.0 Touch
Рутокен Lite
Рутокен ЭЦП 2.0, 2.0 Flash
Рутокен ЭЦП 2.0 3000
Рутокен ЭЦП PKI
Рутокен ЭЦП 2.0 2100
Рутокен ЭЦП 3.0 NFC
Рутокен ЭЦП 3.0 3220
Рутокен VCR 3001 NFC

JaCarta LT
JaCarta PRO
JaCarta-2 SE
JaCarta-2 SF
JaCarta SF/ГОСТ
JaCarta-2 SE/PKI/ГОСТ
JaCarta-2 PKI/BIO/ГОСТ
JaCarta PKI/BIO
JaCarta PKI
JaCarta-2 ГОСТ
JaCarta-2 PRO/ГОСТ

ESMART Token ГОСТ
ESMART Token
ESMART Token 192k

Новые возможности

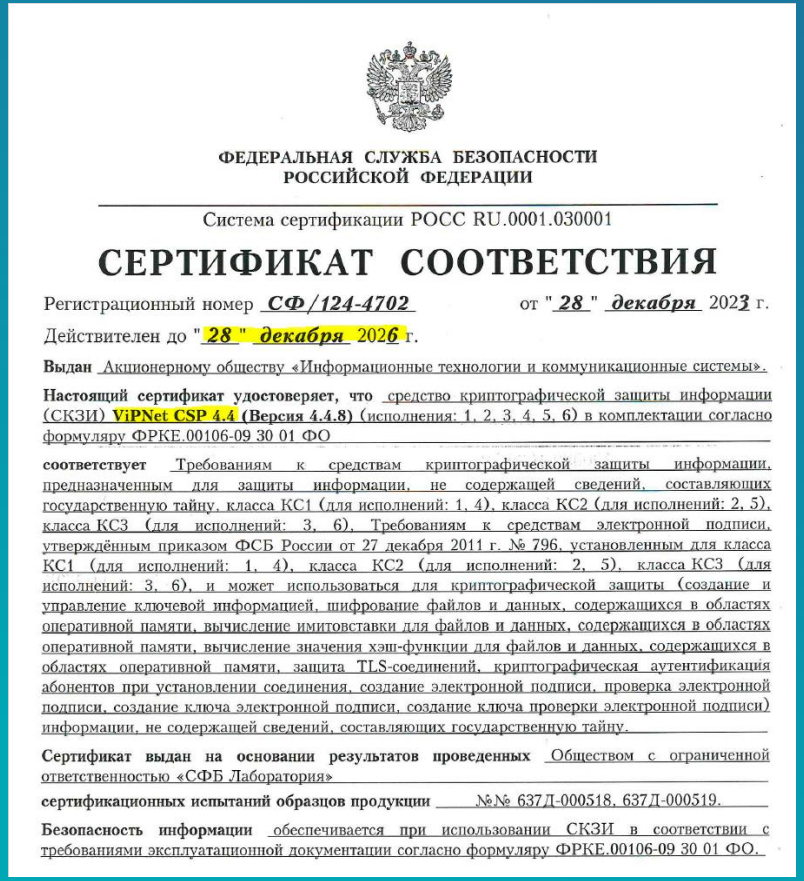
- Шифрование PFX на алгоритмах ГОСТ 34.12-2018 ("Магма" и "Кузнечик")
- Поддержка ACME на зарубежных алгоритмах
- Подключение к Рутокен через виртуальный NFC для iPad
- Облегченная настройка TLS за счет добавления дополнительных конфигурационных файлов для поддержки западных и отечественных алгоритмов в протоколе TLS 1.3
- Регистрация для Linux, Windows и macOS с помощью контрольных команд движка
- Определение расположения закрытого ключа по сертификату
- Работа с контейнерами ключей формата ViPNet CSP 4.4
- Одноэтапная регистрация для мобильных ОС

Новые возможности

- Разработали утилиту для десктопных исполнений ossl_admin. Она объединяет функциональность, которая требуется в сертифицированных исполнениях
  - лицензирования/регистрации ПО
  - контроля целостности
  - версионирования ПО
  - безопасной очистки файлов (wiper)
- Быстрый старт для исполнений под Apple

Если вы используете ViPNet CSP

Пора задуматься о будущем :)



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.

Сертификат на ViPNet CSP 4.4 заканчивается в 2026 году и не будет продлеваться

Мы готовим ViPNet CSP 5, но он будет только под Windows

Если используете ViPNet CSP Linux – пора переходить на новый инструмент ViPNet OSSL✨

Подробная документация и примеры кода

Руководство администратора

Информация об установке и настройке для работы со сторонним ПО

Справочник функций

Описание функций и их параметров

Инструкция по переходу с CSP на OSSL

Руководство разработчика

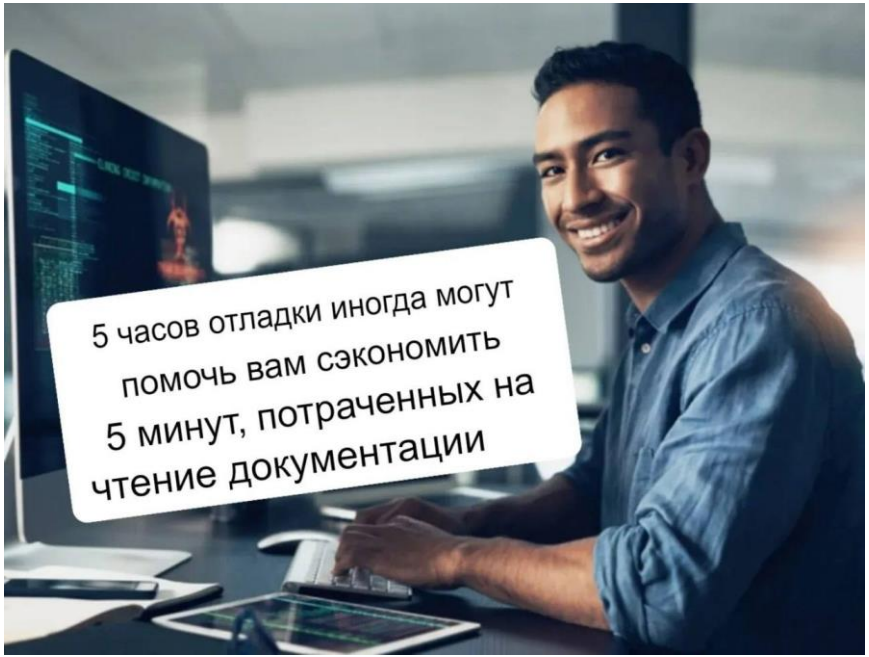
Сведения о разработке с помощью библиотек

Примеры

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

Быстрые старты

Народная мудрость



Как с нами связаться

Купить или взять на тесты:
soft@infotecs.ru

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

Полезные материалы

Вебинары	Как разрабатывать ПО с криптографией внутри Всё, что вам нужно знать об оценке влияния при встраивании СКЗИ
Брошюра	ViPNet Crypto

Мероприятия

infotecs

Вебинар

Что нужно знать при использовании СКЗИ
5 сентября 2024 года
Регистрация

Конференция

Технофест в Иркутске
9 октября 2024 года
Регистрация: https://infotecstechfest.ru/

Легкого встраивания!

Арина Эм

Arina.Em@infotecs.ru

Подписывайтесь на наши соцсети

vk.com/infotecs_news

https://t.me/infotecs_official

rutube.ru/channel/24686363