VIPNet OSSL 5.4: новости, сертификат

Арина Эм

infotecs

План на сегодня

1. ViPNet OSSL 5.4: о продукте
2. Что нового в версии ViPNet OSSL 5.4
3. Где и как использовать ViPNet OSSL
4. Важное о сертификации
5. Полезные материалы
6. Розыгрыш

ViPNet OSSL 5.4: о продукте

ViPNet OSSL

Библиотека **для встраивания** на базе OpenSSL, используется для разработки приложений и сервисов

Это продукт для разработчиков прикладного ПО

Для серверов

Для десктопов

Для мобильных и планшетов

ViPNet OSSL

Особенности

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

Сертификат ФСБ России:
КС1, КС2, КС3

Клиентское и
серверное исполнение

Поддержка
мобильных ОС

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

- OpenSSL
- PKCS#11

Архитектуры и операционные системы

Архитектуры

- x86
- x86-64
- ARM
  - Android
  - Байкал-М
  - Аврора
  - macOS, iOS
- Эльбрус
- M1

Linux

CentOS
Debian
Red Hat Enterprise Linux
Ubuntu, Ubuntu Server
SUSE Linux Enterprise Server
Альт СП, 9, 10
ГосЛинукс ИК6
AlterOS
РЕД ОС
РОСА «КОБАЛЬТ»
Astra Linux (SE, CE)
ROSA Enterprise Linux Server
Лотос
Атлант ОС
Аврора

Windows

Windows 8.1, 10, 11
Windows Server 2008 R2, 2012, 2012 R2, 2016, 2019, 2022

Мобильные ОС

Android 5.x – 12.x.
iOS 11.x – 15.x.
iPadOS 14, 15

macOS

macOS 10.13, 10.14, 10.15, macOS 11, macOS 12

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

ViPNet OSSL для клиентов

- Возможность интеграции в приложения для десктопных и мобильных ОС
- Возможность обеспечить функции подписи и шифрования на клиентских устройствах
- Возможность распространения через магазины приложений

Лицензирование для клиентов

Десктоп

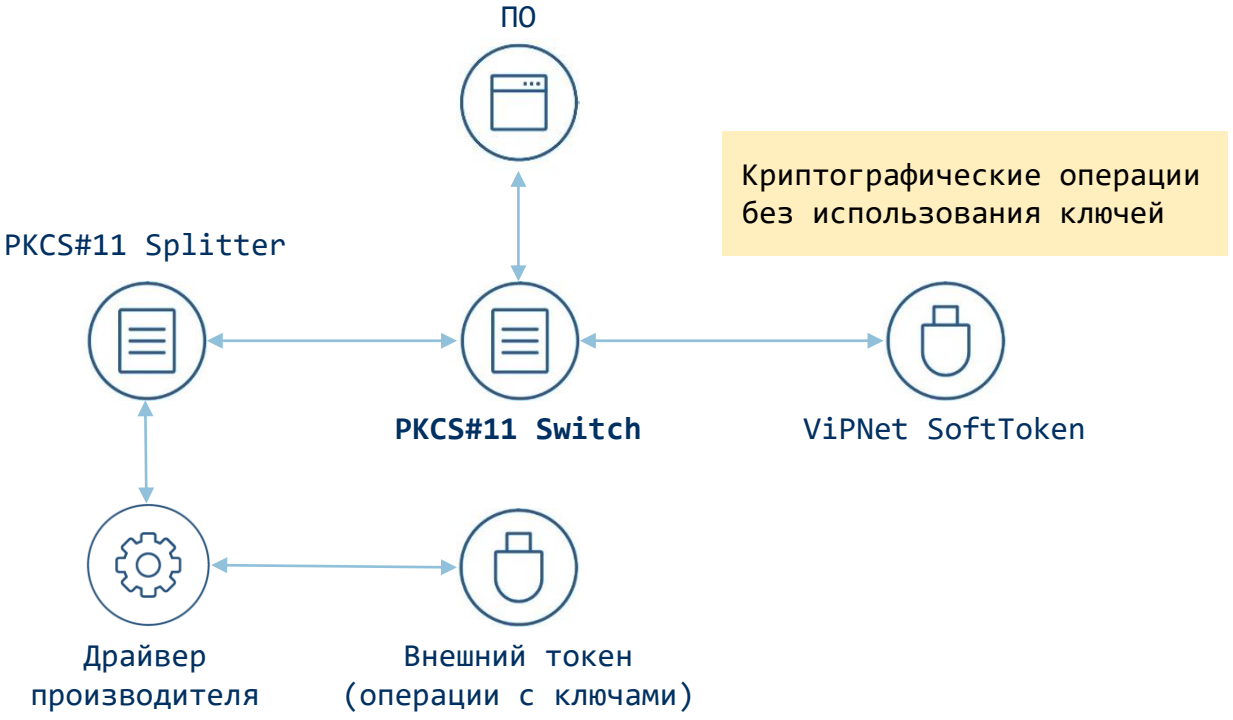
1 лицензия – 1 устройство

Мобильные

1 лицензия – 100 устройств

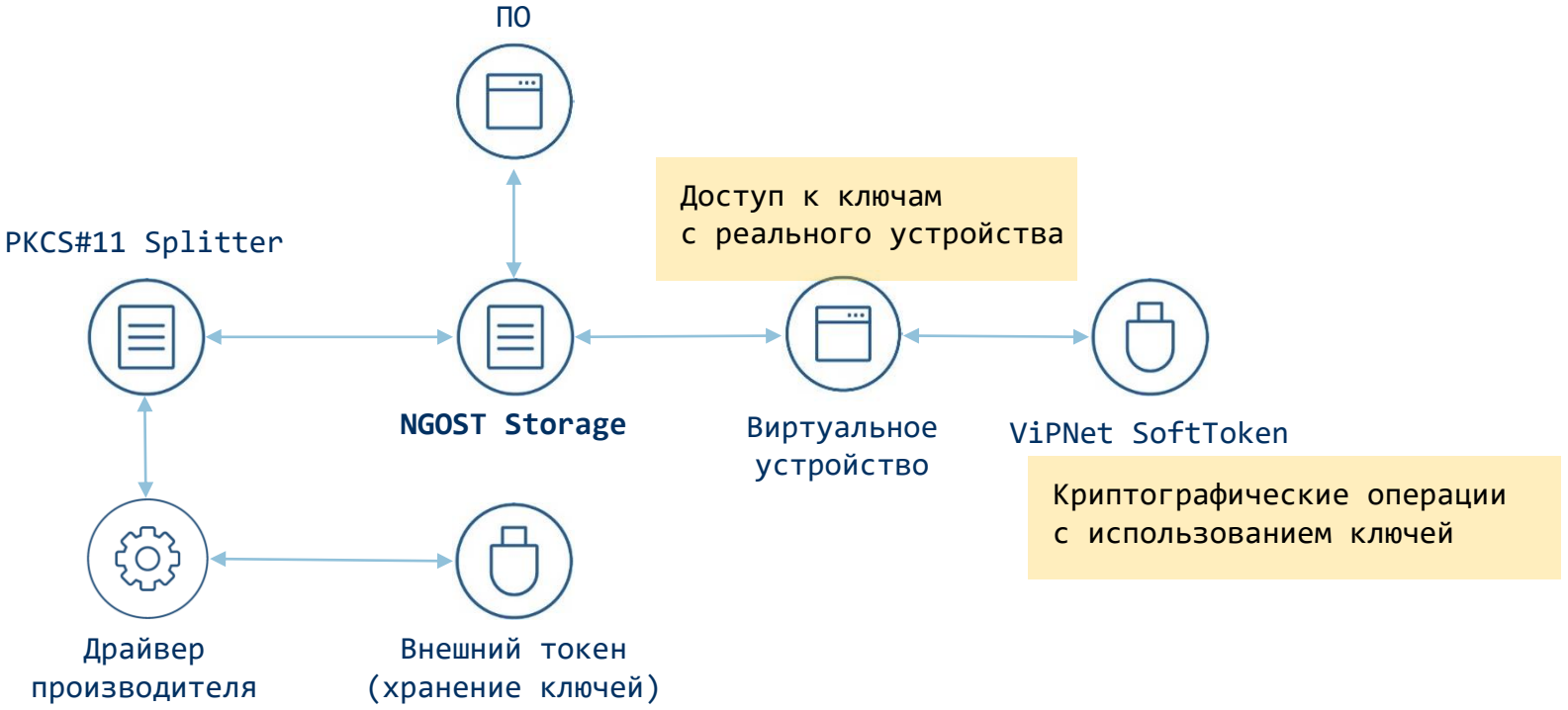
Работа с токенами

Токен поддерживает криптооперации



Работа с токенами

Токен в роли хранилища ключей



Сертификация ФСБ России

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

Новое в версии ViPNet OSSL 5.4

Что нового: совместимость

- Поддержали новые ОС
- Обеспечили работу токенов в мобильных исполнениях
- Поддержали Байкал-М
- Поддержали KVM
- Поддержали macOS под ARM
- Обновили компонент OpenSSL до 1.1.1t
- Добавили поддержку новых моделей внешних устройств (токенов, смарт-карт, Bluetooth-устройств)

Поддерживаемые устройства

ViPNet HSM

Рутокен ЭЦП 2.0 Touch
Рутокен ЭЦП Bluetooth
Рутокен Lite
Рутокен ЭЦП 2.0, 2.0 Flash
Рутокен ЭЦП 2.0 3000
Рутокен ЭЦП PKI
Рутокен ЭЦП 2.0 2100
Рутокен 2151
Рутокен ЭЦП 3.0 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

Что нового

- Реализовали хранилище сертификатов
- Корневые сертификаты ГУЦ автоматически сохраняются в общее хранилище сертификатов при установке приложения
- Улучшили и дополнили документацию
- Доработали датчик случайных чисел ViPNet UPRNG
- Улучшили комплект поставки для Apple: теперь поставляется в виде DMG-дистрибутива для автоматизированной установки самого продукта и SDK для разработчика
- Улучшили контроль целостности среды функционирования
- Добавили примеры кода, реализующие базовые функции продукта

А также

Проводим оценку влияния NGINX, Apache, Stunnel
на ViPNet OSSL 5.4, чтобы нашим заказчикам
не нужно было проходить ее самостоятельно

Где и как использовать ViPNet OSSL?

Частые сценарии использования

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

Есть дистрибутив – что дальше?

Шаг 1: Регистрация движка

Шаг 2: Подключение и инициализация движка

Шаг 3: Конфигурация интерфейса PKCS#11

Шаг 4: Инициализация хранилища ключевой информации

Шаг 5: Реализация бизнес-логики работы с ключами и данными

Что понадобится для разработки

- пакеты ViPNet OSSL для разработчика
- g++ (GNU C++)
- утилита make
- CMake ДЛЯ СБОРКИ ПРИМЕРОВ
- библиотеки C++ Boost ДЛЯ СБОРКИ ПРИМЕРОВ

Важно: встроили – пройдите оценку влияния

Особенность встраивания СКЗИ

infotecs

1 ViPNet OSSL – это СКЗИ

У НАС ЕСТЬ

- Сертификат ФСБ
- Выделенное множество функций

2 Нужно одобрение регулятора

Оценка влияния

или

Полноценная сертификация

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

Полезные материалы

Программные встраиваемые СКЗИ

ViPNet JCrypto SDK

Для разработки ПО на Java

Интерфейсы JNI/JCA, PKCS#11
Класс защиты КС1
Сертификат ФСБ В процессе

ViPNet CSP

Для разработки ПО под Windows

Интерфейсы MS CryptoAPI
Класс защиты КС1, КС2, КС3
Сертификат ФСБ Да

ViPNet CryptoSmart

Для тех, кому нужен ГОСТ в блокчейне

Интерфейсы OSSL, PKCS#11
Класс защиты КС1, КС2
Сертификат ФСБ В процессе

Полезные материалы

Вебинары

Вебинар ViPNet OSSL v.1

Вебинар ViPNet OSSL v.2

Мастер-класс: Настройка TLS с помощью ViPNet OSSL

Про оценку влияния при встраивании СКЗИ

Статья

Шпаргалка по криптографии: что делать, если попал в проект с криптографами

Как с нами связаться

Купить или взять на тесты:
soft@infotecs.ru

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

Или пишите мне!

infotecs

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