

ViPNet CSP: **НОВОСТИ И ПЛАНЫ**

Арина Эм
Менеджер продукта



Что мы знаем о ViPNet CSP

Что мы знаем о ViPNet CSP



Криптопровайдер
для граждан и
разработчиков



Сертификат ФСБ России:
КС1, КС2, КС3



Упрощенная интеграция
на Windows



Бесплатно под Windows

Нужен 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

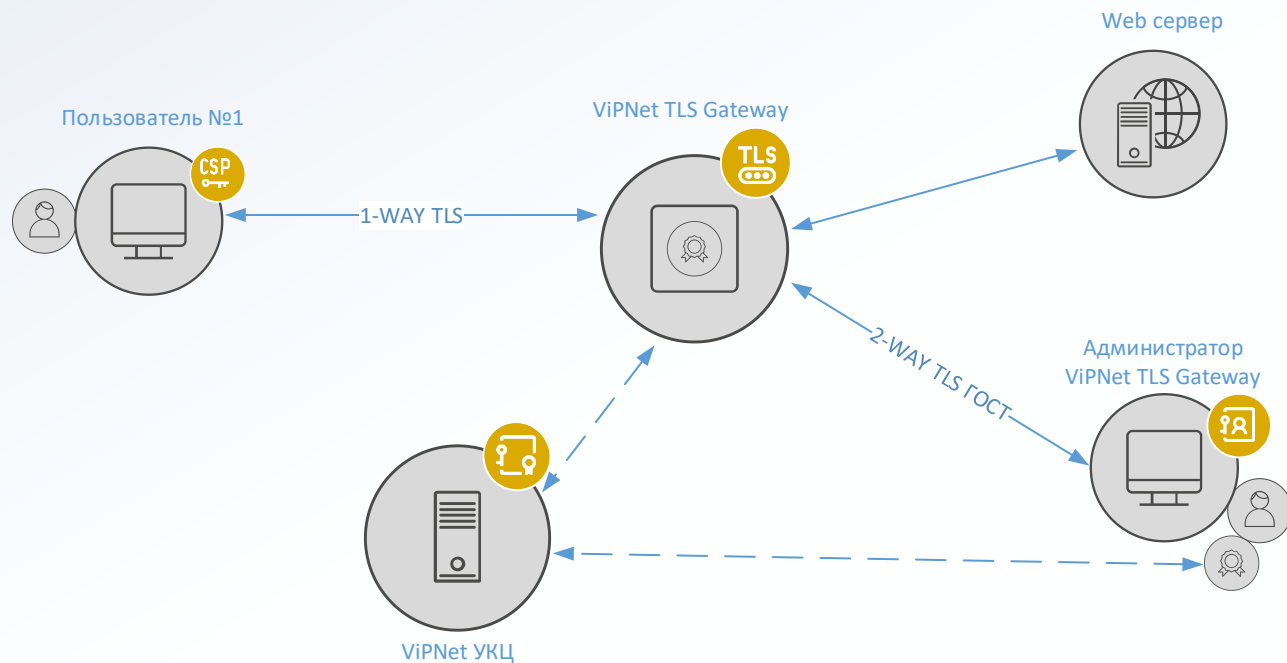


Схема удаленных защищенных подключений

Задачи:

- Подтверждение подлинности сервера
- Защита передаваемых данных
- Защита соединений
- Аутентификация клиентов

Поддерживаем токены

ViPNet HSM

Рутокен ЭЦП 2.0 Flash

Рутокен ЭЦП 2.0 Touch

Рутокен ЭЦП 2.0

Рутокен ЭЦП 2.0 3000

Рутокен Lite

Рутокен ЭЦП 3.0 3220

Рутокен ЭЦП PKI (2.0)

Рутокен ЭЦП 2.0 2100

Рутокен 2151

Рутокен ЭЦП 3.0 (NFC) 3100

R301 Форос

ESMART Token

ESMART Token ГОСТ

JaCarta-2 SE

JaCarta SF/ГОСТ

JaCarta-2 SE/PKI/ГОСТ

JaCarta LT

JaCarta-2 SF

JaCarta-2 ГОСТ

JaCarta PRO

JaCarta-2 PRO/ГОСТ

JaCarta PKI/ГОСТ

JaCarta-2 PKI/ГОСТ

JaCarta-2 PKI/BIO/ГОСТ

JaCarta PKI/BIO

JaCarta PKI

Gemalto

Поддержка операционных систем



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



Astra Linux
Альт 8 СП
Альт
РЕД ОС
ROSA Enterprise Linux
РОСА «КОБАЛЬТ»
ЛотОС
AlterOS
Атлант ОС
CentOS
Debian 10, 11
Red Hat Enterprise
Ubuntu
Ubuntu Server

Что нового в ViPNet CSP 4.4.8

Добавили отображение срока действия ключей

Поддержка внешних устройств

Рутокен ЭЦП 2.0 3000

Рутокен ЭЦП 3.0 3220

Рутокен ЭЦП 3.0 3100

Поддержка новых драйверов для внешних устройств

Поддержка новых версий Windows

Новая иконка





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



Пользовательские сценарии



Организация защищенного
TLS-соединения



Работа с токенами



Работа с плагинами



Работа с приложениями
(Windows)



Работа с системами ЭДО



Создание запроса на сертификат

Поддержка вызовов криптографических функций

Интерфейсы для Windows

- Microsoft CSP
- Microsoft CNG
- Microsoft CryptoAPI
- CAPICOM
- Certificate Enrollment API

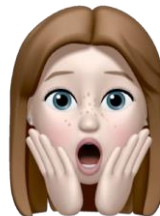
Интерфейсы для Linux

- ViPNet CryptoAPI for Linux

Планы

Новости №1

Мы не будем продлевать сертификат
на ViPNet CSP 4.4



Новости №2

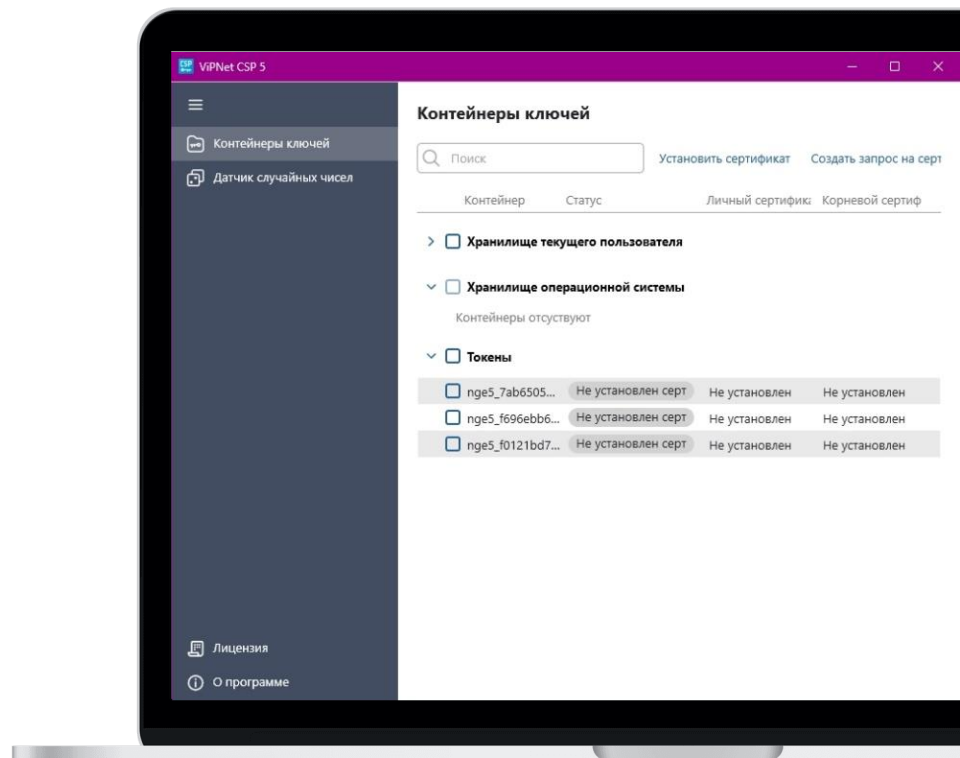
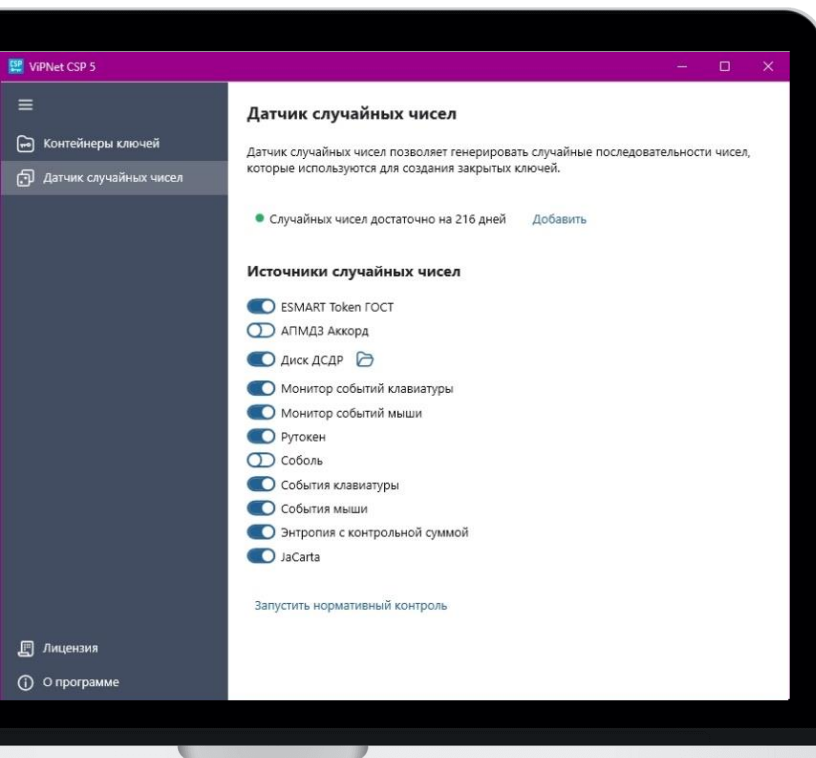
Нас ждет новый красивый современный
ViPNet CSP 5



Что изменится в VipNet CSP 5

- Новый GUI
- Новый интерфейс MS CNG взамен устаревшего MS CryptoAPI
- Переработана архитектура
- Новый принцип лицензирования
- Поддержана только ОС Windows

Новый интерфейс ViPNet CSP 5



Почему только под Windows?

Всему виной те самые интерфейсы Microsoft.
Они очень удобны для работы и разработки на Windows:

- предназначены для разработчиков приложений на основе Windows
- Позволяют интегрироваться с приложениями Microsoft, встроиться в механизмы ОС

И они совершенно неудобны для Linux

**А если мне нужно
решение под Linux?**

Чем заменить ViPNet CSP

Разработчик



ViPNet OSSSL

Пользователь



ViPNet PKI
Client

VIPNet OSSL

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

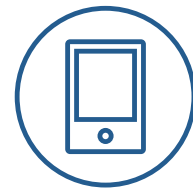
Это продукт для разработчиков прикладного ПО



Для серверов



Для десктопов



Для мобильных и планшетов



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

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

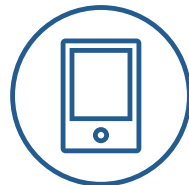
Лицензирование для клиентов

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



Десктоп

1 лицензия –
1 устройство

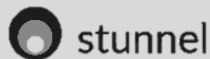


Мобильные

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

infotecs

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.

VipNet OSSL 5.4

сертифицирован

ФСБ России по

классам КС1,

КС2, КС3

До 21 августа 2026 года



VIPNet PKI Client

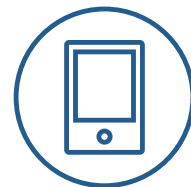
Универсальный клиент для работы
в инфраструктуре открытых ключей

Предназначен для работы с сервисами, использующими:

- заверение документов электронной подписью
- шифрование файлов
- аутентификацию пользователей для доступа к веб-сервисам; построение защищенных TLS-соединений



Для десктопов



Для мобильных

Это продукт для конечных пользователей

VipNet PKI Client

File Unit

модуль защиты
файлов

TLS Unit

модуль организации
TLS-соединений

Web Unit

модуль защиты данных,
передаваемых
браузерами

Cloud Unit

модуль
взаимодействия с
сервисом VipNet PKI
Service

Certificate Unit

менеджер сертификатов

CRL Unit

модуль обновления CRL



VIPNet PKI Client

Универсальный клиент для работы в инфраструктуре открытых ключей

- Простой и удобный
- Мультиплатформенный



Остаемся на связи!

Арина Эм

Arina.Em@infotecs.ru

Подписывайтесь на наши соцсети



vk.com/infotecs_news



https://t.me/infotecs_official



rutube.ru/channel/24686363