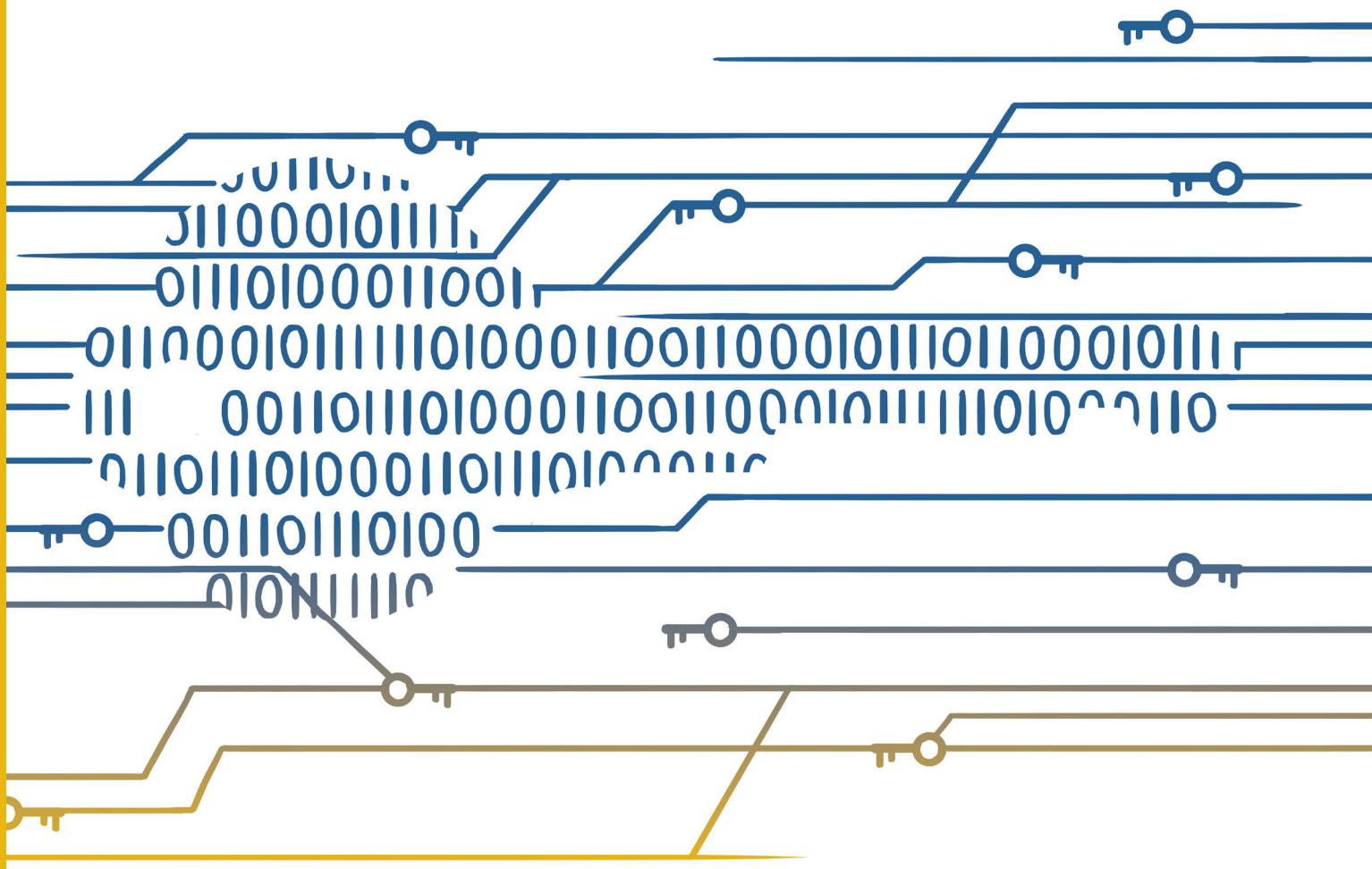
инфотекс

ViPNet PKI

Решения для работы
в инфраструктуре открытых ключей



Инфраструктура открытых ключей

Решение ViPNet PKI – это ряд продуктов, предназначенных для защиты информации и обеспечения целостности, конфиденциальности и подтверждения авторства, передаваемых данных и файлов. В состав решения входят компоненты, позволяющие как организовать пространство доверия PKI, так и подключиться к существующим инфраструктурам.

ViPNet Удосто-веряющий центр 4 (версия 4.6)

Программный комплекс, реализующий функции Удостоверяющего центра в соответствии с Федеральным законом №63-ФЗ «Об электронной подписи» от 6 апреля 2011 г.

В состав программного комплекса входят следующие компоненты:

ViPNet Administrator – базовый компонент, являющийся центром сертификации

ViPNet Registration Point / ViPNet CA Web Service предназначены для регистрации пользователей УЦ и выдачи сертификатов ключей проверки электронной подписи (ЭП)

ViPNet CA Informing – сервис информирования администраторов и пользователей УЦ о событиях, связанных с сертификатами

ViPNet TSP-OCSP Service предназначен для реализации функционала выдачи меток времени и проверки сертификатов в онлайн-режиме

ViPNet Publication Service – сервис публикации списков отозванных сертификатов (CRL) и сертификатов пользователей

ПРЕИМУЩЕСТВА

01. Возможность развертывания УЦ в организациях с территориально распределенной структурой
02. ViPNet Удостоверяющий центр 4 (версия 4.6) может использоваться аккредитованными УЦ для выпуска квалифицированных сертификатов
03. Может использоваться совместно с ПАК ViPNet HSM для хранения ключа ЭП УЦ, что позволяет повысить безопасность решения за счет применения сертифицированного СКЗИ класса КВ и средства ЭП класса КВ2

ВОЗМОЖНОСТИ

01. Регистрация пользователей УЦ
02. Издание сертификатов ключей проверки ЭП, в том числе в формате квалифицированных
03. Издание списков отозванных (аннулированных) сертификатов
04. Ведение реестров пользователей и изданных сертификатов

СЕРТИФИКАЦИЯ

ViPNet Удостоверяющий центр 4 (версия 4.6) соответствует:

> Требованиям ФСБ России к информационной безопасности УЦ класса КС2 (исполнение 1) и класса КС3 (исполнение 2)

> Требованиям к средствам УЦ, утвержденным приказом ФСБ России от 27.12.2011 №796 по классу КС2 (исполнение 1), классу КС3 (исполнение 2)

> Требованиям к форме квалифицированного сертификата ключа проверки ЭП, утвержденным приказом ФСБ России от 27.12.2011 №795

Свидетельства

В реестре российского ПО

ViPNet Удосто-веряющий центр 5

Программно-аппаратный комплекс, реализующий функции Удостоверяющего центра в соответствии с требованиями Федерального закона от 6 апреля 2011 г. №63-ФЗ «Об электронной подписи»

Состав программно-аппаратного комплекса ViPNet Удостоверяющий центр 5

ViPNet Certification Authority 5

Разработанный на базе криптографической платформы безопасности ViPNet HSM программно-аппаратный комплекс ViPNet Certification Authority 5 (ViPNet CA 5) выступает в роли центра сертификации. Этот компонент реализует все основные функции удостоверяющего центра – издание сертификатов и управление их жизненным циклом.

ViPNet PKI Client 2

ПК ViPNet PKI Client 2, входящий в комплект поставки ПАК ViPNet Удостоверяющий центр 5, предназначен для организации безопасного подключения администратора и оператора УЦ к веб-интерфейсу ViPNet CA 5 и подписи передаваемых запросов.

Администратор УЦ осуществляет настройку сервиса УЦ, а также издает и аннулирует сертификаты, создает запросы в вышестоящие УЦ и т.п. Оператор УЦ осуществляет передачу запросов на издание и аннулирование сертификатов, а также их выдачу. По запросу пользователя может сформировать ключи ЭП.

ViPNet TSP-OCSP Service 5

Сервис для реализации функционала выдачи меток времени и проверки сертификатов в онлайн-режиме. Программный комплекс работает совместно с ViPNet OSSL 5.6, для хранения ключей ЭП сервиса могут использоваться устройства из списка поддерживаемых ViPNet CSP, в т.ч. ViPNet OSSL.

ВОЗМОЖНОСТИ

> Регистрация пользователей УЦ
> Издание сертификатов ключей проверки ЭП, в том числе в формате квалифицированных
> Издание списков отозванных (аннулированных) сертификатов
> Ведение реестров пользователей и изданных сертификатов
> Импорт реестра сертификатов из ViPNet Удостоверяющий центр 4 (версия 4.6)

ПРЕИМУЩЕСТВА

01. ViPNet CA 5 является программно-аппаратным комплексом, разработанным на базе криптографической платформы ViPNet HSM под управлением ОС Linux. Использование дополнительного HSM для хранения и использования ключей ЭП УЦ не требуется

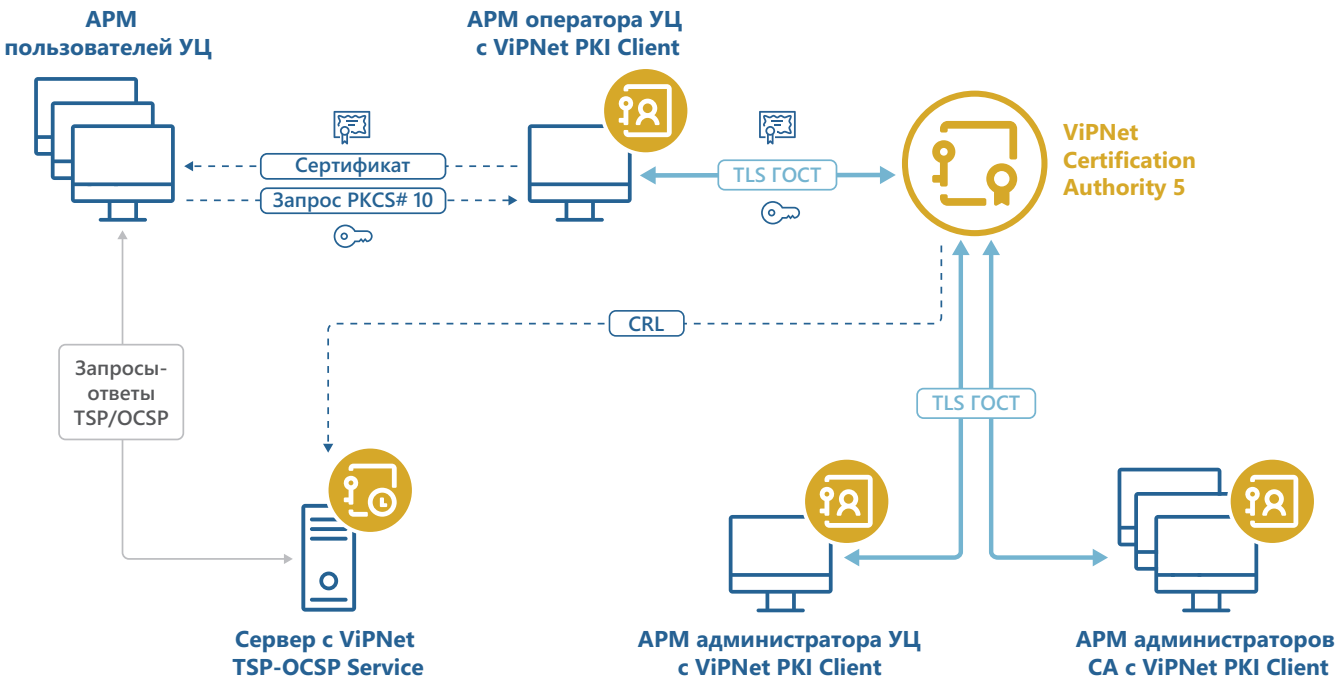
02. Защита от несанкционированного физического доступа к хранимым данным в ViPNet CA 5 с использованием встроенного в платформу датчика контроля вскрытия корпуса и изменения физических параметров платформы

03. Возможность организации рабочих мест для администраторов и операторов УЦ под управлением ОС Linux

04. Возможность одновременного использования нескольких сертификатов УЦ для выпуска пользовательских сертификатов

05. Возможность построения удостоверяющего центра любого масштаба, в том числе с территориально распределенной структурой

ViPNet Certification Authority 5



Основные отличия от ViPNet Удостоверяющий центр 4 (версия 4.6)

01. ViPNet Удостоверяющий центр 5 не связан с ViPNet-сетями и продуктами направления ViPNet VPN
02. Для хранения ключа ЭП УЦ не требуется дополнительный HSM
03. Центр сертификации ViPNet Certification Authority 5 разработан на базе криптографической платформы ViPNet HSM
04. Возможность организации рабочих мест для администраторов и операторов УЦ под управлением ОС Linux с использованием СКЗИ ViPNet PKI Client 2
05. Допускается возможность одновременного использования нескольких сертификатов УЦ для выпуска сертификатов пользователей

Рекомендованный сценарий перехода с ViPNet УЦ 4.6 на ViPNet УЦ 5:

> Выпуск новых сертификатов пользователей в ViPNet Удостоверяющий центр 4 (версия 4.6) прекращается. Осуществляется только отзыв ранее изданных сертификатов вплоть до выпуска финального списка отозванных (аннулированных) сертификатов

> Новые пользовательские сертификаты издаются и отзываются в ViPNet Удостоверяющий центр 5. Этот УЦ становится основным в рамках имеющейся инфраструктуры открытых ключей

ViPNet HSM

Универсальный криптографический модуль, платформа для разработки криптографических сервисов

ViPNet HSM – высокопроизводительная и высокозащищенная платформа, выполняющая криптооперации по запросам различных сервисов.

ViPNet HSM может располагаться в любом окружении, так как все операции выполняются во внутренней защищенной среде: ключи невозможно извлечь, данные изменить.

ViPNet HSM может использоваться в сценариях работы платежных систем, удостоверяющих центров, систем электронного документооборота, АСУ ТП.

ViPNet HSM обеспечивает поддержание полного жизненного цикла криптоключей, реализацию операций ЭП, шифрования и имитозащиты.

ПРЕИМУЩЕСТВА

01. Надежная защита от физического НСД к хранимым данным с помощью датчика контроля вскрытия корпуса и изменения физических параметров платформы (температура, питание)
02. Широкие возможности применения посредством интеграции для обработки запросов различных сторонних сервисов
03. Криптостойкий механизм выработки ключей с использованием встроенного физического датчика случайных чисел
04. Гарантия неизменности настроек платформы за счет применения ролевой модели разграничения прав администраторов (кворум) и разделения секрета по схеме Шамира
05. Возможность организации высокопроизводительного масштабируемого кластера
06. Поддержка актуальных отечественных и иностранных криптоалгоритмов

ОСОБЕННОСТИ

> Запись значимых для безопасности событий в системный журнал

> Веб-интерфейс для удаленного администрирования по защищенному каналу и сенсорный экран для локальной настройки

> Интерфейс PKCS#11 для работы с прикладными сервисами

> Поддержка работы с прикладными сервисами, управляемыми ОС Windows и Linux

> Возможность использования ViPNet HSM в качестве доверенной платформы для разработки новых криптографических сервисов, в том числе путем встраивания

Для разработчиков и ознакомления потенциальных заказчиков с ViPNet HSM по запросу предоставляется эмулятор продукта в виде Virtual Appliance.

ПРИМЕНЕНИЕ

Удостоверяющий центр

Увеличение сроков действия ключей электронной подписи и корневых сертификатов, снижение рисков компрометации ключей.

> Создание и хранение ключей администраторов удостоверяющих центров в изолированной доверенной среде ViPNet HSM
> Формирование и проверка электронной подписи по ГОСТ Р 34.10-2012, хэширование данных по ГОСТ Р 34.11-2012
> Совместное использование с серверами меток времени (TSP) и серверами проверки статуса сертификатов (OCSP)

Криптографическая платформа

Разработка прикладных криптографических сервисов с возможностью сертификации по высоким классам безопасности.

> TLS-шлюз
> сервер меток (штампов) времени
> платежный HSM
> генератор ключей для различных систем, например, ИСУЭ

Облачный сервис ЭП

Снижение расходов на развертывание инфраструктуры открытых ключей (PKI).

> надежное хранение ключей пользователей в зашифрованном виде
> защищенный доступ пользователей к ключам и к операциям с электронной подписью

СЕРТИФИКАЦИЯ

ФСБ России
СКЗИ класса КВ
и средство ЭП класса КВ2

Свидетельства
> В реестре российского ПО
> В реестре Минпромторга
> В реестре ПАК Минцифры

ViPNet PKI Service

Программно-аппаратный комплекс для генерации ключей, формирования и проверки электронной подписи, шифрования данных

Разработанный на базе криптографической платформы безопасности ViPNet HSM программно-аппаратный комплекс ViPNet PKI Service предназначен для выполнения криптографических операций в прикладных сценариях информационных систем: генерации ключей, формирования и проверки электронной подписи (ЭП), шифрования данных.

ПРЕИМУЩЕСТВА

01. Благодаря встраиванию в сертифицированную криптографическую платформу ViPNet HSM изделие ViPNet PKI Service обеспечивает криптографическую защиту данных, соответствующую высоким классам – СКЗИ класса КВ и средство ЭП класса КВ2
02. Реализована защита от злонамеренных действий администратора за счет применения ролевой модели с разграничением прав (кворум) и разделения секрета по схеме Шамира
03. Возможность реализации высокопроизводительного масштабируемого кластера
04. Надежная защита от физического несанкционированного доступа к хранимым данным обеспечивается датчиком контроля вскрытия корпуса и изменения физических параметров платформы (температура, питание)
05. Поддержание актуальности списков отозванных сертификатов (CRL) для проверки используемых пользователями сертификатов в автоматическом режиме
06. Криптостойкий механизм выработки ключей с использованием встроенного физического датчика случайных чисел

ВОЗМОЖНОСТИ

> Генерация и безопасное хранение ключей (компонентов ключей)
> Создание запроса на сертификат ключа проверки электронной подписи (ЭП)
> Шифрование и имитозащита данных
> Формирование и проверка ЭП в формате CMS, XMLDSig, CAdES, XAdES, WS-Security
> Хэширование данных
> Импорт ключей ЭП и сертификатов в формате PFX

Дополнительные возможности

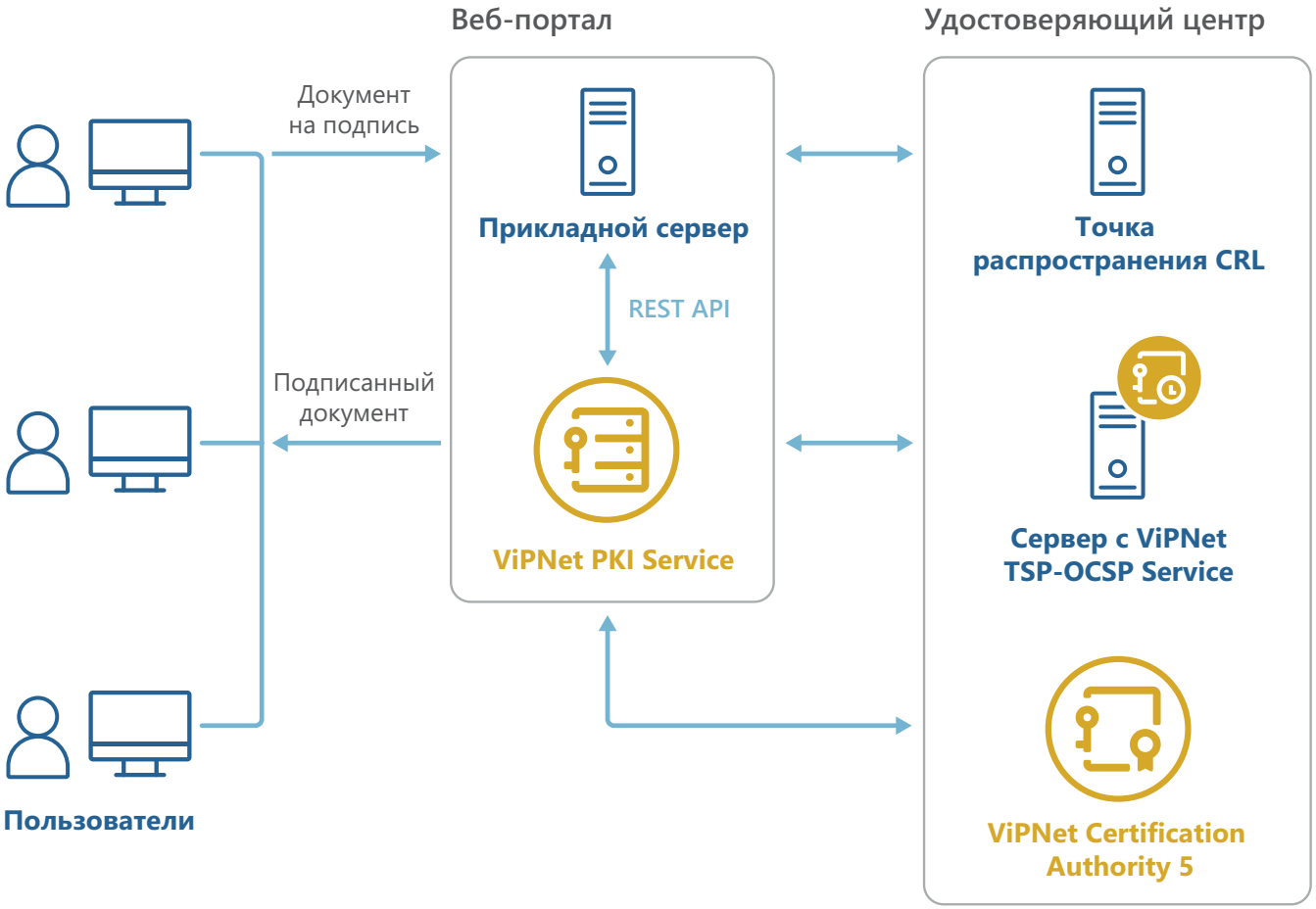
> Для интеграции с внешними информационными системами предоставляется REST API
> Для удаленного администрирования предоставляется веб-интерфейс
> Возможна совместная работа с ViPNet УЦ или КриптоПРО УЦ, серверами меток времени (в соответствии с RFC 3161) и OCSP (в соответствии с RFC 2560)
> Для разработчиков и ознакомления потенциальных заказчиков с ViPNet PKI Service по запросу предоставляется эмулятор продукта в виде Virtual Appliance

СЦЕНАРИИ

Корпоративный сервер подписи, обеспечивающий выполнение криптографических операций по запросам различных прикладных сервисов:

> электронного документооборота
> электронных торговых площадок
> автоматизированных систем управления
> технологическим процессом (АСУ ТП)
> дистанционного банковского обслуживания (ДБО)
> единой биометрической системы
> инфраструктуры Цифрового рубля финансовых посредников (коммерческих банков)

Сервер подписи, обеспечивающий выполнение криптографических операций по запросам пользователей и взаимодействие с другими компонентами PKI («облачная подпись»).



СЕРТИФИКАЦИЯ

ФСБ России
> СКЗИ класса КВ и средство ЭП класса КВ2

Свидетельства
> В реестре российского ПО
> В реестре Минпромторга
> В реестре ПАК Минцифры

ViPNet TLS Gateway

Шлюз безопасности, предназначенный для организации защищенных соединений по протоколу TLS с использованием отечественных и иностранных криптоалгоритмов

Использование протокола TLS обеспечивает аутентификацию пользователей и организацию защищенных соединений при работе с портальными решениями.

ВОЗМОЖНОСТИ

> Защищенный доступ к ресурсам по HTTPS

> Организация TLS-туннеля для защищенного доступа к ресурсам по TCP

> Интеграция с LDAP (Active Directory)

> Поддержка режимов односторонней и двусторонней аутентификации с использованием сертификатов, изданных различными удостоверяющими центрами (в т.ч. аккредитованными)

> Поддержка аутентификации по протоколам NTLM

> Поддержка политик разграничения доступа, в т.ч. по IP-адресам

> Возможность организации доступа к защищаемым ресурсам с использованием российских и/или иностранных криптоалгоритмов

> Поддержка TLS 1.3

> Поддержка IPv6

> Автоматическое поддержание актуальности списков аннулированных сертификатов (CRL), возможность использования протокола OCSP

> Возможность организации масштабируемого кластера высокой производительности с балансировкой нагрузки за счет внешнего балансировщика

> Управление кластером осуществляется с любого элемента кластера

> Импорт ключей и сертификатов в формате PFX

> Мониторинг состояния по протоколу SNMP

> Удаленное администрирование через веб-интерфейс и по протоколу SSH

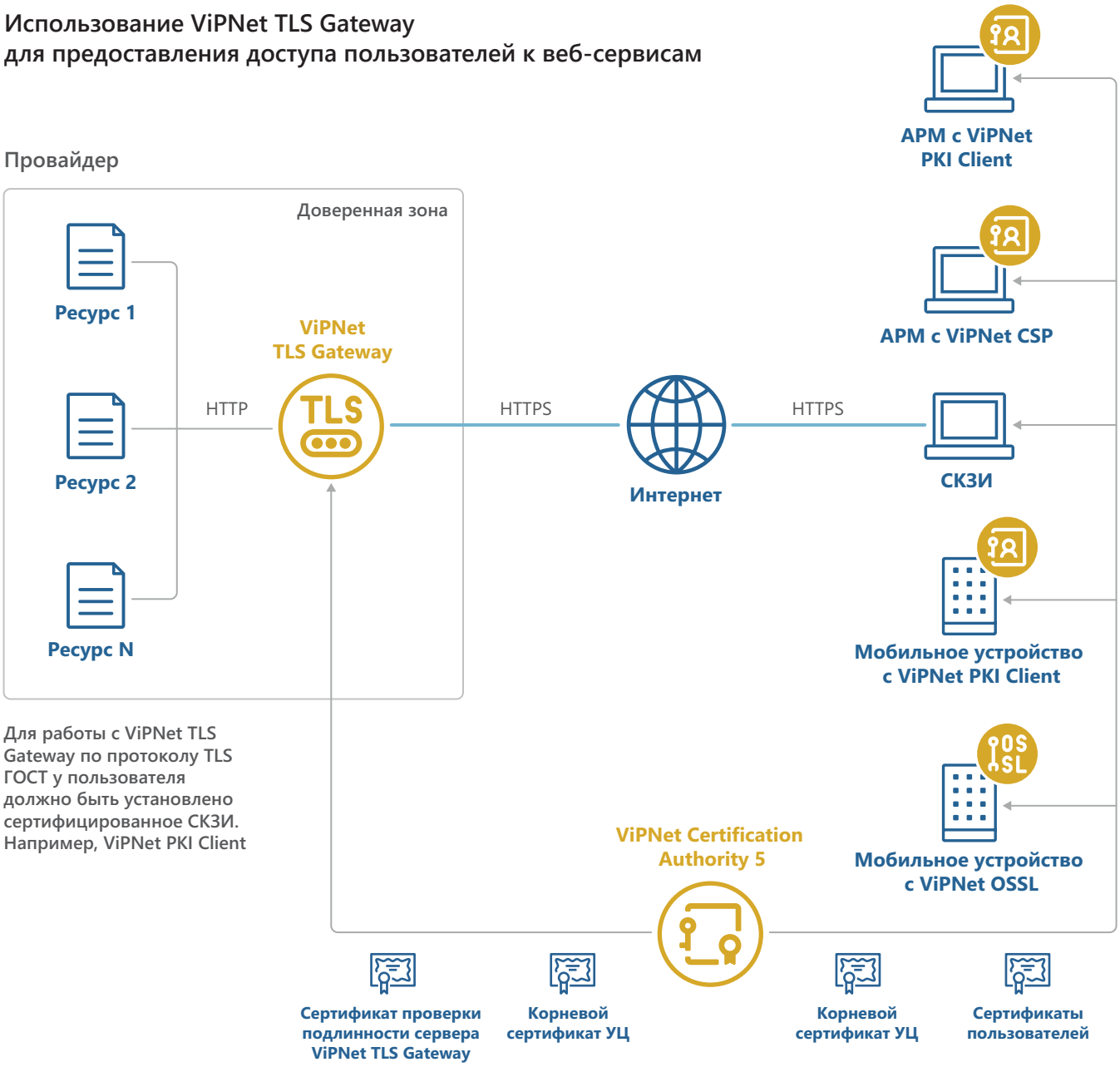
> Синхронизация времени с NTP-серверами

ОБЛАСТЬ ПРИМЕНЕНИЯ

1 Удаленный доступ сотрудников к корпоративным ресурсам

2 Предоставление электронных услуг по защищенному каналу

Использование ViPNet TLS Gateway для предоставления доступа пользователей к веб-сервисам



Для работы с ViPNet TLS Gateway по протоколу TLS ГОСТ у пользователя должно быть установлено сертифицированное СКЗИ. Например, ViPNet PKI Client

Поддерживаемые криптографические стандарты и рекомендации

- ГОСТ Р 34.10-2012, RSA, ECDSA
- ГОСТ Р 34.11-2012
- ГОСТ 28147-89, ГОСТ Р 34.12-2015 (ГОСТ 34.12-2018), ГОСТ Р 34.13-2015 (ГОСТ 34.13-2018), AES
- Рекомендации Технического комитета 26

Поддерживаемые виртуальные среды (для TLS VA)

- VMware Workstation
- VMware vSphere ESXi
- Oracle VM VirtualBox
- Microsoft Hyper-V
- Платформы виртуализации, основанные на Kernel Virtual Machine (KVM), в том числе отечественные гипервизоры

МОДЕЛЬНЫЙ РЯД

Исполнения TLS	TLS VA	TLS 550	TLS 1100	TLS 5500
Аппаратная платформа	виртуальная машина	TLS 500 Q2	TLS 1000 Q3	TLS 5000 Q2
Предельная пропускная способность в режиме обратного HTTPS-прокси, Мбит/с	зависит от характеристик аппаратного обеспечения	до 600	до 1800	до 7600
Максимальное число одновременных соединений в режиме обратного HTTPS-прокси и TCP-туннеля	зависит от характеристик аппаратного обеспечения	до 17000	до 34000	до 155000
Интерфейсы	зависят от характеристик аппаратного обеспечения	6x Ethernet 10/100/1000	8x Ethernet 10/100/1000 4x 1G Ethernet Fiber SFP	4x Ethernet 10/100/1000 8x 10G Ethernet Fiber SFP+

СЕРТИФИКАЦИЯ

ФСБ России

> СКЗИ класса КС3 для исполнений TLS 500, TLS 1000, TLS 5000, TLS 550, TLS 1100, TLS 5500

> СКЗИ класса КС1 для исполнения TLS VA

Свидетельства

> В реестре российского ПО

> В реестре Минпромторга

> В реестре ПАК Минцифры

ViPNet PKI Client

Универсальный клиент для работы
в инфраструктуре открытых ключей

Для обеспечения конфиденциальности и целостности передаваемых данных современные веб-сервисы позволяют пользователям применять различные методы криптографической защиты информации:

1 организацию защищенных соединений и аутентификацию по протоколу TLS

2 формирование и проверку электронной подписи

Чтобы задействовать эти средства защиты, пользователи зачастую вынуждены сочетать различные средства криптографической защиты информации, их компоненты или плагины. Все это усложняет использование веб-сервисов.

РЕШАЕМЫЕ ЗАДАЧИ

ViPNet PKI Client – универсальный программный комплекс, который решает основные задачи пользователя при работе с веб-сервисами:

> заверение документов электронной подписью и проверка электронной подписи
> шифрование файлов
> аутентификация пользователей для доступа к веб-сервисам
> построение защищенных TLS-соединений
> взаимодействие с сервером подписи ViPNet PKI Service с использованием хранящихся в нем ключей для формирования ЭП, расшифрования

СЕРТИФИКАЦИЯ

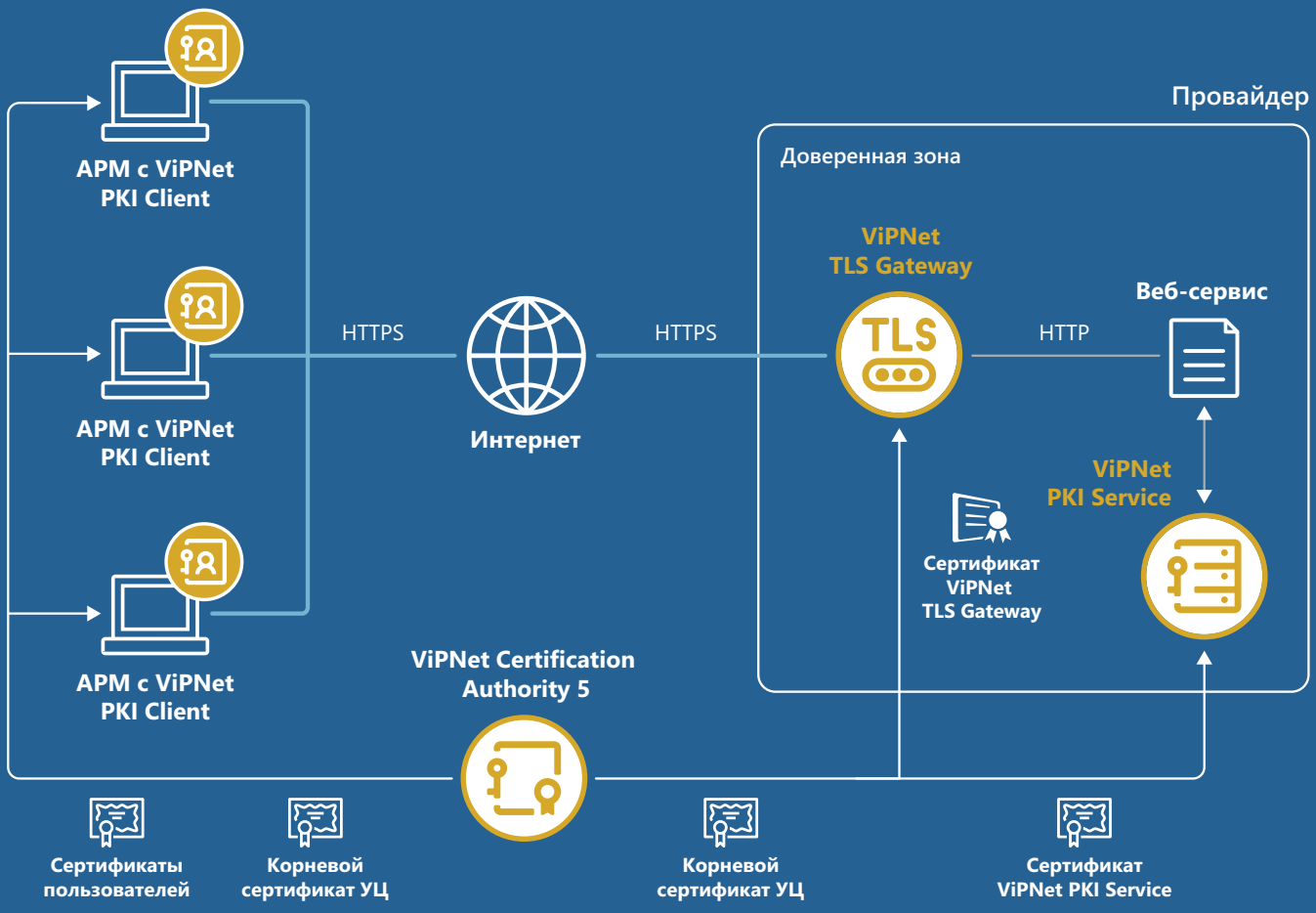
ФСБ России

СКЗИ и средство ЭП:

> КС1, КС2, КС3 для исполнений 1, 2, 3 (ОС Windows)
> КС1, КС2, КС3 для исполнений 4, 5, 6 (ОС Linux)
> КС1 для исполнения 7 (Android)

Свидетельства

В реестре российского ПО



ПРЕИМУЩЕСТВА

> Поддержка основных сценариев работы в PKI в рамках одного продукта

> Кроссбраузерность: для использования сервисов ЭП и шифрования в веб-сервисах пользователь может выбрать любой браузер

> Автоматическое обновление списков аннулированных сертификатов (CRL) для проверки ЭП (по расписанию)

> Поддержка различных форматов ЭП: PKCS#7 (CMS), XMLDSig, CAdES, XAdES, WS-Security

> Поддержка меток времени (TSP) и OCSP

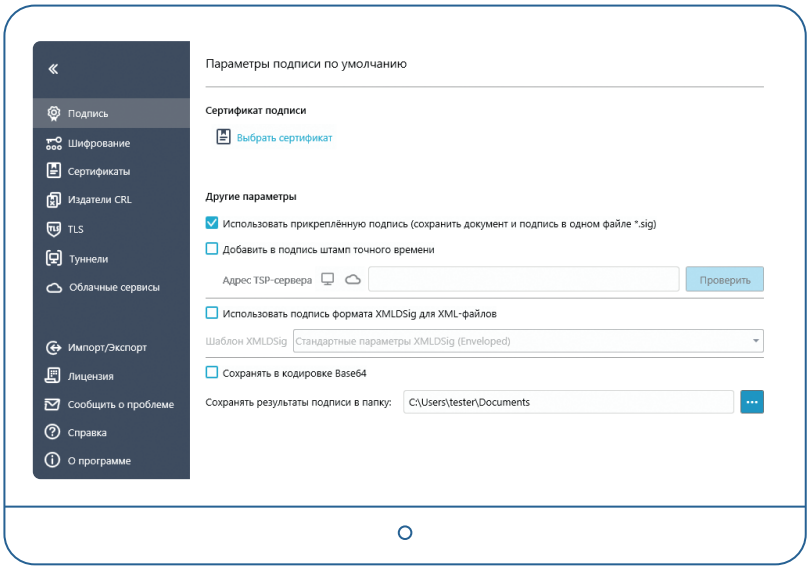
> Туннелирование TCP-трафика по протоколу TLS

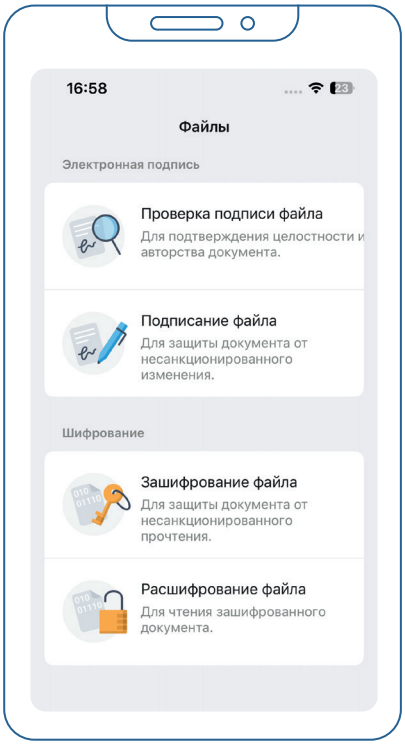
> Комплект для разработчиков веб-сервисов, обеспечивающий возможность вызова механизмов криптографической защиты информации ViPNet PKI Client

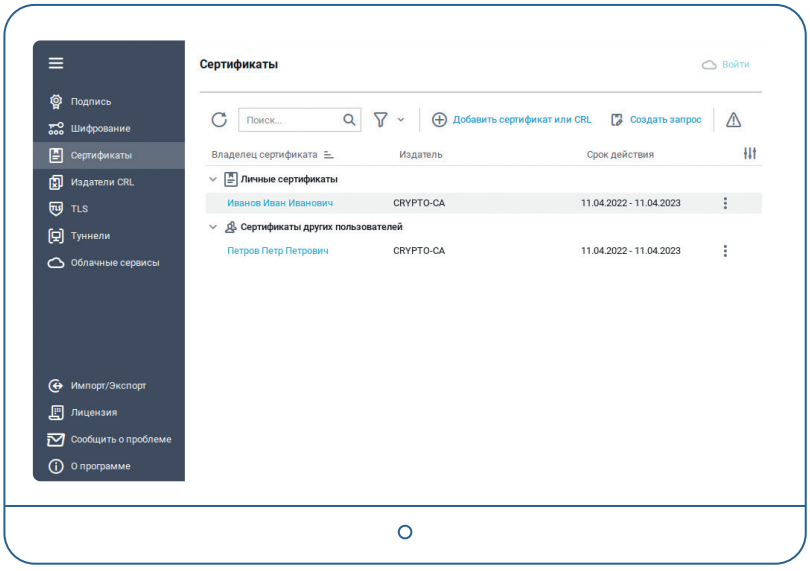
> Управление сертификатами ключей проверки ЭП:

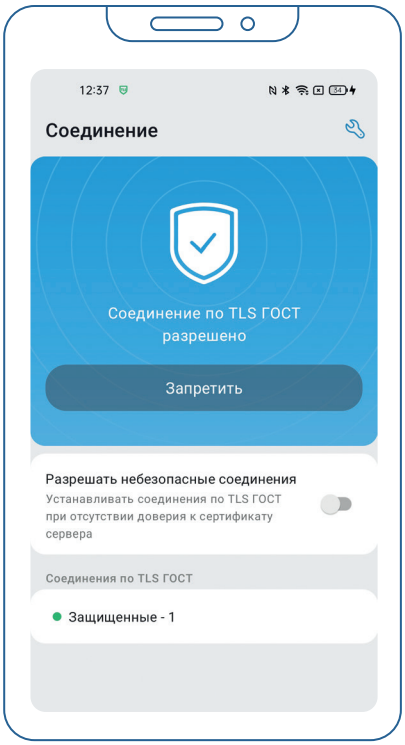
- удобный интерфейс для формирования запросов на сертификат (в формате PKCS#10)
- мониторинг и информирование пользователя об истечении сроков действия сертификатов и ключей ЭП
- работа с хранилищем сертификатов через интерфейс ViPNet PKI Client (установка сертификата в системное хранилище сертификатов в один клик)
- сертификаты из локального хранилища/токена/ViPNet PKI Service отображаются в одном окне

> Поддержка мобильных операционных систем (Android, Аврора)









КРИПТОАЛГОРИТМЫ

ГОСТ Р 34.10-2012

ГОСТ Р 34.11-2012

ГОСТ 28147-89

ГОСТ Р 34.12-2015 (ГОСТ 34.12-2018)

ГОСТ Р 34.13-2015 (ГОСТ 34.13-2018)

ViPNet Crypto

Криптографические
библиотеки для встраивания

Встраиваемые криптографические библиотеки ИнфоТеКС – это решение для разработчиков прикладного ПО, позволяющее использовать опыт специалистов в области информационной безопасности, воплощенный в реализованных криптоалгоритмах, интерфейсах и стандартах.

Библиотеки для встраивания ViPNet позволяют использовать криптографические алгоритмы ГОСТ в различных прикладных системах: от мобильных приложений до серверных решений.

Криптобиблиотеки в портфеле продуктов ИнфоТеКС:

ViPNet OSSL
кроссплатформенная библиотека на базе OpenSSL

ViPNet CSP
криптобиблиотека, реализующая Microsoft CryptoAPI

ViPNet CryptoSmart
криптография для блокчейн-платформ на базе Hyperledger Fabric

ViPNet JCrypto SDK
библиотека для разработки на Java

ПРЕИМУЩЕСТВА

Стандартные API
Используем стандартные API для быстрой интеграции: MS CryptoAPI, OpenSSL, PKCS#11, JCA

Надежная ГОСТ-криптография
Реализовали криптоалгоритмы ГОСТ в соответствии с методическими рекомендациями и требованиями регулятора

Расширенный SDK и примеры для встраивания
Предоставляем необходимые инструменты для работы с библиотекой

Разработчикам не требуется глубокое знание криптографии
Необходимые функции уже реализованы в криптобиблиотеках, поэтому разработчикам не нужно самостоятельно разбираться в математических основах

Поддержка от разработчиков
Прямые консультации и сопровождение от разработчиков криптобиблиотек

Прозрачность для пользователя
Встраиваемые криптобиблиотеки не влияют на брендинг и интерфейс прикладной системы

ВОЗМОЖНОСТИ

> Организация защищенных соединений

> Вычисление значений хэш-функций

> Вычисление имитовставки

> Обеспечение работы с электронной подписью на любых устройствах

> Шифрование файлов и данных

ФУНКЦИИ

> **Работа с ЭП**
ГОСТ Р 34.10-2001*, ГОСТ Р 34.10-2012

> **Хэширование**
ГОСТ Р 34.11-94*, ГОСТ Р 34.11-2012

> **Шифрование**
ГОСТ 28147-89* , ГОСТ Р 34.12-2015
ГОСТ Р 34.13-2015

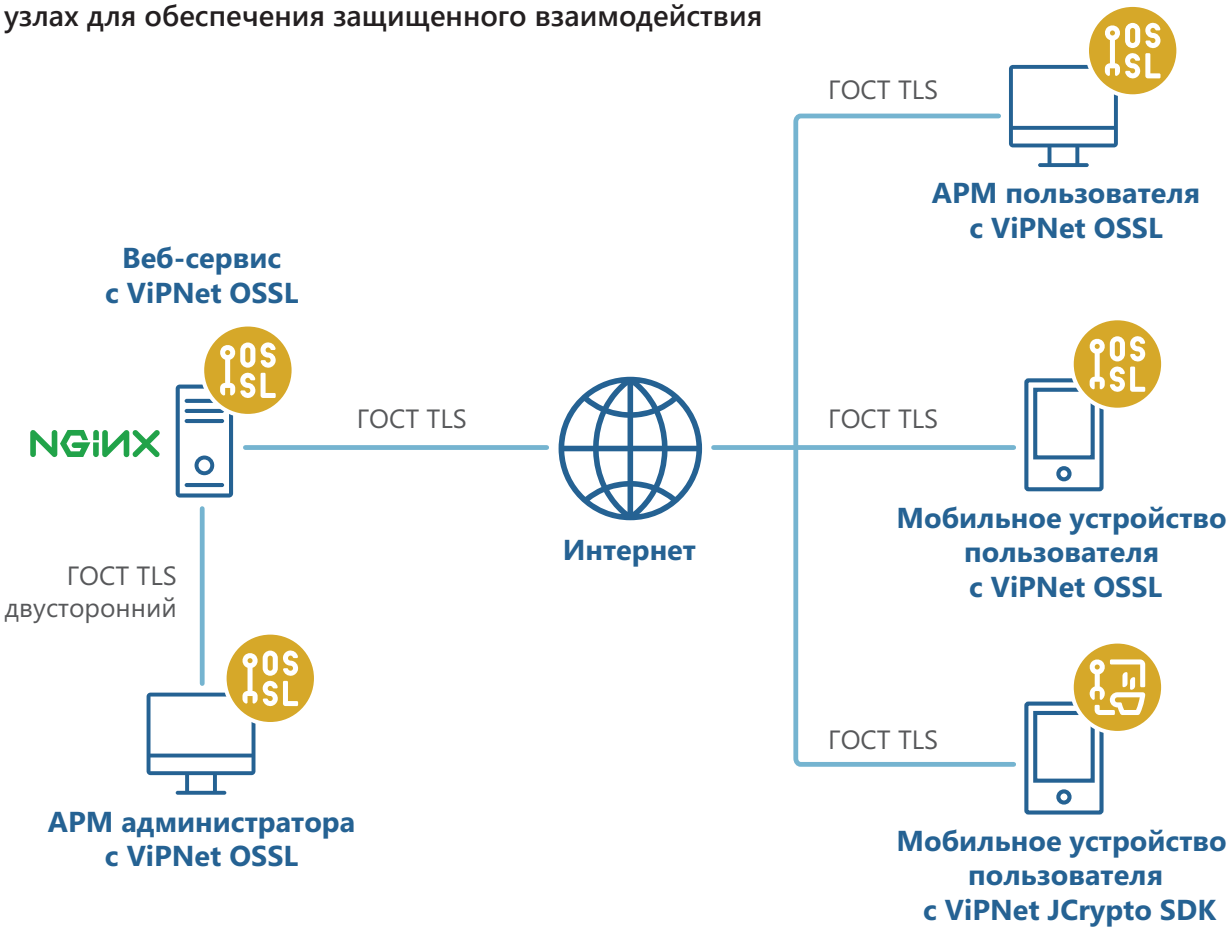
> **Защищенные соединения**
TLS 1.2, TLS 1.3

> **Работа с ключами на внешних устройствах**
Rutoken, JaCarta, Esmart и др.

> **Форматы**
CMS, PFX, XMLDsig, CAdES, XAdES, X.509

*в режиме совместимости

Использование криптобиблиотек на клиентских и серверных узлах для обеспечения защищенного взаимодействия



КРИПТОБИБЛИОТЕКИ ИНФОТЕКС

	ViPNet CSP	ViPNet OSSL	ViPNet JCrypto SDK	ViPNet CryptoSmart
Ключевая особенность	Для разработки ПО под Windows	Кроссплатформенная библиотека на базе OpenSSL	Библиотека для разработки на Java	Криптография для блокчейн-платформ (HLF)
Платформы	Windows, Linux	Windows, Linux, macOS, iOS, Android, Аврора	Windows, Linux, Android	Linux
Интерфейсы	MS CryptoAPI	PKCS#11 OpenSSL	JNI/JCA PKCS#11	MSP NetCSP BCCSP Lite
Класс защиты	КС1, КС2, КС3	КС1, КС2, КС3	КС1	КС1, КС2
Сертификация	Сертификат ФСБ России	Сертификат ФСБ России	Сертификат ФСБ России	Заключение ФСБ России

+7 495 737-61-92
8 800 250-0-260 (бесплатный звонок по России)

soft@infotecs.ru
hotline@infotecs.ru
www.infotecs.ru

PKI26_00RU