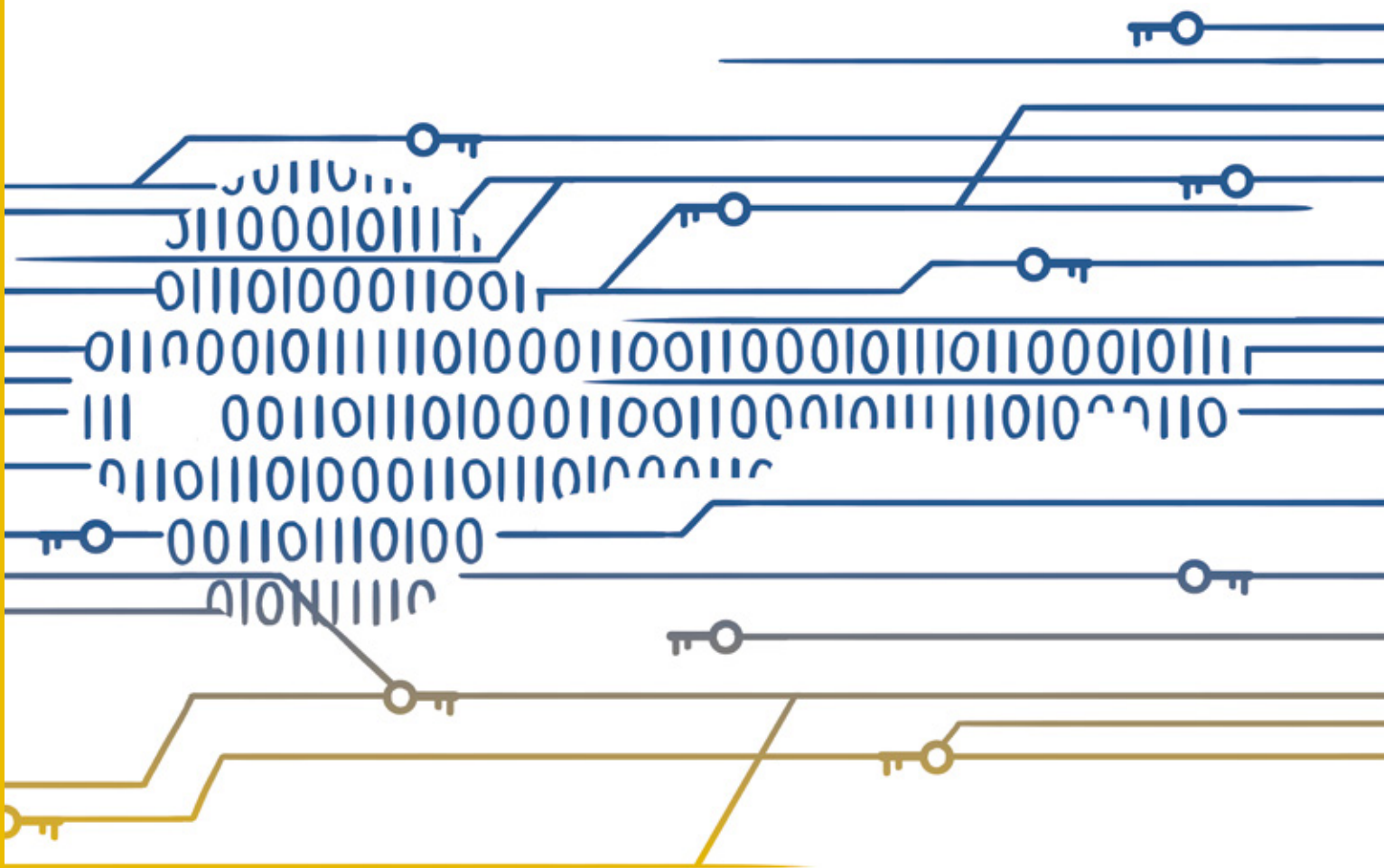



ViPNet PKI

Решения для работы
в инфраструктуре открытых ключей



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



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



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

[ПРЕИМУЩЕСТВА]

- 1 Возможность развертывания УЦ в организациях с территориально распределенной структурой
- 2 ViPNet Удостоверяющий центр 4 (версия 4.6) может использоваться аккредитованными УЦ для выпуска квалифицированных сертификатов
- 3 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]

- 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
- Для реализации функционала меток времени и OCSP может использоваться ViPNet TSP-OCSP Service

[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



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 (ГОСТ 28147-89, ГОСТ Р 34.10-2001/2012, 34.11-94/2012, ГОСТ Р 34.12-2015 (ГОСТ Р 34.12-2018), ГОСТ Р 34.13-2015 (ГОСТ Р 34.13-2018)).



[ПРЕИМУЩЕСТВА]

- Надежная защита от физического НСД к хранимым данным с помощью датчика контроля вскрытия корпуса и изменения физических параметров платформы (температура, питание)
- Широкие возможности применения посредством интеграции для обработки запросов различных сторонних сервисов
- Криптостойкий механизм выработки ключей с использованием встроенного физического датчика случайных чисел
- Гарантия неизменности настроек платформы за счет применения ролевой модели разграничения прав администраторов (кворум) и разделения секрета по схеме Шамира

[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

[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 34.10-2001/2012, хэширование данных по ГОСТ Р 34.11-94/2012
- Совместное использование с серверами меток времени (TSP) и серверами проверки статуса сертификатов (OCSP)

ОБЛАЧНЫЙ СЕРВИС ЭП

Снижение расходов на развертывание инфраструктуры открытых ключей (PKI).

- Надежное хранение ключей пользователей в ViPNet HSM
- Защищенный доступ пользователей к ключам и к операциям с электронной подписью
- Для разработчиков и ознакомления потенциальных заказчиков с ViPNet HSM по запросу предоставляется эмулятор продукта в виде Virtual Appliance

ПЛАТЕЖНЫЕ СИСТЕМЫ

Обеспечение безопасности финансовых операций в национальной и международных системах платежных карт, включая Мир, MasterCard и Visa.

- Обработка банковских транзакций* в режиме совместимости с протоколами отечественной и международных платежных систем
- Поддержка эмиссии банковских карт, выработка и печать ПИН-кодов
- Реализация функций центра сертификации платежных систем
- Поддержка международного стандарта операций по банковским картам EMV, в том числе со встроенными отечественными криптоалгоритмами
- Работа с основными отечественными и международными платежными приложениями терминального оборудования (M/Chip, VSDC)

* По результатам совместного тестирования с модулем авторизации системы WAY4 компании OpenWay и ПО TranzWare Online компании Compass Plus

[СЕРТИФИКАЦИЯ]

ФСБ РОССИИ

СКЗИ класса KB и средство ЭП класса KB2



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]

- 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
- Надежная защита от физического несанкционированного доступа к хранимым данным обеспечивается датчиком контроля вскрытия корпуса и изменения физических параметров платформы (температура, питание)
- Поддержание актуальности списков отозванных сертификатов (CRL) для проверки используемых пользователями сертификатов в автоматическом режиме
- Реализована защита от злонамеренных действий администратора за счет применения ролевой модели с разграничением прав (кворум) и разделения секрета по схеме Шамира
- Возможность реализации высокопроизводительного масштабируемого кластера

[ВОЗМОЖНОСТИ]

- Генерация и безопасное хранение ключей (компонентов ключей)
- Создание запроса на сертификат ключа проверки электронной подписи (ЭП)
- Формирование и проверка ЭП в формате CMS и XMLDSig
- Шифрование и имитозащита данных
- Хэширование данных

ДОПОЛНИТЕЛЬНЫЕ ВОЗМОЖНОСТИ

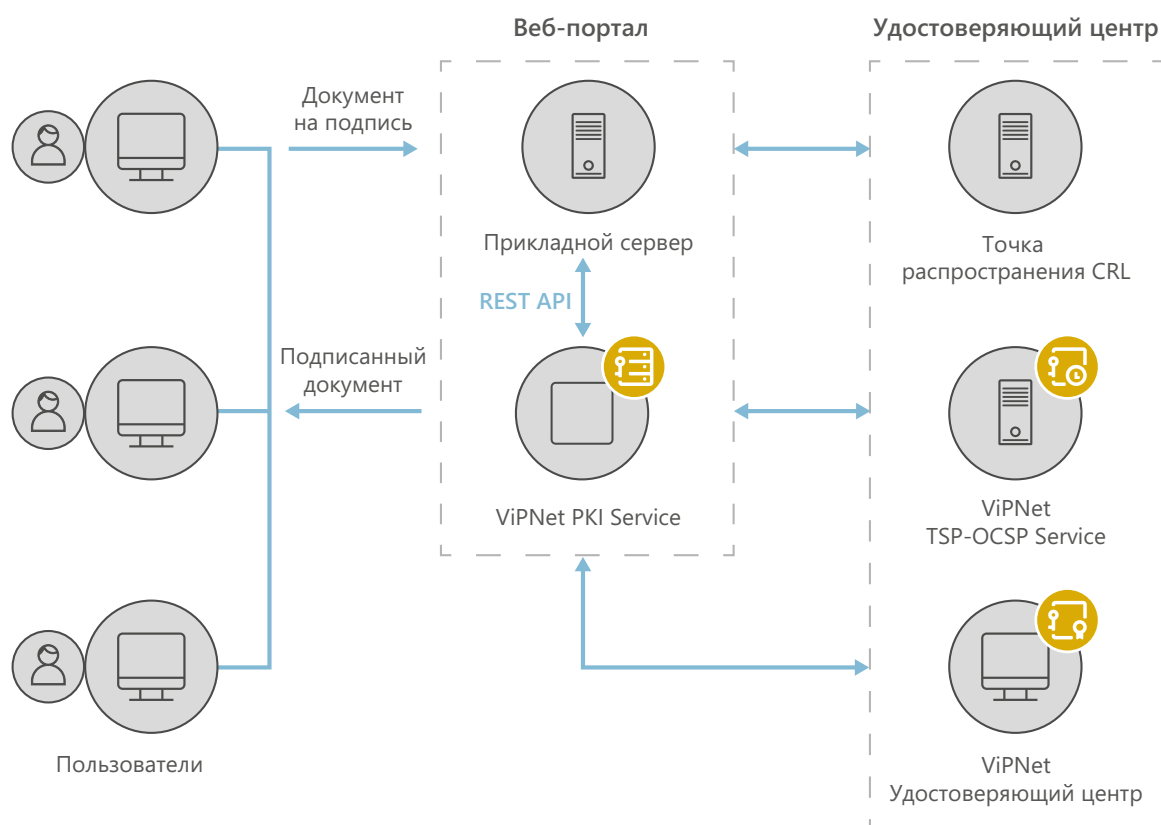
- Для интеграции с внешними информационными системами предоставляется REST API
- Для удаленного администрирования предоставляется веб-интерфейс
- Возможна совместная работа с УЦ (pkcs#10), серверами меток времени (в соответствии с RFC 3161) и OCSP (в соответствии с RFC 2560)
- Для разработчиков и ознакомления потенциальных заказчиков с ViPNet PKI Service по запросу предоставляется эмулятор продукта в виде VA

[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

Сервер подписи, обеспечивающий выполнение криптографических операций по запросам пользователей и взаимодействие с другими компонентами PKI.



[СЕРТИФИКАЦИЯ]

ФСБ РОССИИ

СКЗИ класса КВ и средство ЭП класса КВ2



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:



организацию защищенных соединений и аутентификацию по протоколу TLS



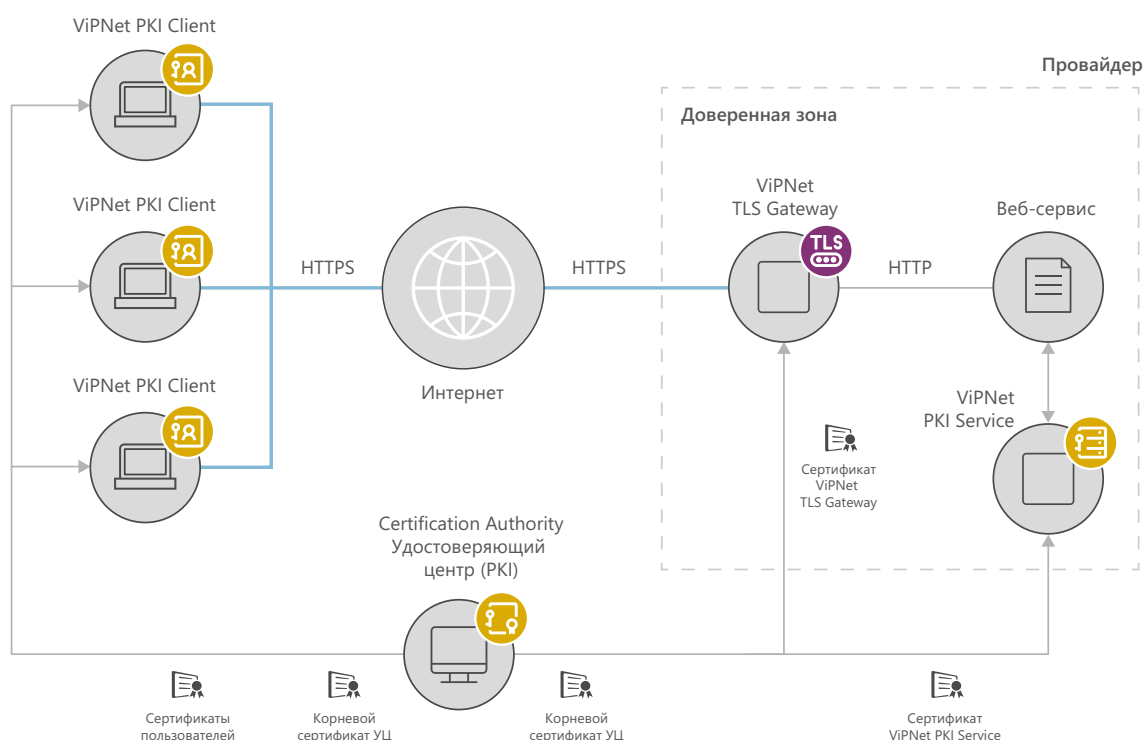
формирование и проверку электронной подписи

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:

- 1 заверение документов электронной подписью
- 2 шифрование файлов
- 3 аутентификация пользователей для доступа к веб-сервисам
- 4 построение защищенных TLS-соединений



[ПРЕИМУЩЕСТВА]

- 1 Поддержка основных сценариев работы в PKI в рамках одного продукта
- 2 Кросс-браузерность: для использования сервисов ЭП и шифрования в веб-сервисах пользователь может выбрать любой браузер
- 3 Автоматическое обновление списков аннулированных сертификатов (CRL) для проверки ЭП и сертификатов ключей проверки ЭП (по расписанию)
- 4 Поддержка различных форматов ЭП: PKCS#7 (CMS), XMLDSig, CAdES
- 5 Поддержка меток времени (TSP) и OSCP
- 6 Туннелирование TCP-трафика по протоколу TLS
- 7 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
 - работа с хранилищем сертификатов через интерфейс ViPNet PKI Client (установка сертификата в системное хранилище сертификатов в один клик)
- 8 Комплект для разработчиков веб-сервисов, обеспечивающий возможность вызова механизмов криптографической защиты информации ViPNet PKI Client
- 9 Поддержка мобильных операционных систем (Android и iOS)

[СЕРТИФИКАЦИЯ]

ФСБ РОССИИ

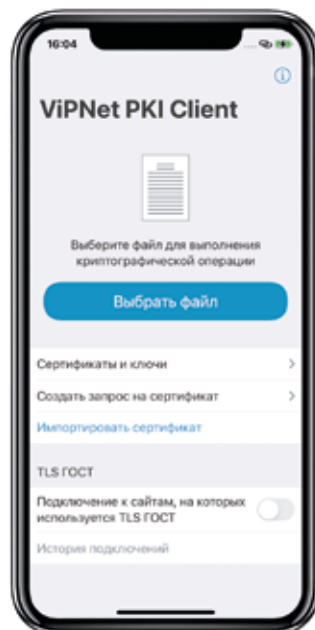
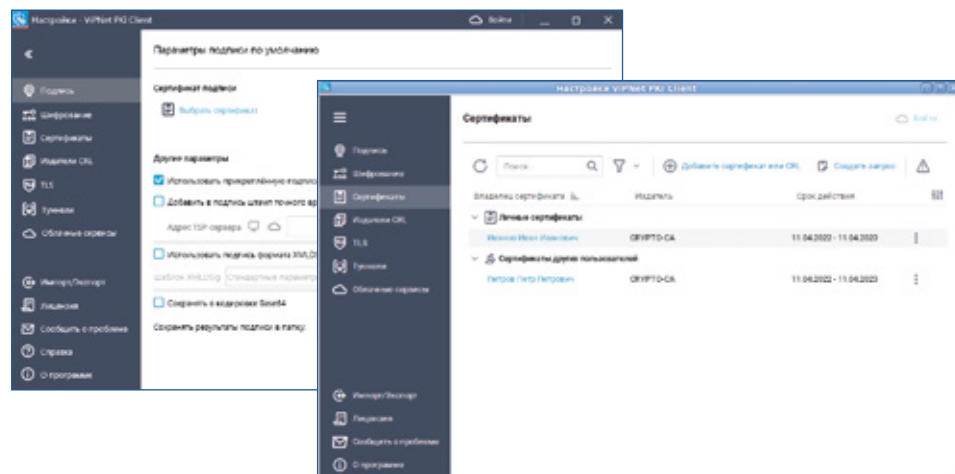
СКЗИ и средство ЭП:

- KC1, KC2, KC3 для исполнений 1, 2, 3 (OC Windows)
- KC1, KC2, KC3 для исполнений 4, 5, 6 (OC Linux)

[КРИПТОАЛГОРИТМЫ]

ГОСТ Р 34.10-2001/2012
 ГОСТ Р 34.11-94/2012
 ГОСТ 28147-89

ГОСТ Р 34.12-2015 (ГОСТ Р 34.12-2018)
 ГОСТ Р 34.13-2015 (ГОСТ Р 34.13-2018)



ViPNet OEM Crypto

Встраивание криптографии в прикладное ПО

Криптобиблиотеки ИнфоТеКС – это готовые для встраивания решения, которые позволяют разработчикам ПО использовать опыт квалифицированных специалистов в области информационной безопасности, воплощенный в уже готовых криптоалгоритмах.

При интеграции в конечный продукт криптобиблиотека обогащает его дополнительными возможностями и становится его частью за счет гибкости встраивания и возможностей тонкой настройки.

КРИПТОБИБЛИОТЕКИ В ПОРТФЕЛЕ ПРОДУКТОВ ИнфоТеКС:



ViPNet CSP –
библиотека для
разработки ПО под Windows



ViPNet JCrypto SDK –
библиотека для разработки
на Java



ViPNet OSSL –
кроссплатформенная
библиотека на базе OpenSSL



ViPNet CryptoSmart –
криптография для блокчейн-
платформ (HLF)

[СЦЕНАРИИ ИСПОЛЬЗОВАНИЯ]

- 1 Встраивание криптографических функций в сторонние приложения, например:
 - в системы юридически значимого защищенного электронного документооборота
 - в системы сдачи электронной отчетности в государственные органы
- 2 Защищенная работа с веб-сервисами:
 - nginx
 - apache

[ПРЕИМУЩЕСТВА]

- Встраивание в различные типы приложений благодаря поддержке популярных ОС и архитектур
- Использование веб-серверов apache, nginx
- Совместимость форматов ключей с решениями других производителей
- Облегченная интеграция новых устройств за счет использования интерфейса PKCS#11
- Нет необходимости понимать математические аспекты криптографии
- Реализация криптографических функций и интерфейсов согласно стандартам
- Подробная документация с примерами

[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
- и др.

ФОРМАТЫ

- CMS
- PFX
- XMLDsig
- CAdES
- XAdES
- X.509

* в режиме совместимости

[БИБЛИОТЕКИ 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 Авропа	Windows Linux Android	Linux
Интерфейсы	MS CryptoAPI	PKCS#11 OpenSSL	JNI/JCA PKCS#11	MSP NetCSP BCCSP Lite
Класс защиты	KC1, KC2, KC3	KC1, KC2, KC3	KC1	KC1, KC2



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



soft@infotecs.ru
hotline@infotecs.ru



www.infotecs.ru



Содержимое документа носит исключительно информационный характер и не является публичной офертой. Для получения подробной информации об указанных в документе продуктах и услугах вы можете обратиться в АО «ИнфоТеКС». Все изображения являются лишь иллюстрациями. Все технические характеристики, внешний вид и комплектность описываемой продукции могут меняться без предварительного уведомления. Символы ™ или ® в документе не используются, однако, если не указано иного, все товарные знаки в данном документе защищены соответствующим правом, которое принадлежит их владельцам.