infotecs

ViPNet Crypto

Прикладная криптография для встраивания

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 JCrypto SDK
библиотека для разработки на Java

ViPNet CryptoSmart
криптография для блокчейн-платформ на базе Hyperledger Fabric

ViPNet CSP
криптобиблиотека, реализующая Microsoft CryptoAPI

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

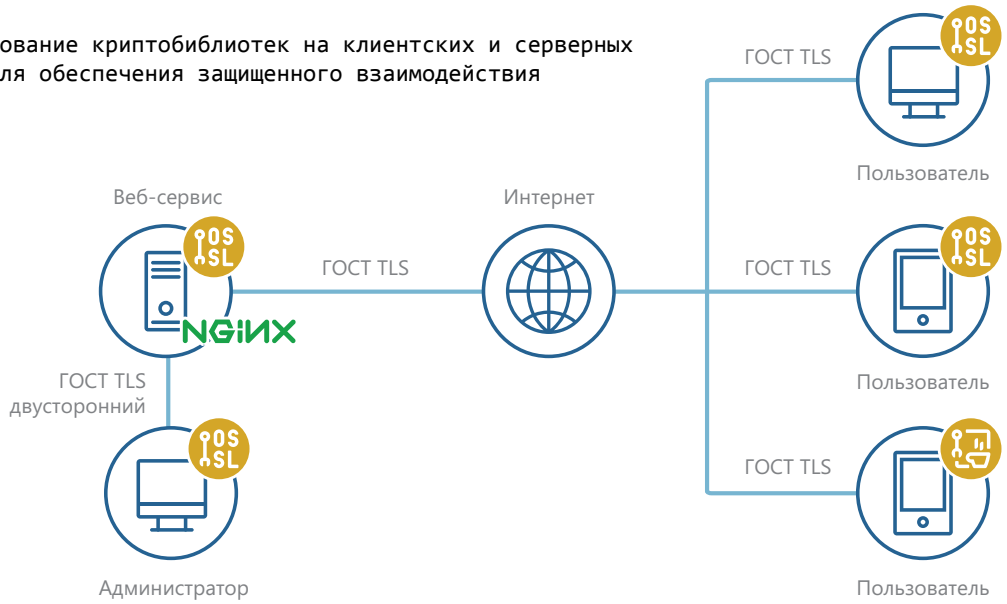
> Организация защищенных соединений
> Вычисление значений хэш-функций
> Вычисление имитовставки
> Обеспечение работы с электронной подписью на любых устройствах
> Шифрование файлов и данных

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

ViPNet OSSL

Кроссплатформенная криптографическая библиотека на базе OpenSSL

ViPNet OSSL – готовое решение для встраивания ГОСТ-криптографии в прикладные системы, созданное на базе библиотеки с открытым исходным кодом OpenSSL.

ViPNet OSSL позволяет использовать российские криптографические алгоритмы ГОСТ через обращения по интерфейсу OpenSSL.

ViPNet OSSL применяется на рабочих станциях, мобильных устройствах, серверах.

ВОЗМОЖНОСТИ

- Не требуется оценка влияния при работе с NGINX, Apache, Stunnel
- ГОСТ-TLS на клиентской и серверной стороне
- Работа с УКЭП на клиентских устройствах, в том числе мобильных
- Работа с NGINX, Apache, Stunnel
- Организации защищенных соединений
- Поддержка работы токенов как на стационарных, так и на мобильных устройствах
- Шифрование файлов и данных
- Поддержка дуальной криптографии

СОВМЕСТИМОСТЬ

Операционные системы

- MS Windows
- Linux, в т.ч. Astra Linux, Роса, Альт
- macOS
- iOS
- Android
- Аврора

Среды виртуализации

- среды с поддержкой Kernel Virtual Machine (KVM)
- Microsoft Hyper-V
- VMware
- VirtualBox

Внешние устройства

- ViPNet HSM
- Рутокен
- Jacarta
- ESMART*

*Полный перечень совместимых операционных систем, сред виртуализации и внешних устройств с указанием версий и модификаций указан в документации на продукт.

СЕРТИФИКАЦИЯ

ФСБ России

СКЗИ и средство ЭП по классам КС1, КС2, КС3

Свидетельства

В реестре российского ПО

ViPNet JCrypto

Криптобиблиотека для разработки на Java

ViPNet JCrypto SDK – готовое решение для встраивания ГОСТ-криптографии в прикладные системы, работающие в Java-машинах под операционными системами Android, Windows и Linux через стандартизованный интерфейс JCA.

ВОЗМОЖНОСТИ

> Организация защищенных TLS-соединений на клиентских устройствах

> Удобная разработка под Android за счет использования Java-интерфейсов

> Работа с УКЭП на клиентских устройствах, в том числе мобильных

> Поддержка отечественных сред разработки

СОВМЕСТИМОСТЬ

Операционные системы

> MS Windows

> Linux, в т.ч. Astra Linux, Роса, Альт

> Android

Среды разработки:

> Oracle JRE

> OpenJDK

> Axiom JDK

СЕРТИФИКАЦИЯ

В процессе сертификации на соответствие требованиям ФСБ России: СКЗИ и средство ЭП по классу КС1

ViPNet CryptoSmart

Криптография для блокчейн-платформ на базе Hyperledger Fabric

ViPNet CryptoSmart – готовое решение для встраивания ГОСТ-криптографии в прикладные системы, работающие с распределенными реестрами.

ВОЗМОЖНОСТИ

> Формирование, проверка и защита цепочки блоков

> Аутентификация пользователей

> Управление правами доступа

> Защита данных

> Защита каналов связи по протоколу TLS

СОВМЕСТИМОСТЬ

Операционные системы
Linux, в т.ч. Astra Linux, Роса, Альт

СЕРТИФИКАЦИЯ

В процессе сертификации на соответствие требованиям ФСБ России: СКЗИ и средство ЭП по классам КС1 и КС2

ViPNet CSP

Криптобиблиотека, реализующая Microsoft CryptoAPI

ВОЗМОЖНОСТИ

> Предоставление криптографических сервисов для физических лиц

> Встраивание криптографических функций в прикладное ПО

> Организация защищенных TLS-соединений

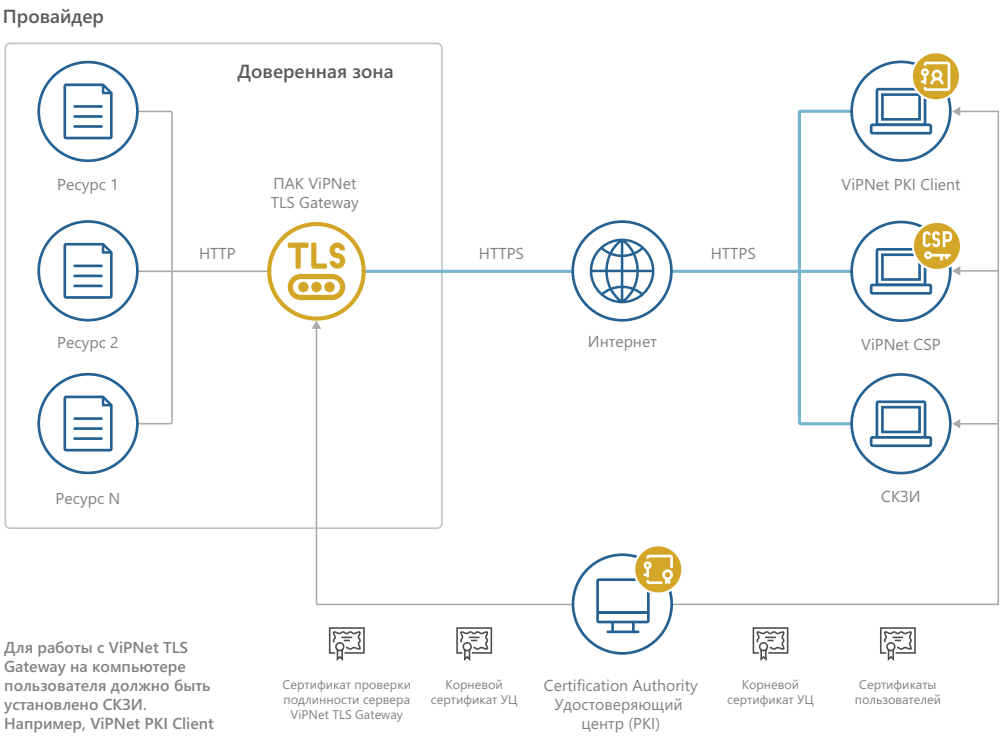
> Формирование и проверка ЭП

> Шифрование файлов и данных

> Интеграция с популярными плагинами (Госуслуги, КриптоПро ЭЦП Browser plug-in)

> Поддержка работы токенов

Использование ViPNet CSP для предоставления доступа пользователей к веб-сервисам



СОВМЕСТИМОСТЬ

Операционные системы

> MS Windows
> Linux, в т.ч. Astra Linux, Роса, Альт

Поддерживает среды виртуализации:

> среды с поддержкой Kernel Virtual Machine (KVM)
> VMware

Поддерживает внешние устройства:

> ViPNet HSM
> ESMART
> Рутокен
> JaCarta*

*Полный перечень совместимых операционных систем, сред виртуализации и внешних устройств с указанием версий и модификаций указан в документации на продукт.

СЕРТИФИКАЦИЯ

ФСБ России

СКЗИ и средство ЭП по классам КС1, КС2, КС3

Свидетельства

В реестре российского ПО

Стенд для тестирования TLS 1.3

Загрузить дистрибутивы

infotecs

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

soft@infotecs.ru
hotline@infotecs.ru

www.infotecs.ru

PKI24_00RU

ViPNet Virtual Private Network

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.