Говорите шепотом, здесь криптобиблиотека

Арина Эм

Ведущий менеджер продуктов

инфотекс ТЕХНОДЕСТ

Белый поток

Криптография в прикладных системах


Офисные приложения


Документооборот


Логистика


Мобильные приложения


Шифрование данных в облаке

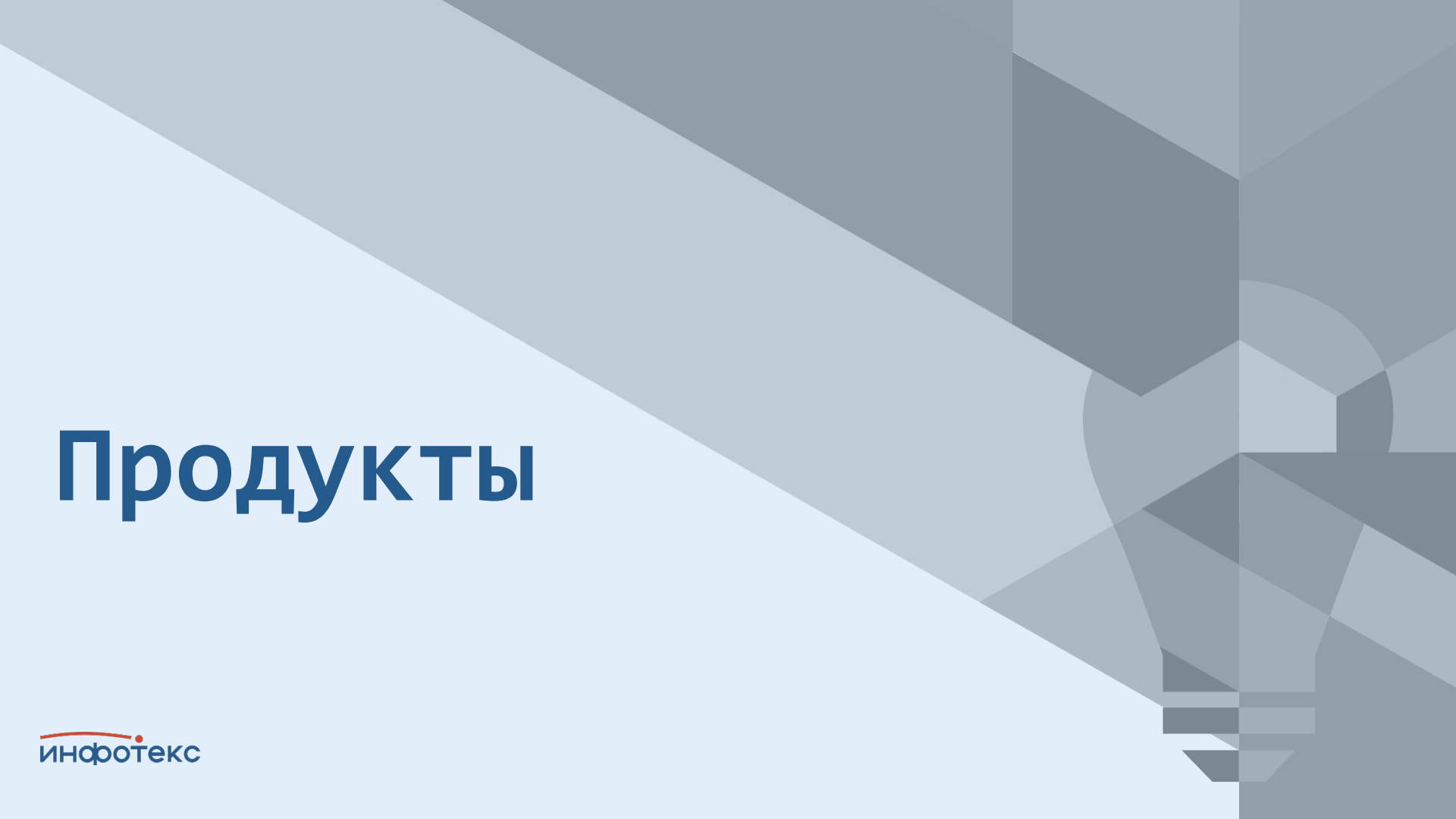

Здравоохранение


Банкинг


Мессенджеры


Интернет вещей

Продукты



инфотекс

Криптобиблиотеки ИнфоТеКС

ViPNet **OSSL**

Для разработки мобильных
и серверных решений

ViPNet **CSP**

Для разработки
ПО под Windows

ViPNet JCrypto SDK

Для разработки ПО на Java

ViPNet CryptoSmart

Для тех, кому нужен
ГОСТ в блокчейне

Функциональность криптобиблиотек

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

Форматы

CMS	CAdES
PFX	XAdES
XMLDsig	X.509

Протоколы

TLS 1.2	TSP
TLS 1.3	OCSP

Работа с ключами на токенах

ViPNet HSM
Rutoken
JaCarta

Интерфейсы

CryptoAPI	Java SDK
OpenSSL	GO

Поддержка ОС

ViPNet OSSL

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

ФЕДЕРАЛЬНАЯ СЛУЖБА БЕЗОПАСНОСТИ
РОССИЙСКОЙ ФЕДЕРАЦИИ

Система сертификации РОСС RU.0001.030001

СЕРТИФИКАТ СООТВЕТСТВИЯ

Регистрационный номер ***СФ/124-5420*** от "***10***" ***марта*** 202***6*** г.

Действителен до "***10***" ***ноября*** 202***7*** 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, 10, 11, 12, 13, 14, 15, 16) в комплектации согласно формуляру ФРКЕ.00221-02 30 01 ФО с учётом извещения об изменении № 7 ФРКЕ.00221.FB.7-2025

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, 10, 11, 14), класса КС2 (для исполнений: 2, 5, 12, 15), класса КС3 (для исполнений: 3, 6, 13, 16). 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, 10, 11, 14), класса КС2 (для исполнений: 2, 5, 12, 15), класса КС3 (для исполнений: 3, 6, 13, 16), 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), № 1015-000510 (для исполнения 10), № 1015-000511 (для исполнения 11), № 1015-000512 (для исполнения 12), № 1015-000513 (для исполнения 13), № 1015-000514 (для исполнения 14), № 1015-000515 (для исполнения 15), № 1015-000516 (для исполнения 16).

Безопасность информации обеспечивается при использовании комплекса, изготовленного в соответствии с техническими условиями ФРКЕ.00221-02 97 01 ТУ с учётом извещения об изменении № 7 ФРКЕ.00221.FB.7-2025, и выполнении требований эксплуатационной документации согласно формуляру ФРКЕ.00221-02 30 01 ФО с учётом извещения об изменении № 7 ФРКЕ.00221.FB.7-2025.

ViPNet OSSL 5.6 сертифицирован ФСБ России

по классам КС1, КС2, КС3

До 10 ноября 2027 года

Что нового в версии OSSL 5.6

Лицензирование в мобильных исполнениях стало **однофакторным**

Актуализировали **ОС**

Изменили подход к **контролю целостности среды** функционирования

Расширили **список белых функций**

Оценка влияния не требуется при использовании

Apache 2.4.57 | NGINX 1.18, 1.22 | Stunnel 5.67

ViPNet OSSL: лицензирование

для клиентов

- функции подписи и шифрования на клиентских устройствах
- нужна оценка влияния

для серверов

NGINX APACHE HTTP SERVER PROJECT stunnel

- гибкость в выборе места установки
- распараллеливание процессов
- не нужна оценка влияния

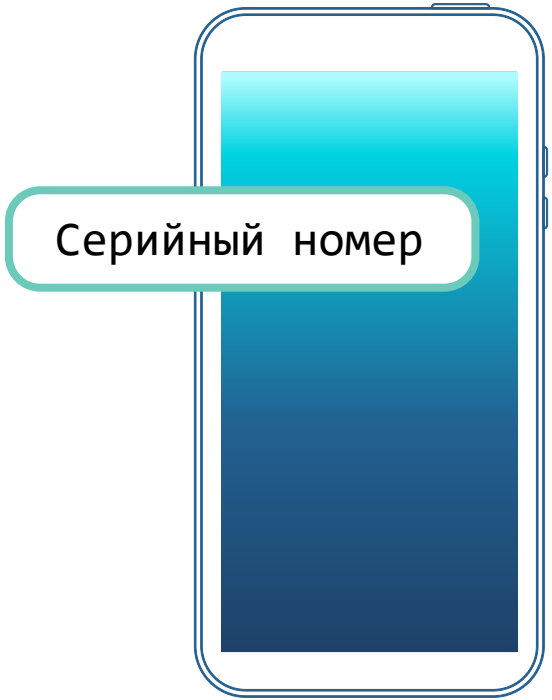
Лицензирование

Было

Двухфакторная регистрация

Стало

Однофакторная регистрация



ViPNet JCrypto SDK

Криптобиблиотека для разработки на Java-машинах

Сертификат ФСБ России: КС1, КС2, КС3

Криптоядро ViPNet OSSL

Поддержка мобильных ОС

Особенности

- Стандартные интерфейсы JNI/JCA и PKCS#11
- Поддержка различных форматов подписи
- Актуальные алгоритмы и протоколы
- Содержит программный токен
- Совместим с токенами и смарт-картами

ФЕДЕРАЛЬНАЯ СЛУЖБА БЕЗОПАСНОСТИ
РОССИЙСКОЙ ФЕДЕРАЦИИ

Система сертификации РОСС RU.0001.030001

СЕРТИФИКАТ СООТВЕТСТВИЯ

Регистрационный номер *СФ/114-5053* от "*20*" *декабря* 2024 г.

Действителен до "*10*" *ноября* 2027 г.

Выдан Акционерному обществу «Информационные технологии и коммуникационные системы».

Настоящий сертификат удостоверяет, что Программный комплекс ViPNet JCrypto SDK (исполнения: 1, 2) в комплектации согласно формуляру ФРКЕ.00145-07 30 01 ФО

соответствует Требованиям к средствам криптографической защиты информации, предназначенным для защиты информации, не содержащей сведений, составляющих государственную тайну, класса КС1, Требованиям к средствам электронной подписи, утверждённым приказом ФСБ России от 27 декабря 2011 г. № 796, установленным для класса КС1, 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 № 1053-000501 (для исполнения 1), № 1053-000502 (для исполнения 2).

Безопасность информации обеспечивается при использовании комплекса в соответствии с требованиями эксплуатационной документации согласно формуляру ФРКЕ.00145-07 30 01 ФО.

Заместитель руководителя Научно-технической службы – начальник Центра защиты информации и специальной связи ФСБ России О.В. Скрябин

инфотекс

ViPNet JCrypto SDK сертифицирован ФСБ России

по классу КС1

До 10.11.2027

ViPNet JCrypto SDK 3.4

Ядро: **ViPNet OSSL 5.6**

Реализована поддержка **PFX**

Реализована функция **создания запроса на сертификат** с помощью ViPNet OSSL API

Обеспечена работа с **несколькими токенами**

Реализована **динамическая инициализация ViPNet OSSL**

Реализовано использование ViPNet JCrypto SDK из **фреймворка Maven**

ViPNet CryptoSmart

Заключение ФСБ

Криптоядро
ViPNet OSSL

Криптобиблиотека
для реализации ГОСТ
в блокчейне

Особенности

- Поддержка различных форматов подписи
- Актуальные алгоритмы и протоколы
- Содержит программный токен
- Совместим с токенами и смарт-картами

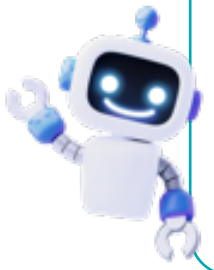
ViPNet CSP

Криптопровайдер
для граждан
и разработчиков

Сертификат ФСБ России: КС1, КС2, КС3

Упрощенная интеграция на Windows

Бесплатно под Windows



Особенности

- Интерфейс MS CryptoAPI
- Поддержка различных форматов подписи
- Актуальные алгоритмы и протоколы
- Совместим с токенами и смарт-картами
- Возможность экспортировать ключи с других машин и криптопровайдеров

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, утверждённым 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.

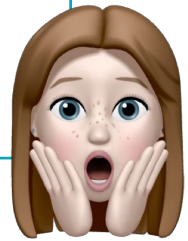
инфотекс

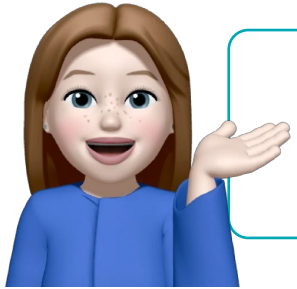
ViPNet CSP 4.4.8 сертифицирован ФСБ России по классам КС1, КС2, КС3

До 28 декабря 2026 года

Важное напоминание!

На данный момент мы не планируем дальнейшее развитие ViPNet CSP 4.4





Переходите на новый красивый современный **ViPNet CSP 5**

Что изменилось в ViPNet CSP 5

Новый GUI

Новый интерфейс MS CNG
взамен устаревшего MS CryptoAPI

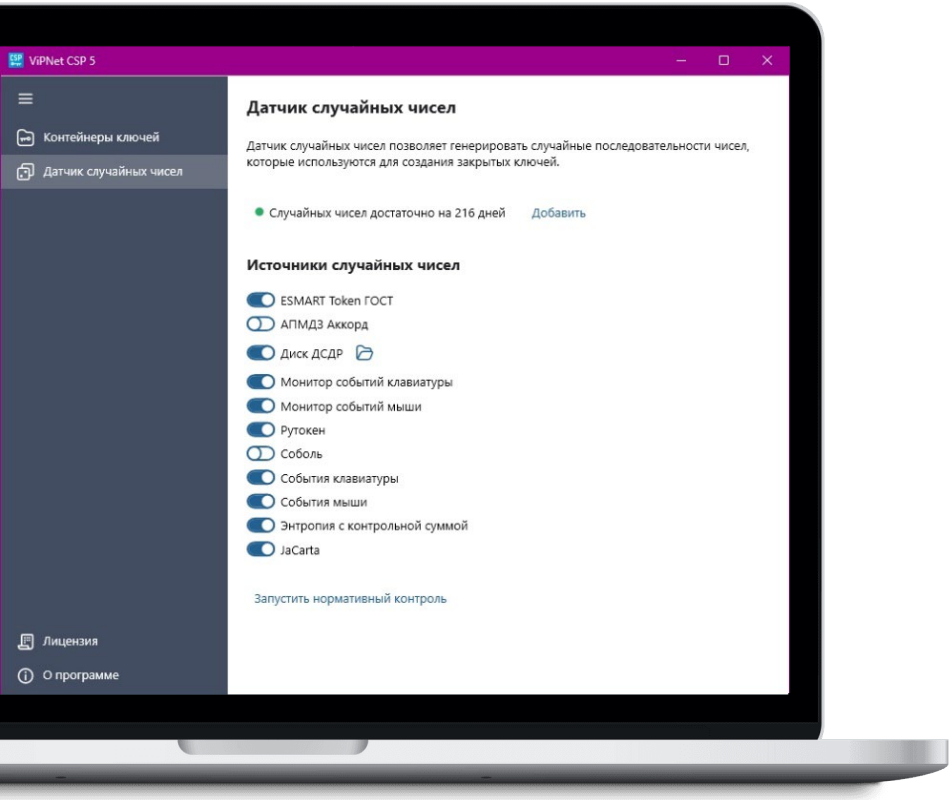
Поддержка новых ГОСТ-алгоритмов через MS CNG

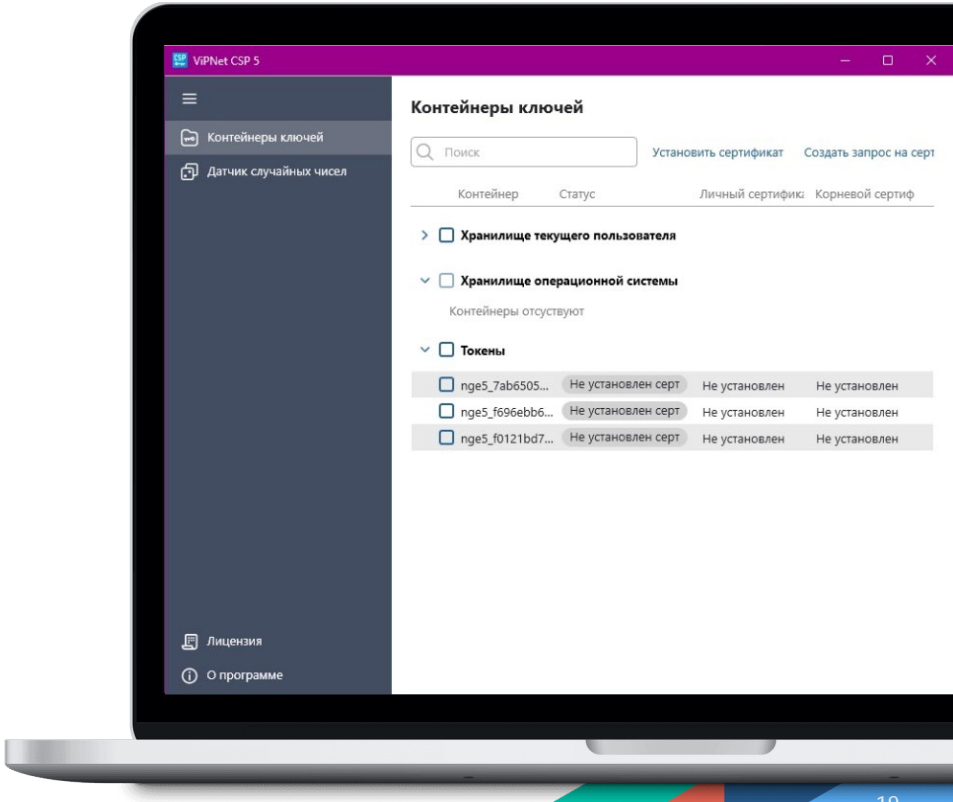
Интеграция с плагинами

Переработана архитектура

Поддержана только ОС Windows

Новый интерфейс ViPNet CSP 5





А если мне нужно решение под Linux?

Чем заменить ViPNet CSP

Разработчик

ViPNet OSSL

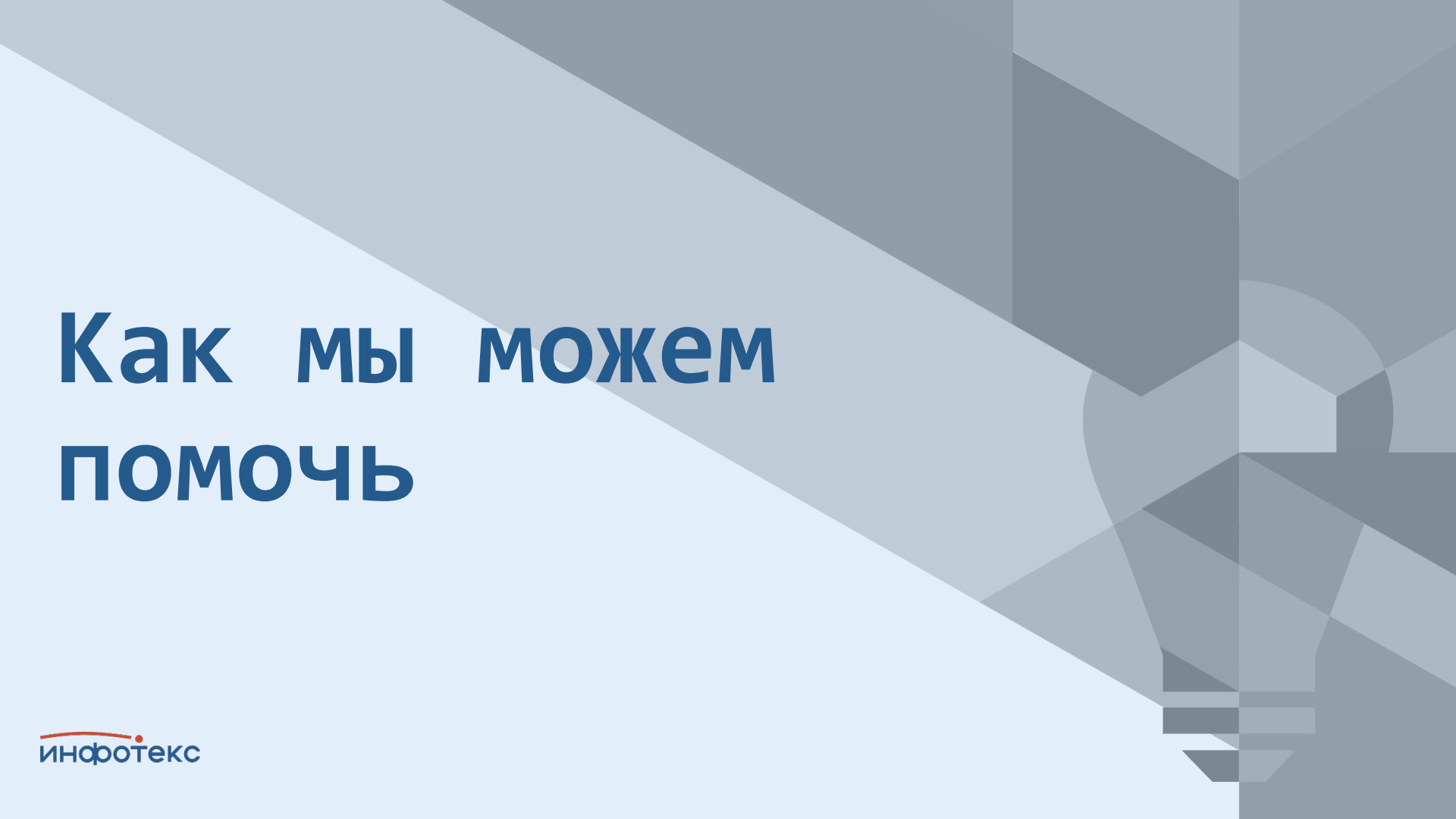
Пользователь

ViPNet PKI Client

Библиотеки ИнфоТеКС

ViPNet CSP	ViPNet OSSL	ViPNet JCrypto SDK	ViPNet CryptoSmart
Платформы	Платформы	Платформы	Платформы
Интерфейсы: MS CryptoAPI	Интерфейсы: PKCS#11, OpenSSL	Интерфейсы: JNI/JCA, PKCS#11	Интерфейсы: MSP, NetCSP, BCCSP Lite
Класс защиты: КС1-КС3	Класс защиты: КС1-КС3	Класс защиты: КС1	Класс защиты: КС1, КС2
Сертификат ФСБ России: да	Сертификат ФСБ России: да	Сертификат ФСБ России: да	Сертификат ФСБ России: да

Как мы можем помочь



инфотекс

Подробная документация и примеры кода

Руководство администратора

Информация об установке и настройке для работы со сторонним ПО

Руководство разработчика

Сведения о разработке с помощью библиотек

Справочник функций

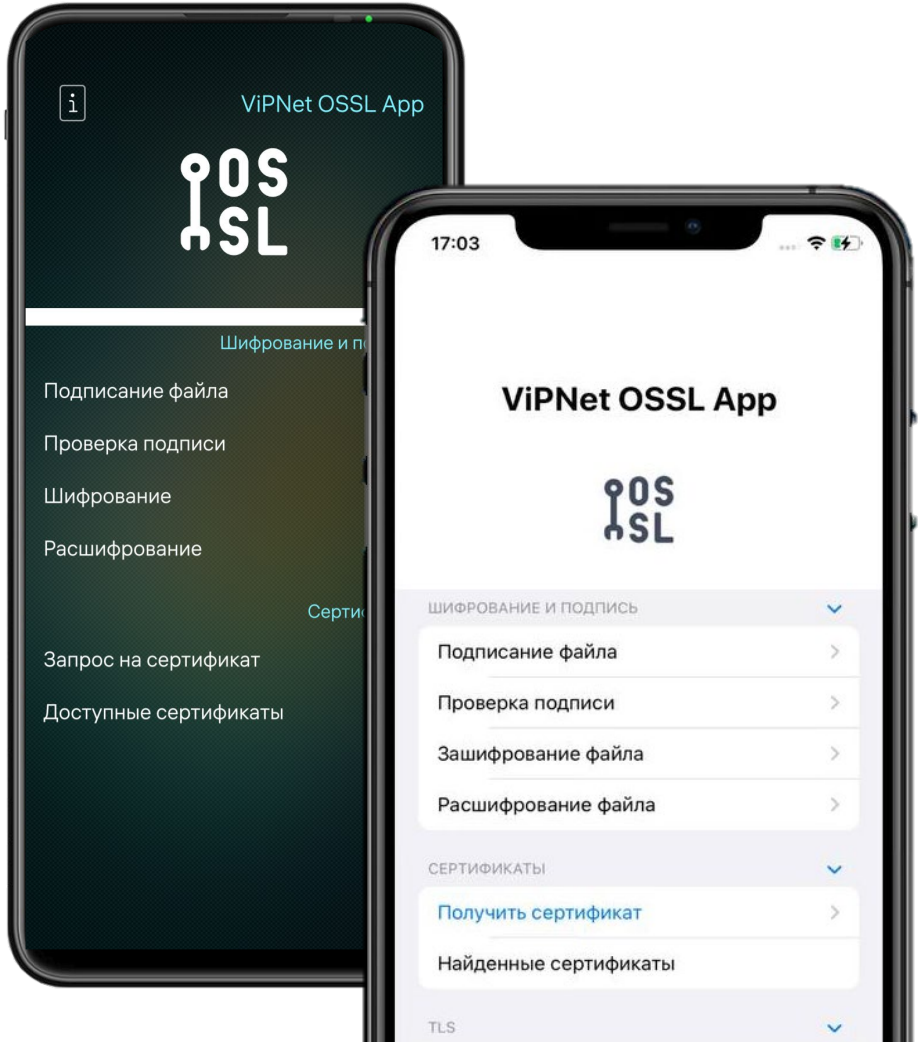
Описание функций и их параметров

Примеры

Примеры кода с обращением к перечисленным функциям

Оценка влияния

Приходите в нашу лабораторию



Приходите на стенд!

Вживую посмотреть на возможную **реализацию встраивания криптобиблиотек** в пользовательские приложения на мобильных ОС

Как с нами связаться

Купить или взять на тесты:
soft@infotecs.ru

Есть идея реализации совместного решения:
techpartners@infotecs.ru

САНКТ ПЕТЕРБУРГ

инфотекс
ТЕХНОФЕСТ

Подписывайтесь
на наши соцсети

инфотекс Академия · Учебный центр инфотекс · AMPIRE · TELEOFIS · КОМФОРТЕЛ · РУТОКЕН · TS Solution · AXOFT