
ТЕХНО 2019 infotecs ФЕСТ
ТЕХНИЧЕСКАЯ КОНФЕРЕНЦИЯ
12 09 2019
Криптографические библиотеки ИнфоТеКС

Криптокомпоненты

ViPNet OEM Crypto - криптографические библиотеки для встраивания сторонними разработчиками.

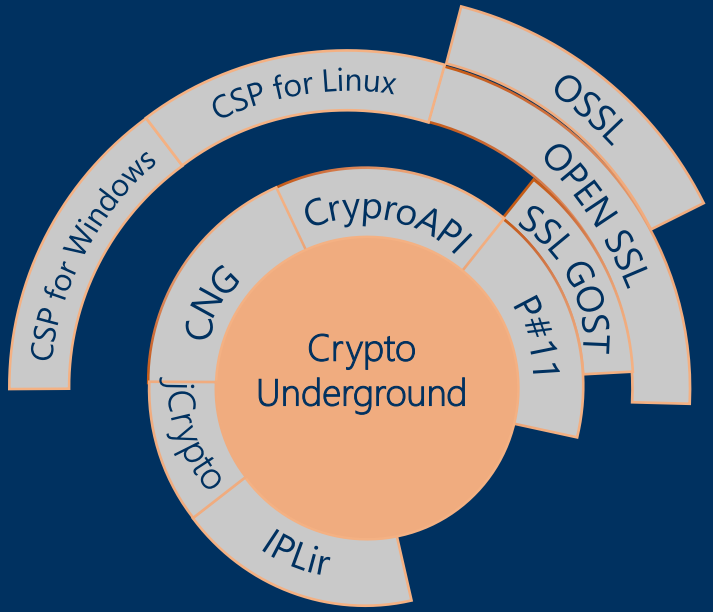
- Выполнение криптографических операций:
  - шифрование,
  - хэширование,
  - формирование/проверка ЭП;
- Организация TLS-соединений;
- Реализация актуальных криптографических ГОСТов и методических рекомендаций ТК 26.

ViPNet OEM Crypto

- Стандартизированные интерфейсы: PKCS#11, OpenSSL, Microsoft CryptoAPI, Microsoft CNG;
- Библиотека для приложений на Java;
- Операционные системы: Windows, Linux, Android, iOS, Sailfish Mobile OS;
- специальные варианты для архитектур процессора “Байкал” и “Эльбрус”;
- расширенный SDK: подробные руководства, примеры использования, утилиты и т.д.

ViPNet OEM Crypto

- **ViPNet CryptoUnderground** – криптографическое ядро;
- **ViPNet SoftToken** – программная реализация PKCS #11 и его расширения;
- **ViPNet OSSL** – реализация алгоритмов ГОСТ на базе библиотеки OpenSSL;
- **ViPNet CSP** – криптопровайдер для ПО с интерфейсом MS CryptoAPI, CNG, CSP;
- **ViPNet CSP Linux** – портирование MS CryptoAPI, CNG, CSP под Linux;
- **ViPNet JCrypto SDK** - криптопровайдер для Java-машин с интерфейсом JCA.



Сертифицированные продукты

ViPNet CSP 4.2

- КС1, КС2, КС3 – под Windows; КС1, КС2 – под Linux;
- Генерация ключей ЭП, формирование и проверка ЭП по ГОСТ Р 34.10-2001/2012;
- Хэширование данных по ГОСТ Р 34.11-2012;
- Шифрование и имитозащита данных по ГОСТ 28147-89;
- Генерация псевдослучайных последовательностей;
- Поддержка сертифицированных аппаратных токенов;
- Создание и проверка ЭП в форматах CAdES-BES, CAdES-T.

ФЕДЕРАЛЬНАЯ СЛУЖБА БЕЗОПАСНОСТИ
РОССИЙСКОЙ ФЕДЕРАЦИИ

Система сертификации РОСС RU.0001.030001

СЕРТИФИКАТ СООТВЕТСТВИЯ

Регистрационный номер СФ/124-3561 от "14" декабря 2018 г.

Действителен до "14" декабря 2021 г.

Выдан Открытому акционерному обществу «Информационные технологии и коммуникационные системы» (ОАО «ИнфоТеКС»)

Настоящий сертификат удостоверяет, что средство криптографической защиты информации ViPNet CSP 4.2 (варианты исполнения 4, 5) в комплектации согласно формуляру ФРКЕ.00106-04 30 01 ФО

соответствует Требованиям к средствам криптографической защиты информации, предназначенным для защиты информации, не содержащей сведений, составляющих государственную тайну, классам КС1 (для варианта исполнения 4), КС2 (для варианта исполнения 5). Требованиям к средствам электронной подписи, утверждённым приказом ФСБ России от 27 декабря 2011 г. № 796, установленным для классов КС1 (для варианта исполнения 4), КС2 (для варианта исполнения 5) 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, реализация функций электронной подписи в соответствии с Федеральным законом от 6 апреля 2011 г. № 63-ФЗ «Об электронной подписи»: 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 ОАО «ИнфоТеКС»
сертификационных испытаний образца продукции № 6374.7-000301.

Безопасность информации обеспечивается при использовании средства в соответствии с требованиями эксплуатационной документации согласно формуляру ФРКЕ.00106-91 30 01 ФО.

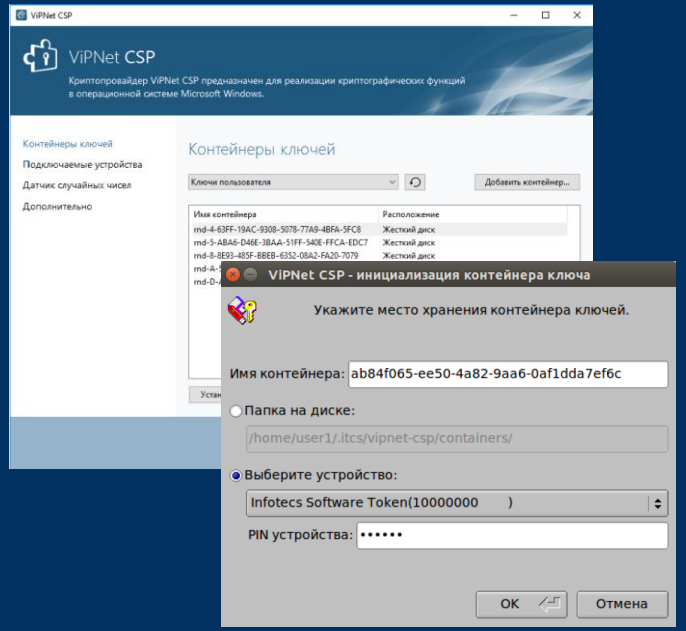
Заместитель руководителя Научно-технической службы – начальник Центра защиты информации и специальной связи ФСБ России А.М. Ивашко

Настоящий сертификат внесён в Государственный реестр сертифицированных средств защиты информации 14 декабря 2018 г.

Заместитель начальника Центра по лицензированию, сертификации и защите государственной тайны ФСБ России А.В. Парфенов

ViPNet CSP 4.4

- Подан на сертификацию по классам КС1, КС2, КС3;
- Поддержка работы в режиме замкнутой программной среды в дистрибутивах Linux;
- Поддержка новых рекомендаций ТК26:
  - Изменение схемы защиты ключа (PBKDF2),
  - Поддержка “кривых Эдвардса”;
- Поддержка внешних устройств новых типов;
- Поддержка последних сборок Windows 10;
- Поддержка алгоритмов экспорта и импорта ключей, в т.ч. PKCS#12 (PFX).



ViPNet OSSL

- Генерация ключей ЭП, формирование и проверка ЭП по ГОСТ Р 34.10-2001/2012;
- Хэширование данных по ГОСТ Р 34.11-2012;
- Шифрование и имитозащита данных по ГОСТ 28147-89, ГОСТ 34.12 -2018, ГОСТ 34.13-2018 (алгоритмы «Магма» и «Кузнечик»);
- Создание защищенного соединения по протоколу TLS 1.2;
- Реализована схема разделения секрета Шамира;
- Работа с электронными ключами на внешних устройствах;
- Создание и проверка ЭП в форматах вплоть до CAdES X Long Type 2 .

ViPNet OSSL

ТЕХНО infotecs 2019 ФЕСТ

2019

- Включает в себя ViPNet SoftToken;
- Подача на сертификацию как СКЗИ по классам КС1, КС2, КС3;
- Лицензия клиентская и серверная;
- Исполнения под Windows, Linux, macOS, iOS, Android, Sailfish Mobile OS;

2020

- TLS 1.3;
- Новая спецификация XMLDSig;
- Сертификация ViPNet JCrypto SDK.

Правовые вопросы

Вопросы применения

ТЕХНО 2019 infotecs ФЕСТ

ПП РФ №313

Лицензирование деятельности

Оценка влияния

ПКЗ-2005

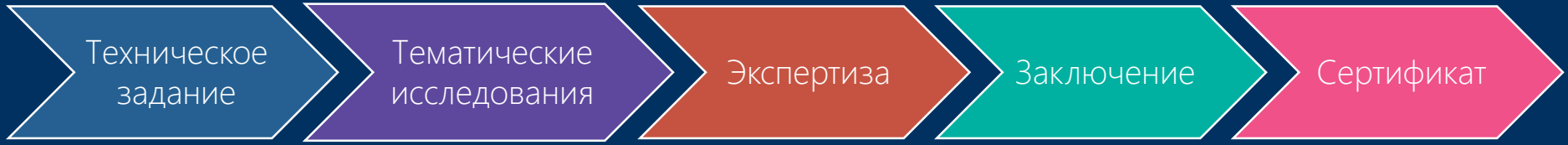
Сертификация

Распространение

Сценарии работы

- Использование готового СКЗИ;
- Доработка прикладного ПО партнера;
- Доработка библиотек/СКЗИ;
- Создание совместного решения и его сертификация при необходимости;
- Лицензионный договор.

Порядок сертификации



Примеры проектов

IDPoint

Мобильное приложение для дистанционного формирования ЭП в защищённой среде.

- Создание и хранение ключей усиленной квалифицированной электронной подписи;
- Установление одно- и двухстороннего TLS;
- Использование ключей для подписания пакетов документов;
- Использование ключей для выработки симметричного ключа защиты контейнера.

Остались вопросы?

Напишите нам!

E-mail: techpartners@infotecs.ru
Ляшенко Анастасия
Anastasia.Lyashenko@infotecs.ru
+7 (495) 737 – 61 – 92 (4368)

ТЕХНО 2019 infotecs Фест

Спасибо
за внимание!