ViPNet HSM

Бадмаева Римма
Ведущий менеджер продуктов

Что такое HSM?

ТехноФест infotecs 2022

≈

Функциональные возможности

Электронная подпись и проверка подписи

Создание ключей (симметричных, асимметричных)

Шифрование, имитозащита данных

Надежное хранение секретных ключей и данных пользователей

Характеристики

- Криптоалгоритмы: ГОСТ 28147-89, ГОСТ 34.12-2018, ГОСТ 34.13-2018, ГОСТ Р 34.10-2001, ГОСТ Р 34.10-2012, ГОСТ Р 34.11-2012
  - RSA, ECDSA, AES и др NIST алгоритмы
- SDK для Windows/Linux для разработки прикладных сервисов
- Криптографический интерфейс PKCS#11
- WEB-консоль удаленного управления под защитой ГОСТ TLS
- Допускает встраивание прикладных сервисов

Меры защиты

- Ролевая модель, обеспечивающая защиту от злонамеренных действий одного администратора: схема разделение секрета (нет суперпользователя), сбор кворума для выполнения критичных операций

- Физические меры защиты: встроенный аппаратный модуль обнаруживает вскрытие корпуса, хранит и гарантированно уничтожает ключи.

Сертифицирован в ФСБ

- СКЗИ по классу КВ
- Средство ЭП по классу КВ2
- Зарегистрирован в Реестре российского ПО

ФЕДЕРАЛЬНАЯ СЛУЖБА БЕЗОПАСНОСТИ
РОССИЙСКОЙ ФЕДЕРАЦИИ

Система сертификации РОСС RU.0001.030001

СЕРТИФИКАТ СООТВЕТСТВИЯ

Регистрационный номер *СФ/124-3747* от "*04*" *сентября* 2019 г.

Действителен до "*04*" *сентября* 2022 г.

Выдан Открытому акционерному обществу «Информационные технологии и коммуникационные системы» (ОАО «ИнфоТеКС»),
Обществу с ограниченной ответственностью «Линия защиты» (ООО «Линза»).

Настоящий сертификат удостоверяет, что программно-аппаратный комплекс **ViPNet HSM** (вариант исполнения 6) в комплектации согласно формуляру ФРКЕ.00127-01 30 01 ФО

соответствует Требованиям к средствам криптографической защиты информации, предназначенным для защиты информации, не содержащей сведений, составляющих государственную тайну, класса КВ, Требованиям к средствам электронной подписи, утверждённым приказом ФСБ России от 27 декабря 2011 г. № 796, установленным для класса КВ2, 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, 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 № 818Е-001001.

Безопасность информации обеспечивается при использовании комплекса, изготовленного в соответствии с техническими условиями ФРКЕ.00127-01 97 01 ТУ, и выполнении требований эксплуатационной документации согласно формуляру ФРКЕ.00127-01 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 4 сентября 2019 г.

Первый заместитель начальника Центра по лицензированию, сертификации и защите государственной тайны ФСБ России В.Н. Мартынов

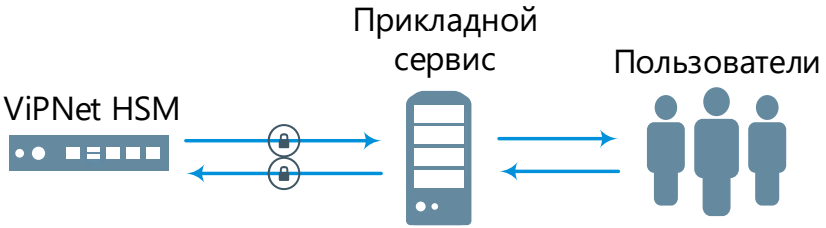
ТЕХНО infotecs 2022 ФЕСТ

Разработка прикладных сервисов

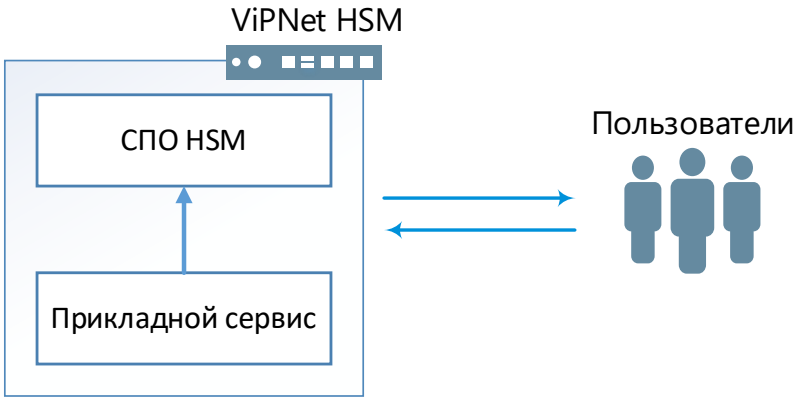
ViPNet HSM: внешний прикладной сервис

Основные преимущества:

- Независимость при разработке
- Изолированность решения
- Возможность использования различных ОС и платформ разработки



ViPNet HSM: внутренний прикладной сервис



Основные преимущества:

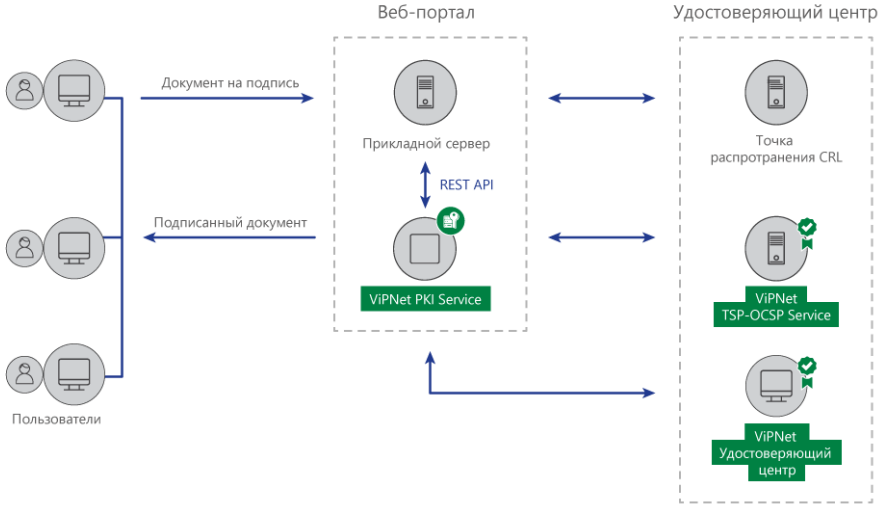
- Проще достичь классов КВ/КВ2
- Запуск и контроль функционирования ПС
- Сброс к заводскому состоянию
- Экспорт/импорт данных ПС
- Резервное копирование

Например: *ViPNet PKI Service*

PKI Service

ViPNet PKI Service: функциональные возможности

- Централизованное хранение и генерация ключей
- Выполнение функций создания и проверки ЭП по запросу АИС и пользователей АИС
- Шифрование и расшифрование данных
- Интерфейс для взаимодействия с информационными системами – REST API



Форматы подписи и новые возможности

Сертифицировано
PKI Service 1.0

- CMS
- CAdES(-BES)(-T)
- XMLDSig

Реализовано
PKI Service 2.0

- CAdES X Long Type 1
- Расширена ролевая модель
- Подтверждение операций
- Увеличен размер обрабатываемых файлов
- Кластер

В разработке
PKI Service 2.x

- XAdES(-BES)(-T)
- Дистанционная подпись*
- Визуализация подписываемых документов

*Требования к дистанционной подписи еще не утверждены

ViPNet PKI Service: функциональные возможности

- Взаимодействие с другими компонентами PKI: УЦ, TSA, OCSP, CDP
- Лицензирование:
  - ✓ По количеству пользователей
  - ✓ По количеству сертификатов
- Для разработчиков: есть эмулятор в виде VA
- Сертифицирован по классу КВ/КВ2, зарегистрирован в Реестре российского ПО

ФЕДЕРАЛЬНАЯ СЛУЖБА БЕЗОПАСНОСТИ
РОССИЙСКОЙ ФЕДЕРАЦИИ

Система сертификации РОСС RU.0001.030001

СЕРТИФИКАТ СООТВЕТСТВИЯ

Регистрационный номер *СФ/124-3743* от "*04*" *сентября* 2019 г.

Действителен до "*04*" *сентября* 2022 г.

Выдан Открытому акционерному обществу «Информационные технологии и коммуникационные системы» (ОАО «ИнфоТеКС»),
Обществу с ограниченной ответственностью «Линия защиты» (ООО «Линза»).

Настоящий сертификат удостоверяет, что программно-аппаратный комплекс **ViPNet PKI Service** (на аппаратной платформе HSM 2000Q2) в комплектации согласно формуляру ФРКЕ.00184-01 30 01 ФО

соответствует Требованиям к средствам криптографической защиты информации, предназначенным для защиты информации, не содержащей сведений, составляющих государственную тайну, класса КВ, Требованиям к средствам электронной подписи, утверждённым приказом ФСБ России от 27 декабря 2011 г. № 796, установленным для класса КВ2, 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, 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 № 905S-000502.

Безопасность информации обеспечивается при использовании комплекса, изготовленного в соответствии с техническими условиями ФРКЕ.00184-01 97 01 ТУ, и выполнении требований эксплуатационной документации согласно формуляру ФРКЕ.00184-01 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 4 сентября 2019 г.

Первый заместитель начальника Центра по лицензированию, сертификации и защите государственной тайны ФСБ России В.Н. Мартынов

Спасибо за внимание!

Бадмаева Римма

e-mail: Rimma.Badmaeva@infotecs.ru

Подписывайтесь на наши соцсети

https://vk.com/infotecs_news

https://t.me/infotecs_news