конференция РусКрипто

infotecs

Проблемы внедрения отечественных СКЗИ в платежных системах

Александр Поташников
Зам. директора Центра Разработок ОАО «ИнфоТеКС»
potashnikov@infotecs.ru

ViPNet HSM

Функциональные возможности

- Электронная подпись данных
- Проверка электронной подписи
- Генерация ключей (симметричных, асимметричных)
- Шифрование, имитозащита (выработка контрольных сумм)
- Надежное хранение секретных ключей и данных пользователей

ViPNet HSM

Повышенные меры защиты

- Имеет встроенный модуль обнаружения вскрытия и контроля основных параметров работы платформы, хранения и гарантированного уничтожения мастер-ключей
- Разделение «секрета», сбор кворума для выполнения критических операций
- Развитая ролевая модель
- Физический датчик случайных чисел

ViPNet HSM PS

Функциональные возможности

- Обработка банковских транзакций электронных платёжных систем.
- Поддержка необходимых режимов для эмиссии карт (генерация секретных величин и электрическая персонализация) .
- Поддержка режимов, необходимых для обеспечения межбанковского взаимодействия.
- Генерация ключей для обеспечения работы терминальной сети
- Генерация и печать паролей, ключей и ПИН-конвертов владельцев карт.

ViPNet HSM PS

Протоколы и совместимость

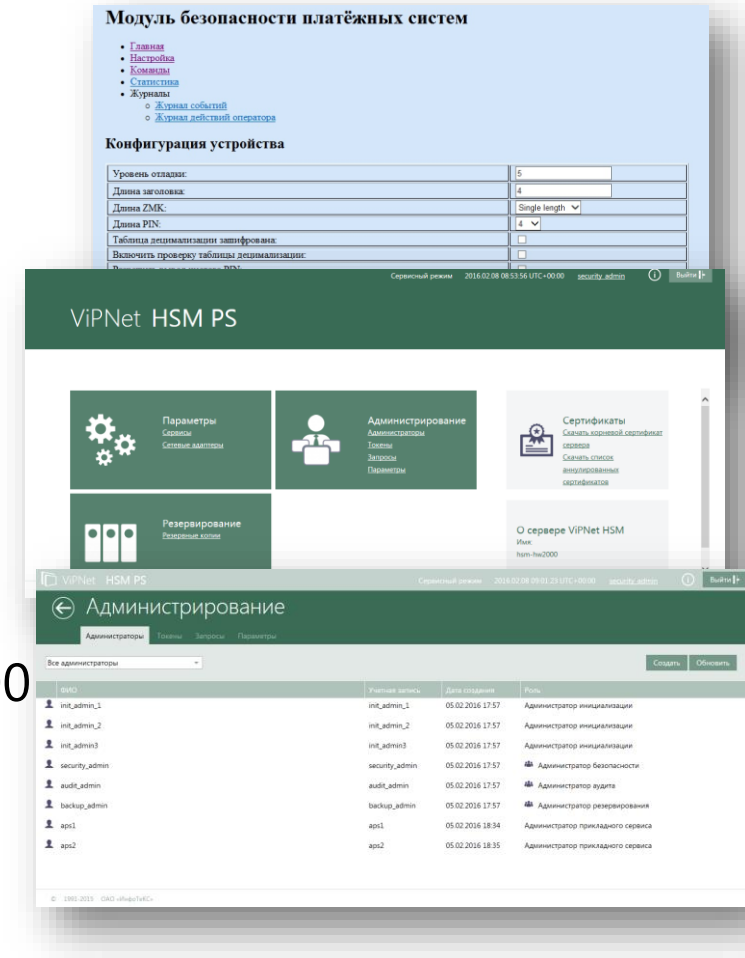
- Поддержка протоколов Visa и Mastercard, China Union Pay, American Express, МИР.
- Система команд и протоколы взаимодействия ViPNet HSM PS соответствуют реализованным в HSM Thales PayShield 9000 при работе в режиме совместимости с международными платёжными системами.
- Имеет дополнительную систему команд с отечественными криптографическими алгоритмами для обеспечения перехода к картам и протоколам с отечественными криптоалгоритмами.

ТК 26 ГОСТР

ViPNet HSM PS

Специфика

- Дополнительно реализованы криптоалгоритмы DES, TripleDES, AES, RSA, SHA-1, SHA-256.
- Раздельное лицензирование функциональности:
  - Процессинг
  - Режим Удостоверяющего центра
  - Поддержка 3D-Secure
  - Печать ПИН-конвертов
  - Предперсонализация карт
  - Персонализация карт
- В режиме проверки PIN PVV/CVV - 4000 транзакций в секунду.
- Дополнительная WEB-консоль для управления платежными сервисами.

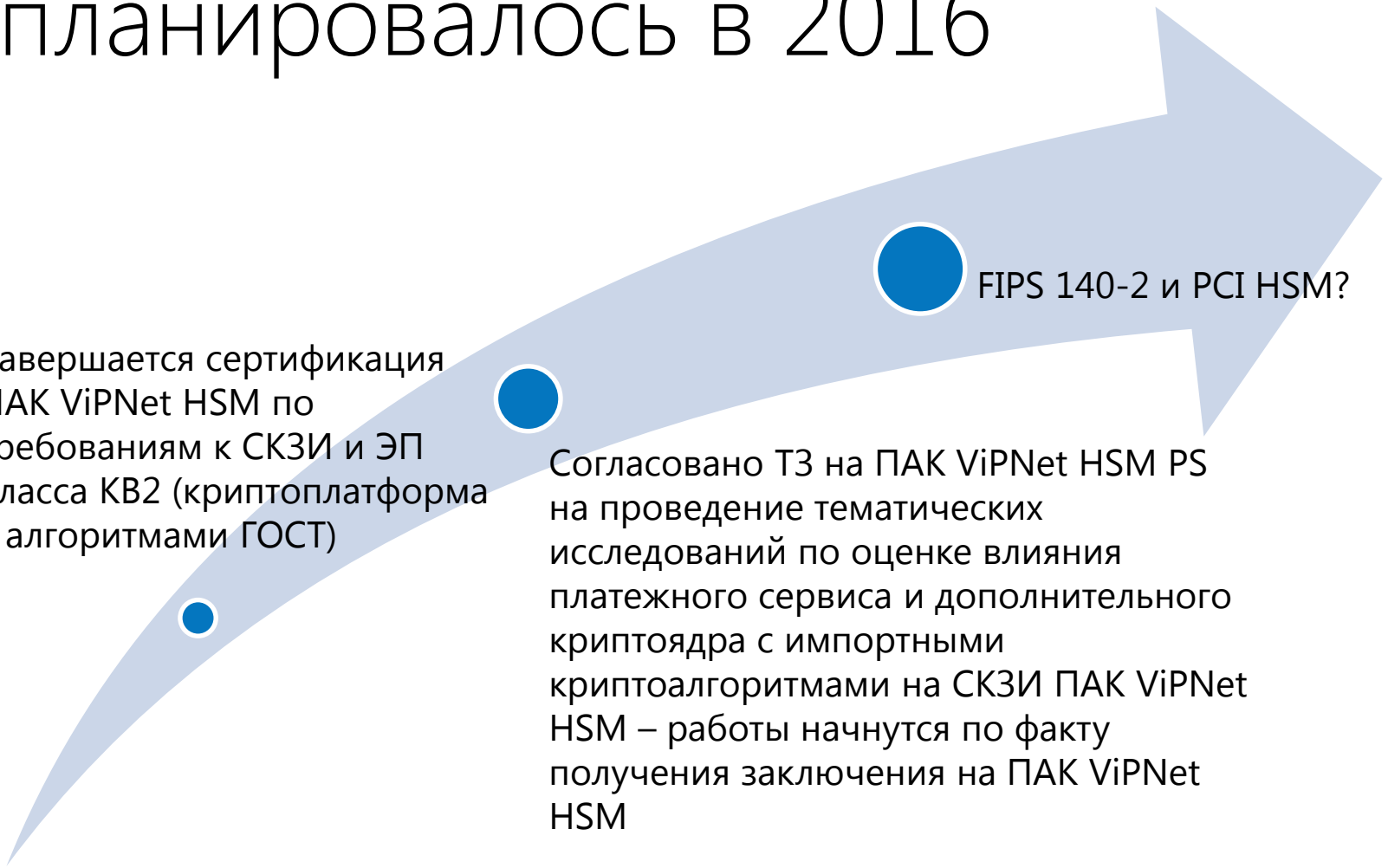


ViPNet HSM PS

Тестирование

- По итогам тестирования в OpenWay в 2016г. ViPNet HSM PS включен в перечень рекомендованных устройств, поддерживаемых коммуникационными серверами NetServer и Transaction Switch Системы WAY4
- В НСПК разработаны ПМИ на HSM для головного удостоверяющего центра НСПК и на соответствие функциональным требованиям, предъявляемым ПС «Мир» к платежным HSM, выбрана лаборатория для проведения функционального тестирования.
- Завершен второй цикл тестирования на площадке Сбербанка/Сбертеха – подтверждена техническая возможность использования изделия как для online операций в АС Way4/SmartVista, так и для выпуска карт.
- Проведено тестирование в АКБ «Россия»
- Стартовал цикл тестирования в компании Compass Plus на совместимость с TranzWare Online.

Сертификация планировалось в 2016



Завершается сертификация ПАК ViPNet HSM по требованиям к СКЗИ и ЭП класса КВ2 (криптоплатформа с алгоритмами ГОСТ)

Согласовано ТЗ на ПАК ViPNet HSM PS на проведение тематических исследований по оценке влияния платежного сервиса и дополнительного криптоядра с импортными криптоалгоритмами на СКЗИ ПАК ViPNet HSM – работы начнутся по факту получения заключения на ПАК ViPNet HSM

FIPS 140-2 и PCI HSM?

ФЕДЕРАЛЬНАЯ СЛУЖБА БЕЗОПАСНОСТИ
РОССИЙСКОЙ ФЕДЕРАЦИИ

Система сертификации РОСС RU.0001.030001

СЕРТИФИКАТ СООТВЕТСТВИЯ

Регистрационный номер *СФ/124-3071* от "*28*" *февраля* 2017 г.

Действителен до "*31*" *декабря* 2018 г.

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

Настоящий сертификат удостоверяет, что программно-аппаратный комплекс ViP… исполнения 1) в комплектации согласно формуляру ФРКЕ.00127-01 30 01 ФО

соответствует требованиям ГОСТ 28147-89, ГОСТ Р 34.11-94, ГО… ГОСТ Р 34.11-2012, Требованиям к средствам криптографичес… для защиты информации, не содержащей сведений, сост… Требованиям к средствам электронной подписи, ут… 2011 г. № 796, установленным для класса КВ2, … защиты (создание и управление ключевой информ… …одержащихся в областях оперативной памяти, вычислени… …содержащихся в областях оперативной памяти, вычисление знач… …анных, содержащихся в областях оперативной памяти, защита TLS-с… …и электронной подписи в соответствии с Федеральным законом от 6 апр… …электронной подписи», создание электронной подписи, проверка электрон… …ча электронной подписи, создание ключа проверки электронной подписи) инф… …ей сведений, составляющих государственную тайну.

Сертификат выдан н… …ультатов проведенных … ОАО «ИнфоТеКС»
сертификационны… …разца продукции … № 818А-001001.

Безопасност… …ации обеспечивается при использовании комплекса в соответствии с требования… …ционной документацией согласно формуляру ФРКЕ.00127-01 30 01 ФО.

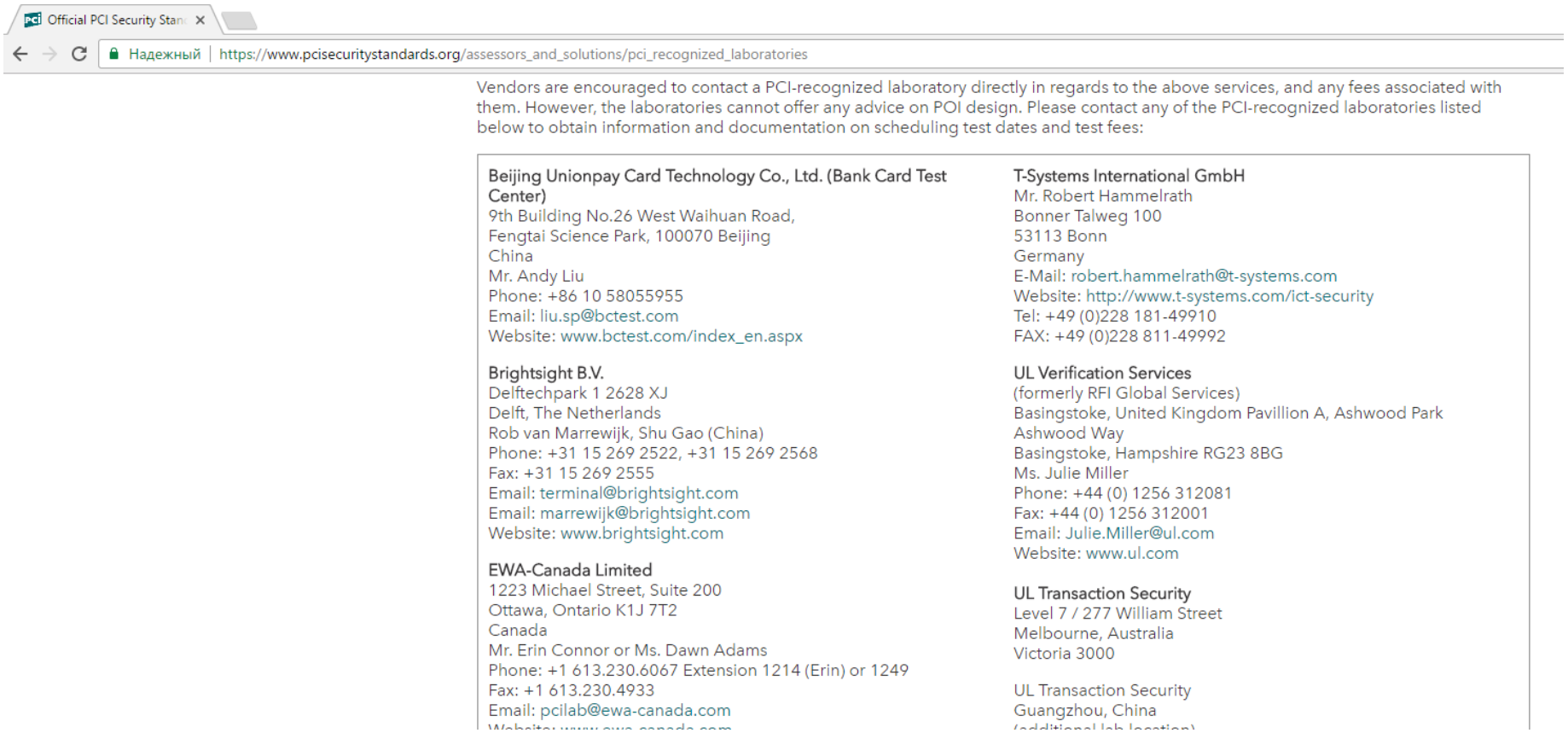
…ь руководителя Научно-технической службы – начальник Центра защиты информации и специальной связи ФСБ России А.М. Ивашко

ViPNet HSM PS
Завершены ТИ
ПАК подготовка заключения

FIPS 140-2 и PCI HSM?

ПАК ViPNet HSM
сертифицирован
по требованиям к
СКЗИ и ЭП класса
КВ

Авторизованные лаборатории



https://www.pcisecuritystandards.org/assessors_and_solutions/pci_recognized_laboratories

PCI PTS/HSM аккредитация лаборатории

- ✓ Подписать с Советом PCI SSC документы: NDA и Соглашение об отсутствии конфликтов интересов.
- ✓ Получить от Совета PCI SSC документы, включая перечень требований к лаборатории и ее оборудованию.
- Подтвердить наличие оборудования и выполнение иных требований.
- Выполнить пробную сертификацию одного устройства.
- Пройти он-сайт аудит лаборатории.

Информация предоставлена компанией **Deiteriy www.deiteriy.com**

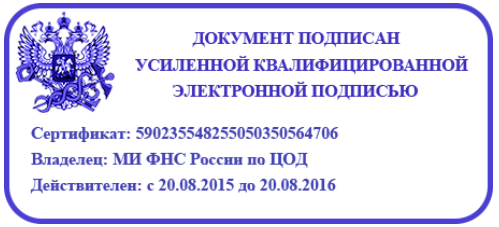
Применение СКЗИ в банках

- Платежные системы, процессинг и эмиссия карт

- Дистанционное банковское обслуживание, аутентификация пользователей

- Документооборот, электронная подпись

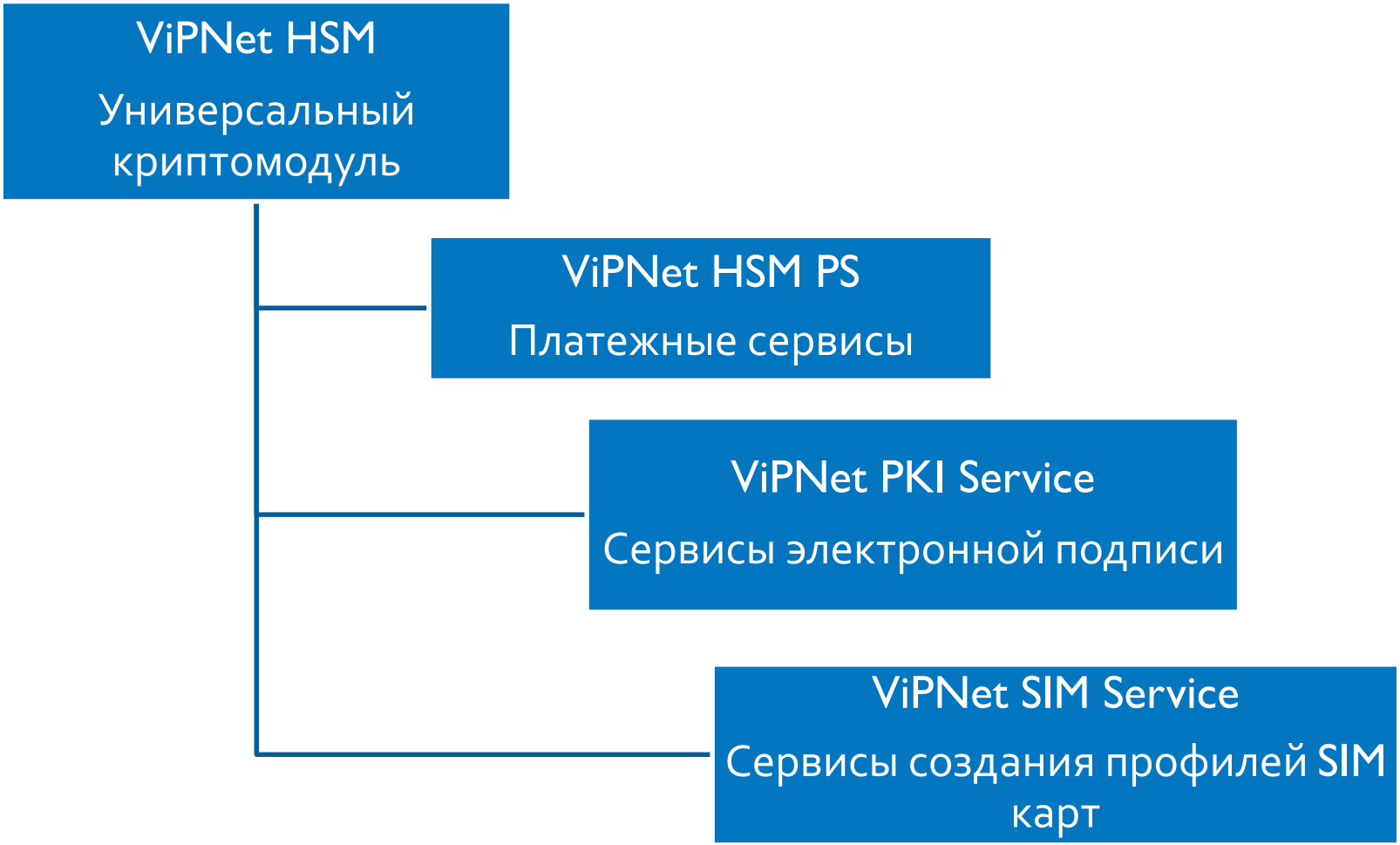
- Дополнительные услуги, требующие применения квалифицированной электронной подписи пользователей



ViPNet HSM

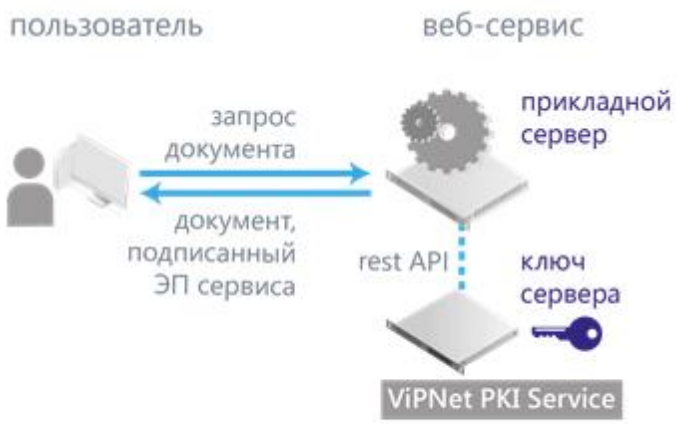
Подключение прикладных сервисов

Платформа ViPNet HSM



ViPNet PKI Service

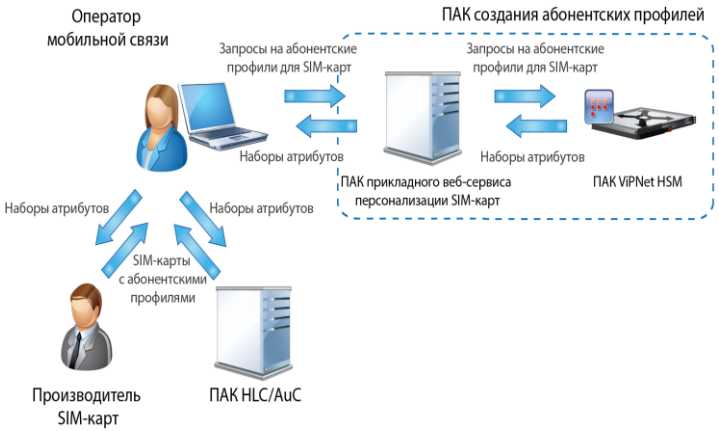
- Выполнение криптографических функций (создание и проверка ЭП, генерация ключей ЭП, шифрование/расшифрование данных, хэширование, формирование имитовставки).
- Возможность встраивания в информационные системы (наличие REST API).
- Ролевая модель и управление учетными записями пользователей.
- Взаимодействие с компонентами PKI: с УЦ (pkcs#10), TSP (RFC 3161), OCSP (RFC 2560), CDP.



- Поддержка криптоалгоритмов ГОСТ Р 34.10 2001/2012, ГОСТ Р 34.11 94/2012, ГОСТ 2814789.
- Поддержка форматов подписи: PKCS#7 (CMS), XMLDSig, CAdESBES.
- Возможность удаленного администрирования через веб-интерфейс

ViPNet HSM SIM Service

Предназначен для создания абонентских профилей, содержащих наборы уникальных атрибутов для записи на SIM-карты*: IMSI, ICCID, PIN1, PIN2, PUK1, PUK2, ключ аутентификации абонента (KI), ADM-ключи, OTA-ключи (KIC, KID, KIK).



ПАК позволяет создавать абонентские профили, в двух форматах:

- Для записи на SIM карту
- Для загрузки в программно-аппаратные комплексы домашнего регистратора местонахождения (HLR) и центра аутентификации абонентов (AuC).

Поддержка конкретных моделей SIM-карт и оборудования реализуется на заказ.

infotecs

Спасибо за внимание!
Вопросы?

Поташников Александр
potashnikov@infotecs.ru