ViPNet HSM-универсальный криптографический модуль и платформа для разработки криптографических сервисов

Бадмаева Римма
Ведущий менеджер продуктов

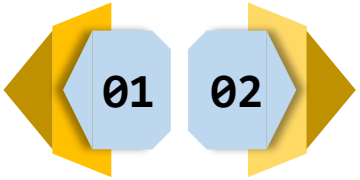
ТехноФест 2023 infotecs

Что такое HSM?

=

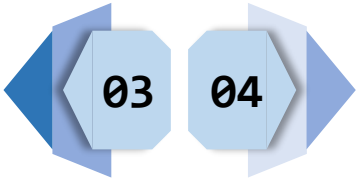
ViPNet HSM

Программно-аппаратный модуль (HSM – Hardware Secure Module)



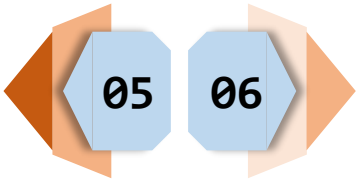
Выполняет криптографические операции по запросам различных сервисов («большой токен»)

Повышенные меры безопасности



Поддержка актуальных криптоалгоритмов

СКЗИ класса КВ



Средство ЭП класса КВ2

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

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

Сертифицирован в ФСБ

ФЕДЕРАЛЬНАЯ СЛУЖБА БЕЗОПАСНОСТИ
РОССИЙСКОЙ ФЕДЕРАЦИИ

Система сертификации РОСС RU.0001.030001

СЕРТИФИКАТ СООТВЕТСТВИЯ

Регистрационный номер *СФ/124-4330* от "*29*" *августа* 2022 г.

Действителен до "*01*" *июня* 2024 г.

Выдан Акционерному обществу «Информационные технологии и коммуникационные системы», Обществу с ограниченной ответственностью «Линия защиты».

Настоящий сертификат удостоверяет, что программно-аппаратный комплекс **ViPNet HSM** (вариант исполнения 6) и 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, 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 Акционерным обществом «Информационные технологии и коммуникационные системы»

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.

Временно исполняющий обязанности начальника Центра защиты информации и специальной связи ФСБ России **И.Ф. Качалин**

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

ТЕХНО infotecs 2023 ФЕСТ

Разработка прикладных сервисов

ViPNet HSM: внешний прикладной сервис

Основные преимущества:

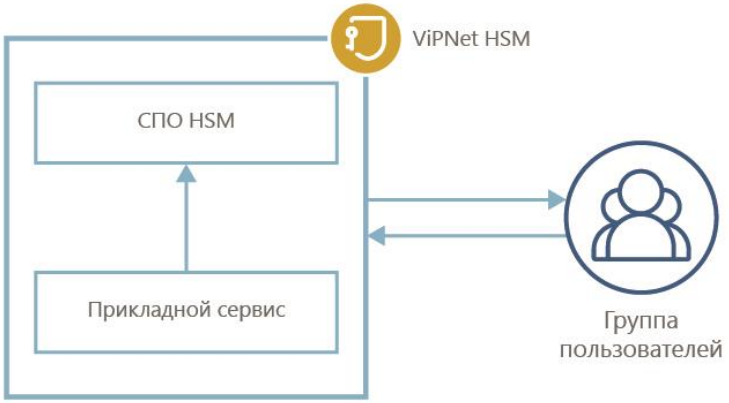
- Независимость при разработке
- Изолированность решения
- Возможность использования различных ОС и платформ разработки

Пример: УЦ КС3+

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

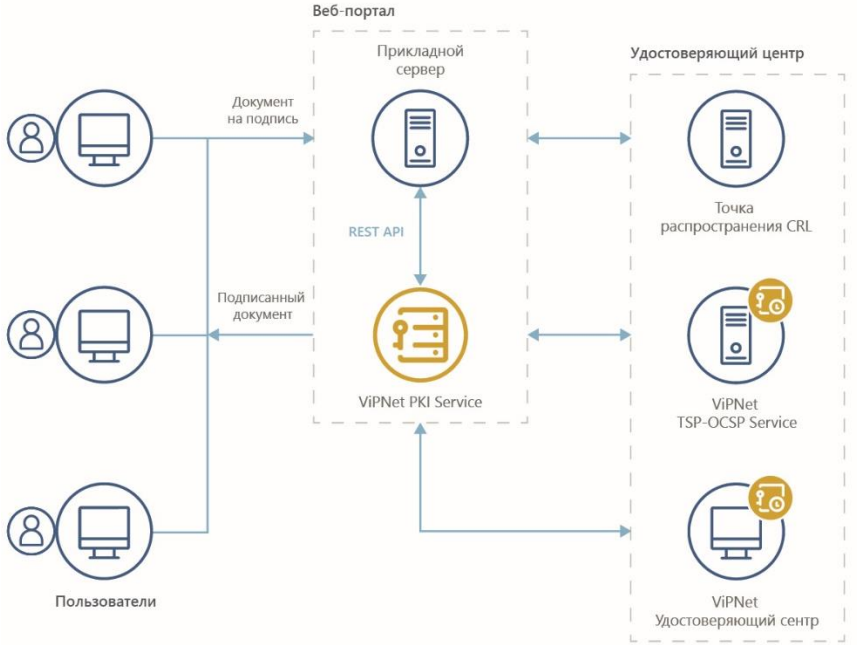


Например: ViPNet PKI Service

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: ViPNet УЦ, КриптоПРО УЦ
- поддержка меток времени
- возможность проверки статусов сертификатов по протоколу OCSP
- поддержание CRL в актуальном состоянии

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/124-4328* от "*29*" *августа* 2022 г.

Действителен до "*01*" *июня* 2024 г.

Выдан Акционерному обществу «Информационные технологии и коммуникационные системы». Обществу с ограниченной ответственностью «Линия защиты».

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

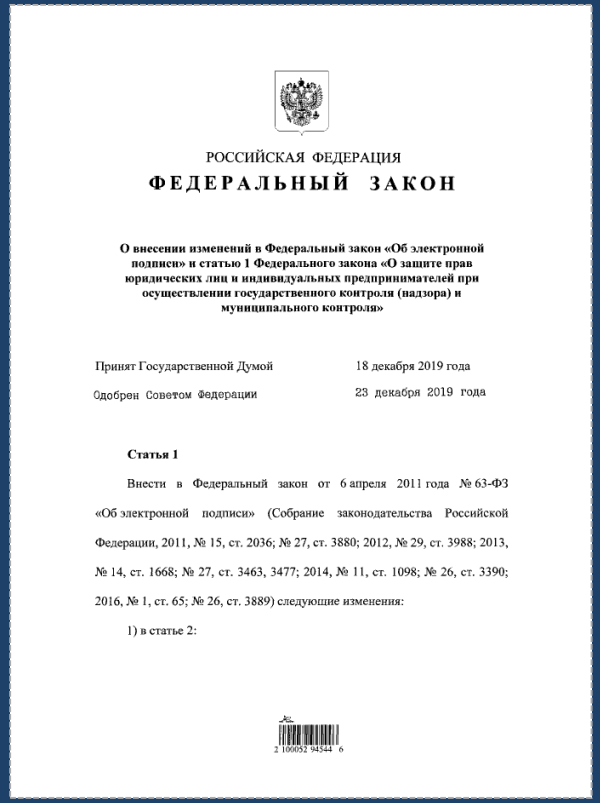
соответствует Требованиям к средствам криптографической защиты информации, предназначенным для защиты информации, не содержащей сведений, составляющих государственную тайну, класса КВ, Требованиям к средствам электронной подписи, утверждённым приказом ФСБ России от 27 декабря 2011 г. № 796, установленным 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, 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 Акционерным обществом «Информационные технологии и коммуникационные системы» сертификационных испытаний образца продукции № 9058-000502.

Безопасность информации обеспечивается при использовании комплексов, 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.

Временно исполняющий обязанности начальника Центра защиты информации и специальной связи ФСБ России — И.Ф. Качалин

Использование HSM на примере реализации требований 171 приказа ФСБ России



РОССИЙСКАЯ ФЕДЕРАЦИЯ

ФЕДЕРАЛЬНЫЙ ЗАКОН

О внесении изменений в Федеральный закон «Об электронной подписи» и статью 1 Федерального закона «О защите прав юридических лиц и индивидуальных предпринимателей при осуществлении государственного контроля (надзора) и муниципального контроля»

Принят Государственной Думой 18 декабря 2019 года

Одобрен Советом Федерации 23 декабря 2019 года

Статья 1

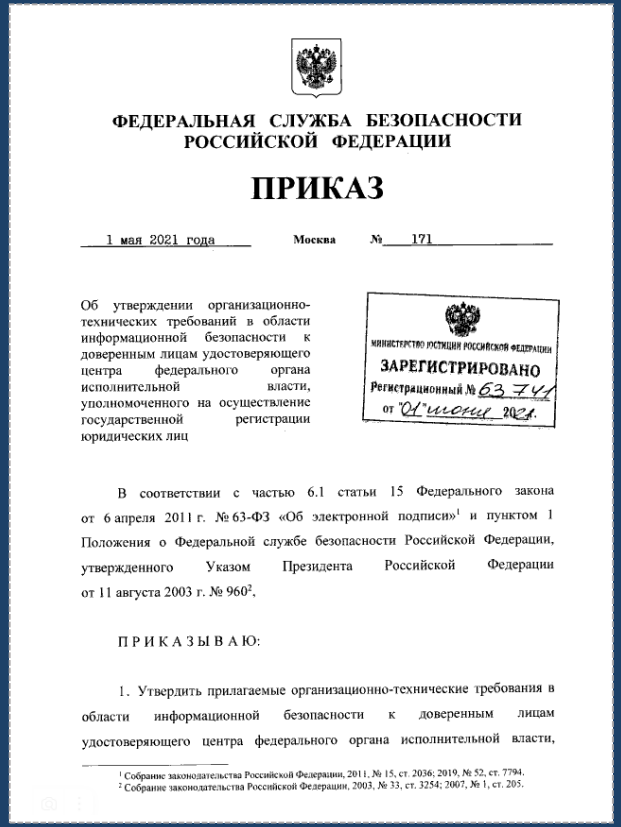
Внести в Федеральный закон от 6 апреля 2011 года № 63-ФЗ «Об электронной подписи» (Собрание законодательства Российской Федерации, 2011, № 15, ст. 2036; № 27, ст. 3880; 2012, № 29, ст. 3988; 2013, № 14, ст. 1668; № 27, ст. 3463, 3477; 2014, № 11, ст. 1098; № 26, ст. 3390; 2016, № 1, ст. 65; № 26, ст. 3889) следующие изменения:

1) в статье 2:

ФЗ от 27.12.2019 №476-ФЗ
«О внесении изменений в Федеральный закон «Об электронной подписи»

Предпосылки

Статья 15 дополнена частью 6.1 о наделении доверенных лиц (ДЛ) полномочиями на прием заявлений о получении квалифицированного сертификата ЮЛ, создание ключа ЭП и т.п. ДЛ должны, в том числе, соответствовать организационно-техническим требованиям в области ИБ, установленным ФСБ России.



ФЕДЕРАЛЬНАЯ СЛУЖБА БЕЗОПАСНОСТИ
РОССИЙСКОЙ ФЕДЕРАЦИИ

ПРИКАЗ

1 мая 2021 года Москва № 171

Об утверждении организационно-технических требований в области информационной безопасности к доверенным лицам удостоверяющего центра федерального органа исполнительной власти, уполномоченного на осуществление государственной регистрации юридических лиц

МИНИСТЕРСТВО ЮСТИЦИИ РОССИЙСКОЙ ФЕДЕРАЦИИ
ЗАРЕГИСТРИРОВАНО
Регистрационный № 63741
от "04" июня 2021

В соответствии с частью 6.1 статьи 15 Федерального закона от 6 апреля 2011 г. № 63-ФЗ «Об электронной подписи»[1] и пунктом 1 Положения о Федеральной службе безопасности Российской Федерации, утвержденного Указом Президента Российской Федерации от 11 августа 2003 г. № 960[2],

П Р И К А З Ы В А Ю:

1. Утвердить прилагаемые организационно-технические требования в области информационной безопасности к доверенным лицам удостоверяющего центра федерального органа исполнительной власти,

[1] Собрание законодательства Российской Федерации, 2011, № 15, ст. 2036; 2019, № 52, ст. 7794.
[2] Собрание законодательства Российской Федерации, 2003, № 33, ст. 3254; 2007, № 1, ст. 205.

Предпосылки

Приказ ФСБ России от 01.05.2021 №171 «Об утверждении организационно-технических требований в области информационной безопасности к доверенным лицам удостоверяющего центра федерального органа исполнительной власти, уполномоченного на осуществление государственной регистрации юридических лиц»

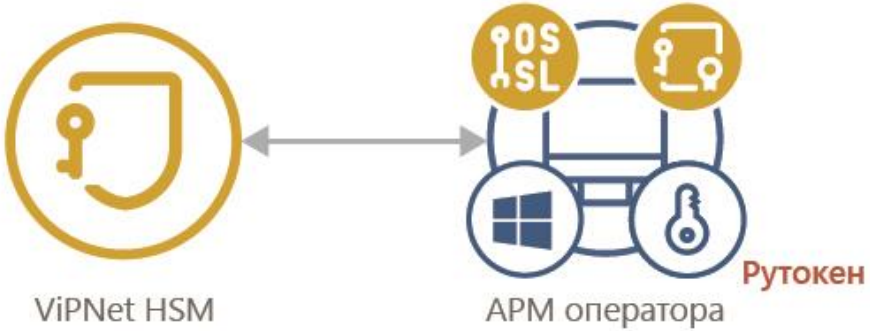
Приказ ФСБ России №171

ViPNet HSM

В пункте 8 было определено, что при создании ключа ЭП по обращению заявителей ДЛ должно:

- применять **средства ЭП КВ2** или КА1, имеющие в своем составе датчик, вырабатывающий случайную последовательность и механизм контроля срока действия ключей ЭП;
- записывать ключи ЭП, созданные по обращению заявителя, **на специализированные ключевые носители**, исключающие их несанкционированное использование и копирование;
- хранить, использовать и уничтожать ключи ЭП доверенного лица, предназначенные для подписания электронных документов и информации, в средстве ЭП, в котором они были созданы;
- применять СКЗИ, не являющиеся средствами ЭП, классов КВ и (или) КА;
- применять средства ЭП классов, отличных от классов КВ2 и (или) КА1, СКЗИ, не являющиеся средствами ЭП, классов, отличных от классов КВ и (или) КА, в схеме доставки заявления о получении квалифицированного сертификата юридического лица в УЦ в соответствии с пунктом 7 дополнительных требований.

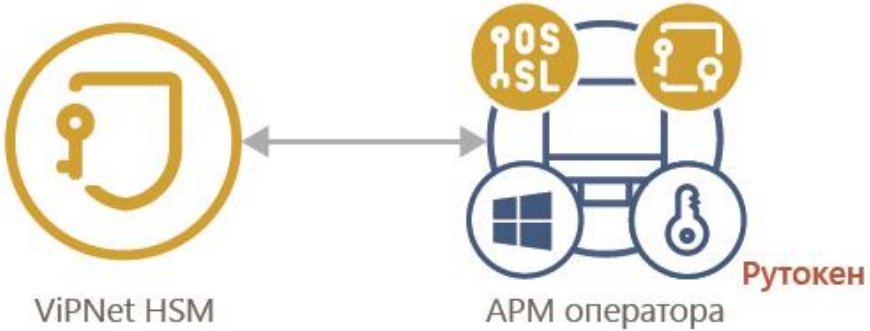
Схема демонстрационного макета



Реализация:

- Средство ЭП КВ2 – ViPNet HSM
- Ключевой носитель – Рутокен ЭЦП 3
- Средство УЦ – ViPNet УЦ (генерация запроса на сертификат p10 –опционально)

Схема демонстрационного макета



Алгоритм защиты и формат переноса ключей между СКЗИ разных производителей - рекомендации ТК26

Спасибо за внимание!

Бадмаева Римма

e-mail: Rimma.Badmaeva@infotecs.ru

Подписывайтесь на наши соцсети

vk.com/infotecs_news

https://t.me/infotecs_official

rutube.ru/channel/24686363