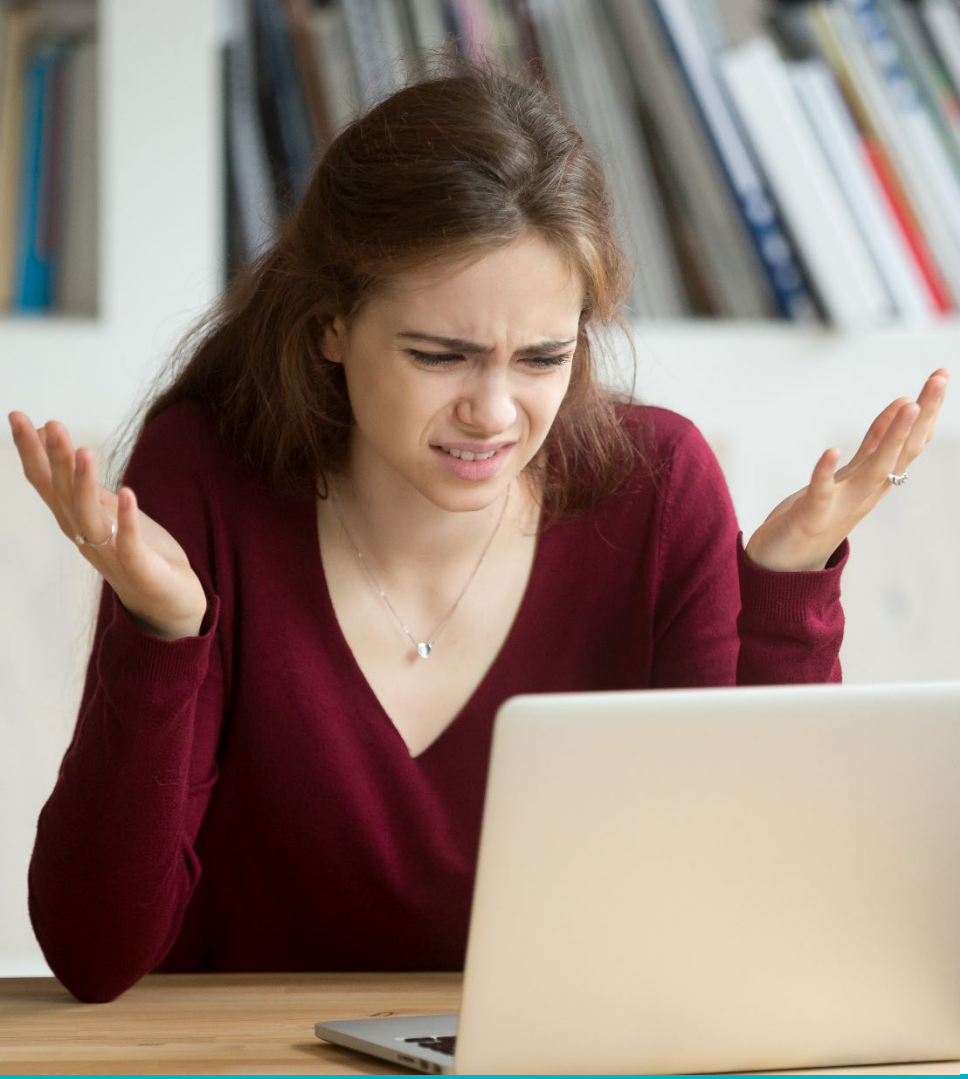
ViPNet HSM и ViPNet PKI Service: от универсального модуля до криптографических сервисов

Бадмаева Римма
Ведущий менеджер продуктов

Что такое HSM?



=


2.0

ViPNet HSM

1. Программно-аппаратный модуль (HSM – Hardware Secure Module)
2. Выполняет криптографические операции по запросам различных сервисов («большой токен»)
3. Повышенные меры безопасности
4. Поддержка актуальных криптоалгоритмов
5. СКЗИ класса КВ
6. Средство ЭП класса КВ2

Меры защиты от НСД

- Ролевая модель, обеспечивающая защиту от злонамеренных действий одного администратора: схема разделения секрета (нет суперпользователя), сбор кворума для выполнения критичных операций.
- Физические меры защиты: встроенный аппаратный модуль обнаруживает вскрытие корпуса, хранит и гарантированно уничтожает ключи.

ViPNet HSM: основные функции

1. Генерация ключей
2. Хранение ключей
3. Создание ЭП
4. Проверка ЭП
5. Шифрование

Характеристики

- Поддерживаемые 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
- Удаленное администрирование через Web-интерфейс по защищенному каналу с использованием ГОСТ TLS (ключи администраторов и сертификаты формируются в HSM и записываются на Рутокен Lite)
- Кластер
- Доступны версии в виде VA для тестирования (VirtualBox, VMWare, KVM)

**для проверки подписи*

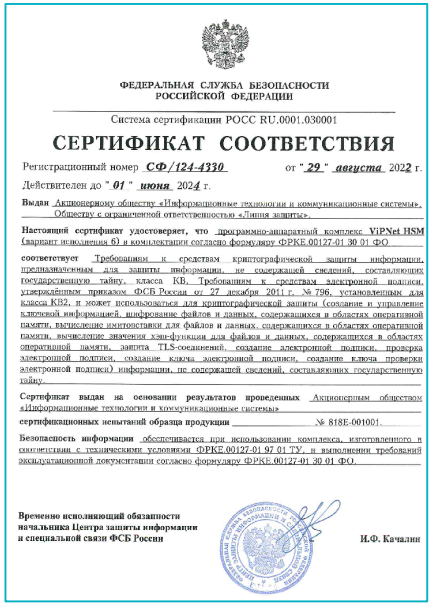
ViPNet HSM: поддержка иностранной криптографии

- Создание асимметричных ключей, создание и проверка ЭП по FIPS 186-4
- Создание симметричных ключей по FIPS 197, FIPS 46-3, NIST SP 800-132
- Шифрование данных по NIST SP 800-38A
- Вычисление функции хэширования по FIPS 180-4
- Формирование производных ключей по NIST SP 800-108 и т.д.

ViPNet HSM: поддержка иностранной криптографии

- Может применяться в банковских системах
- ViPNet HSM с поддержкой иностранной криптографии ≠ HSM с платежным модулем

ViPNet HSM: сертификаты



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) в комплектации согласно формуляру ФРКЕ.00127-01 30 01 ФО

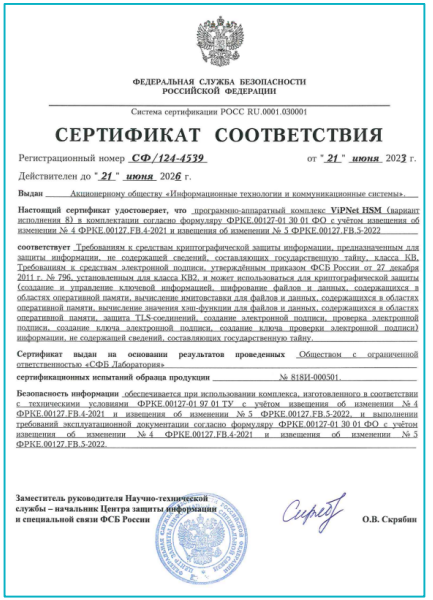
соответствует Требованиям к средствам криптографической защиты информации, предназначенным для защиты информации, не содержащей сведений, составляющих государственную тайну, класса КВ, Требованиям к средствам электронной подписи, утверждённым приказом ФСБ России от 27 декабря 2011 г. № 796, установленным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

Вариант исполнения 6



ФЕДЕРАЛЬНАЯ СЛУЖБА БЕЗОПАСНОСТИ
РОССИЙСКОЙ ФЕДЕРАЦИИ

Система сертификации РОСС RU.0001.030001

СЕРТИФИКАТ СООТВЕТСТВИЯ

Регистрационный номер СФ/124-4539 от "21" июня 2023 г.

Действителен до "21" июня 2026 г.

Выдан Акционерному обществу «Информационные технологии и коммуникационные системы».

Настоящий сертификат удостоверяет, что программно-аппаратный комплекс ViPNet HSM (вариант исполнения 8) в комплектации согласно формуляру ФРКЕ.00127-01 30 01 ФО с учётом извещения об изменении № 4 ФРКЕ.00127.FB.4-2021 и извещения об изменении № 5 ФРКЕ.00127.FB.5-2022

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 Обществом с ограниченной ответственностью «СФБ Лаборатория» сертификационных испытаний образца продукции № 818Н-000501.

Безопасность информации обеспечивается при использовании комплекса, изготовленного в соответствии с техническими условиями ФРКЕ.00127-01 97 01 ТУ с учётом извещения об изменении № 4 ФРКЕ.00127.FB.4-2021 и извещения об изменении № 5 ФРКЕ.00127.FB.5-2022, и выполнении требований эксплуатационной документации согласно формуляру ФРКЕ.00127-01 30 01 ФО с учётом извещения об изменении № 4 ФРКЕ.00127.FB.4-2021 и извещения об изменении № 5 ФРКЕ.00127.FB.5-2022.

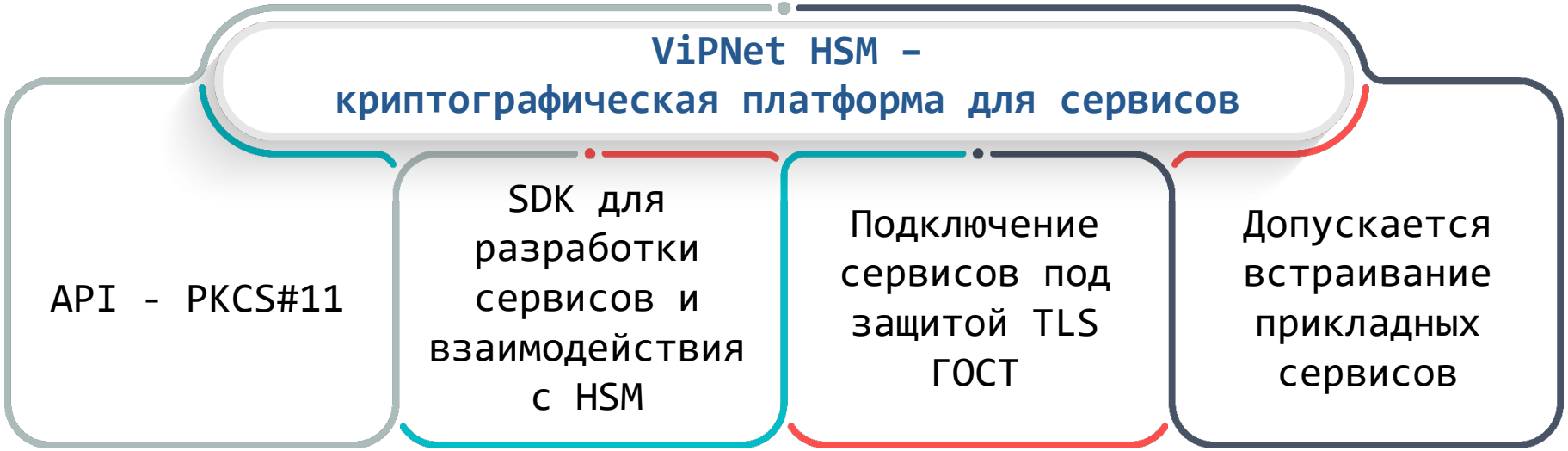
Заместитель руководителя Научно-технической службы – начальник Центра защиты информации и специальной связи ФСБ России О.В. Скрабин

Вариант исполнения 8

ViPNet HSM: сертифицированная версия

1. Кластер
2. Поддержка алгоритмов Магма и Кузнечик
3. Возможность работы АРМ администратора под управлением ОС Linux (с использованием СКЗИ ViPNet PKI Client)
4. Обновлен HSM SDK

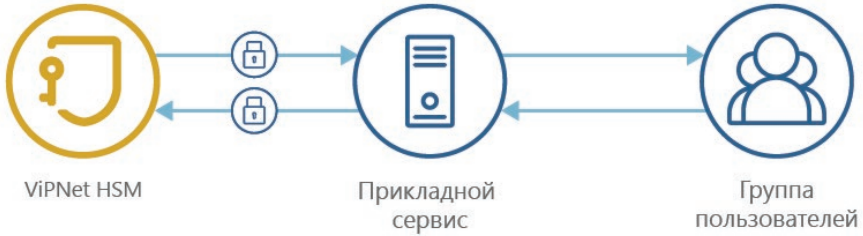
ViPNet HSM: подключение прикладных сервисов



ViPNet HSM: внешний прикладной сервис

Основные преимущества:

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

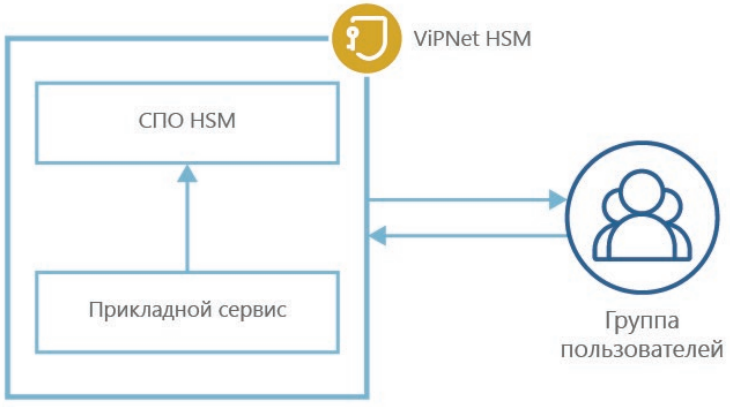


Пример: УЦ КС3+

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

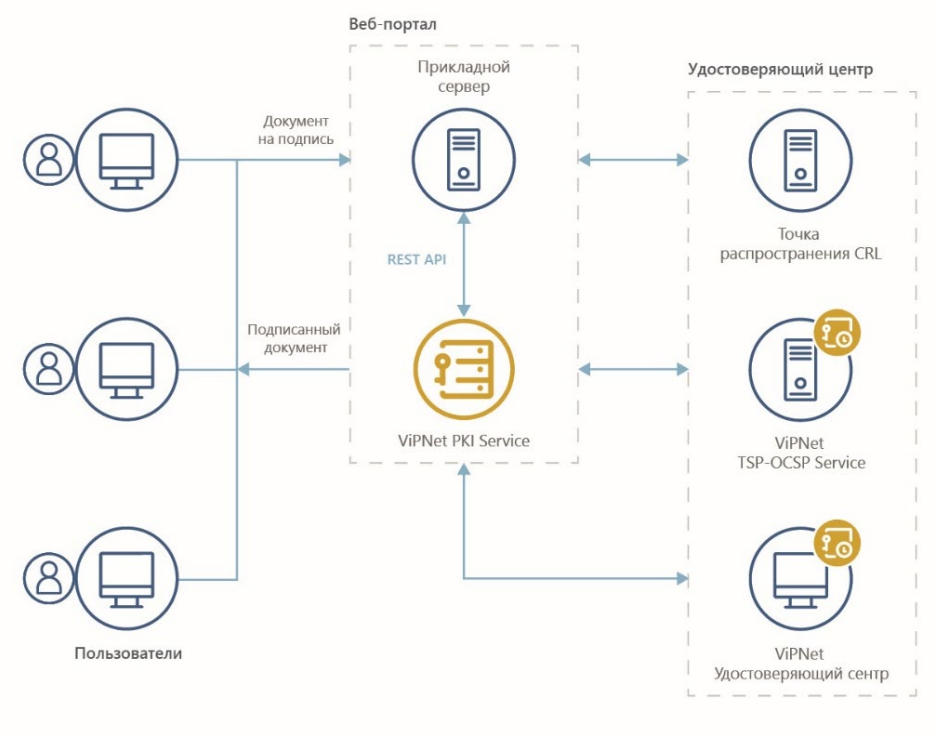


Например: ViPNet PKI Service

ViPNet PKI Service

ViPNet PKI Service

- Сервер подписи, разработанный на базе ViPNet HSM
- Централизованное выполнение криптографических операций
- СКЗИ класса КВ
- Средство ЭП класса КВ2



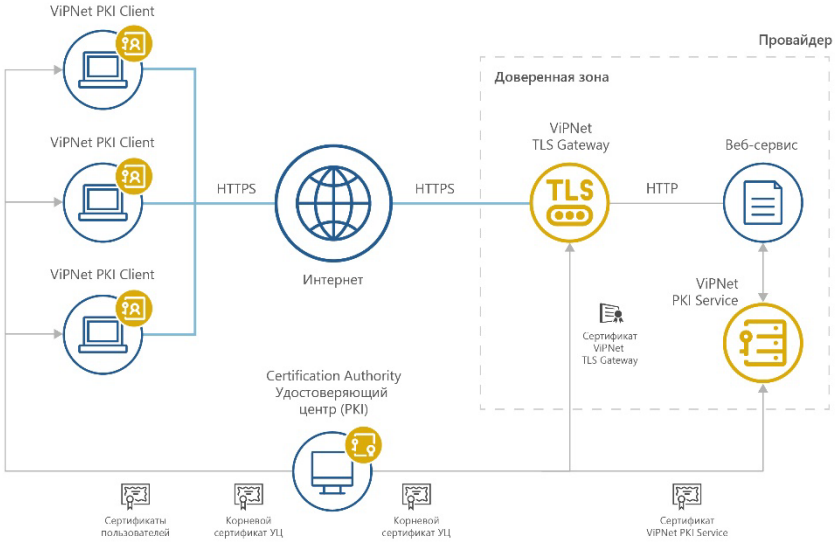
ViPNet HSM

- API – PKCS#11 (предоставляется HSM SDK)
- Поддержка иностранных криптоалгоритмов
- Может потребоваться сертификация

ViPNet PKI Service

- API - REST
- Взаимодействие с другими PKI-продуктами
- Лицензирование
- Может потребоваться оценка влияния (есть список «белых функций»)

ViPNet PKI Service: дополнительные возможности



Взаимодействие с другими компонентами PKI:

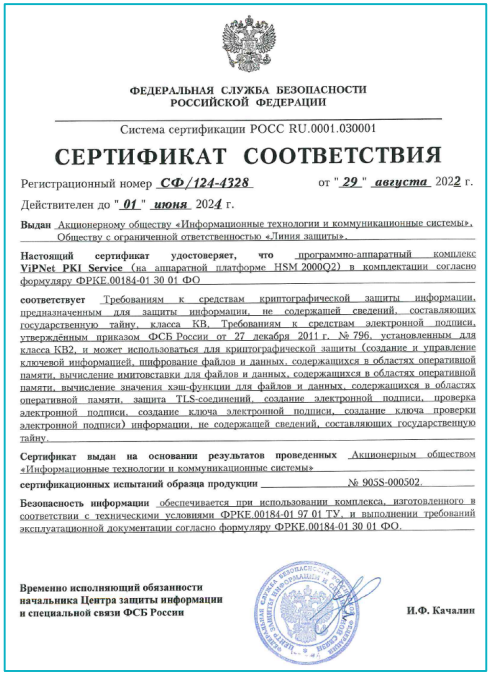
- УЦ: ViPNet УЦ, КриптоПРО УЦ 2.0;
- поддержка меток времени (TSP)
- возможность проверки статусов сертификатов по протоколу OCSP
- поддержание CRL в актуальном состоянии (CDP)
- совместная работа с ViPNet PKI Client (Cloud Unit) в сценарии облачной подписи
- совместная работа с ViPNet TLS Gateway для организации TLS-соединений при доступе пользователей к своим ключам

ViPNet PKI Service: лицензирование

- Лицензируется количество пользователей и количество сертификатов
- В базовую лицензию включена поддержка 10 пользователей и 100 сертификатов (1 пользователь – 10 сертификатов)
- При удалении пользователя или сертификата лицензия высвобождается

ViPNet PKI Service	
ViPNet PKI Service : Базовый продукт	
HC-237-PKI Service-2.X-(HSM5000 Q2)	ПАК ViPNet PKI Service (платформа HSM5000 Q2)
HC-237-PKI Service-HA-2.X-(HSM5000 Q2)	ПАК ViPNet PKI Service (дополнительный элемент кластера) (платформа HSM5000 Q2)
* Дополнительные лицензии на поддержку необходимого количества пользователей и необходимого количества сертификатов пользователей поставляются	
** Поставка дополнительного элемента кластера ViPNet PKI Service возможна только к существующему ранее поставленному базовому ПАК ViPNet PKI Ser	
ViPNet PKI Service : Лицензии расширения	
HC-237-PKI Service-1.X-add-LIC-U-1000	Передача права на расширение функционала ViPNet PKI Service. Лицензия для 1000 пользователей
HC-237-PKI Service-1.X-add-LIC-U-10 000	Передача права на расширение функционала ViPNet PKI Service. Лицензия для 10 000 пользователей
HC-237-PKI Service-1.X-add-LIC-U-20 000	Передача права на расширение функционала ViPNet PKI Service. Лицензия для 20 000 пользователей
HC-237-PKI Service-1.X-add-LIC-U-30 000	Передача права на расширение функционала ViPNet PKI Service. Лицензия для 30 000 пользователей
HC-237-PKI Service-1.X-add-LIC-U-40 00U0	Передача права на расширение функционала ViPNet PKI Service. Лицензия для 40 000 пользователей
HC-237-PKI Service-1.X-add-LIC-U-50 000	Передача права на расширение функционала ViPNet PKI Service. Лицензия для 50 000 пользователей
HC-237-PKI Service-1.X-add-LIC-U-100 000	Передача права на расширение функционала ViPNet PKI Service. Лицензия для 100 000 пользователей
HC-237-PKI Service-1.X-add-LIC-U-200 000	Передача права на расширение функционала ViPNet PKI Service. Лицензия для 200 000 пользователей
HC-237-PKI Service-1.X-add-LIC-S-1000	Передача права на расширение функционала ViPNet PKI Service. Лицензия на 1000 сертификатов пользователей
HC-237-PKI Service-1.X-add-LIC-S-10 000	Передача права на расширение функционала ViPNet PKI Service. Лицензия на 10 000 сертификатов пользователей
HC-237-PKI Service-1.X-add-LIC-S-20 000	Передача права на расширение функционала ViPNet PKI Service. Лицензия на 20 000 сертификатов пользователей
HC-237-PKI Service-1.X-add-LIC-S-30 000	Передача права на расширение функционала ViPNet PKI Service. Лицензия на 30 000 сертификатов пользователей
HC-237-PKI Service-1.X-add-LIC-S-40 00U0	Передача права на расширение функционала ViPNet PKI Service. Лицензия на 40 000 сертификатов пользователей
HC-237-PKI Service-1.X-add-LIC-S-50 000	Передача права на расширение функционала ViPNet PKI Service. Лицензия на 50 000 сертификатов пользователей
HC-237-PKI Service-1.X-add-LIC-S-100 000	Передача права на расширение функционала ViPNet PKI Service. Лицензия на 100 000 сертификатов пользователей
HC-237-PKI Service-1.X-add-LIC-S-200 000	Передача права на расширение функционала ViPNet PKI Service. Лицензия на 200 000 сертификатов пользователей

ViPNet PKI Service: сертификаты



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.

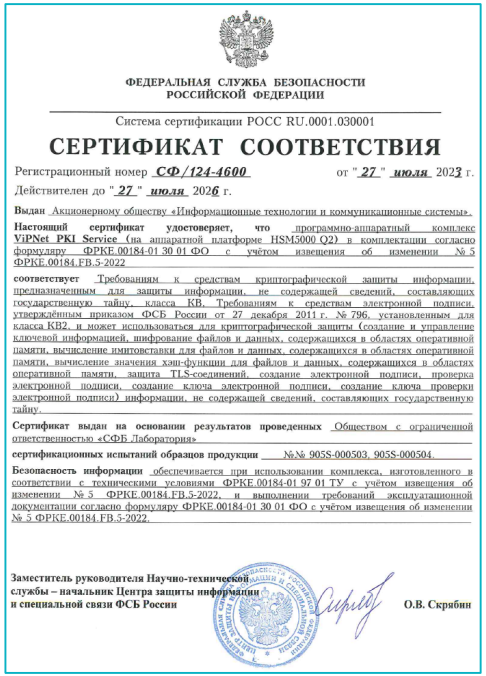
Сертификат выдан на основании результатов проведенных Акционерным обществом «Информационные технологии и коммуникационные системы»

сертификационных испытаний образца продукции № 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.

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

На АП HSM 2000 Q2



ФЕДЕРАЛЬНАЯ СЛУЖБА БЕЗОПАСНОСТИ
РОССИЙСКОЙ ФЕДЕРАЦИИ

Система сертификации РОСС RU.0001.030001

СЕРТИФИКАТ СООТВЕТСТВИЯ

Регистрационный номер *СФ/124-4600* от "*27*" *июля* 2023 г.

Действителен до "*27*" *июля* 2026 г.

Выдан Акционерному обществу «Информационные технологии и коммуникационные системы».

Настоящий сертификат удостоверяет, что программно-аппаратный комплекс **ViPNet PKI Service** (на аппаратной платформе HSM5000 Q2) в комплектации согласно формуляру ФРКЕ.00184-01 30 01 ФО с учётом извещения об изменении № 5 ФРКЕ.00184.ГВ.5-2022

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 Обществом с ограниченной ответственностью «СФБ Лаборатория»

сертификационных испытаний образцов продукции №№ 905S-000503, 905S-000504.

Безопасность информации обеспечивается при использовании комплекса, изготовленного в соответствии с техническими условиями ФРКЕ.00184-01 97 01 ТУ с учётом извещения об изменении № 5 ФРКЕ.00184.ГВ.5-2022, и выполнении требований эксплуатационной документации согласно формуляру ФРКЕ.00184-01 30 01 ФО с учётом извещения об изменении № 5 ФРКЕ.00184.ГВ.5-2022.

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

На АП HSM 5000 Q2

ViPNet PKI Service: сертифицированная версия

1. Кластер
2. Поддержка алгоритмов Магма и Кузнечик
3. Поддержка формата подписи CAdES-X Long Type 1
4. Возможность работы АРМ администратора под управлением ОС Linux (с использованием СКЗИ ViPNet PKI Client)

ViPNet PKI Service: сертифицированная версия

ТЕХНО infotecs 2024 ФЕСТ

5 Расширена ролевая модель, добавлены роли Оператора сервера подписи и Администратора ИС

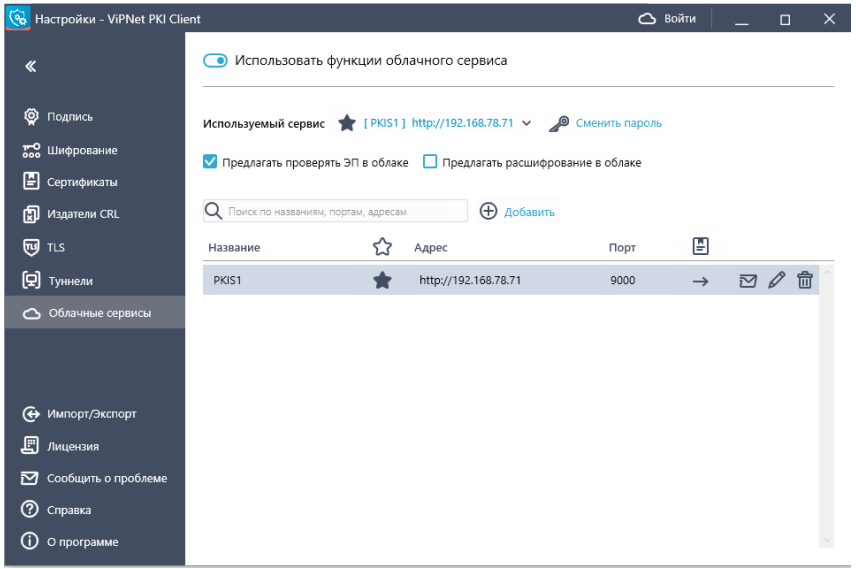
6 Доработаны способы аутентификации пользователей

7 Совместная работа с сертифицированными версиями ViPNet PKI Client в сценариях облачной подписи (с использованием Cloud Unit)

8 Поддержка 795 приказа ФСБ России

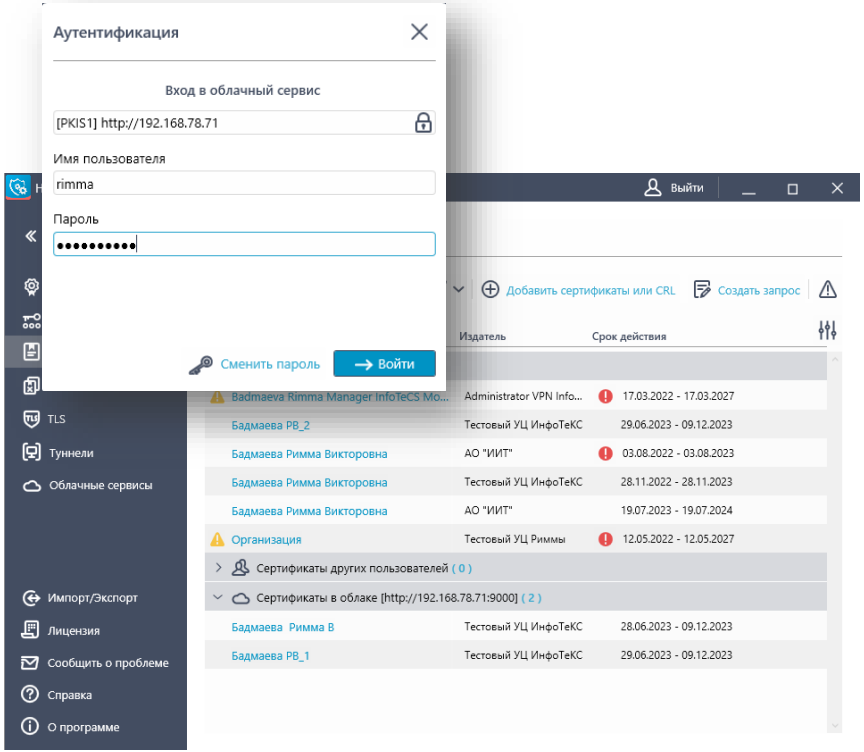
ViPNet PKI Service: облачная подпись

- Только УНЭП, УКЭП – после выхода соответствующих требований
- Совместная работа с сертифицированными версиями ViPNet PKI Client 1.6 Win/Lin с использованием Cloud Unit, а также с официальными версиями ViPNet PKI Client Mobile
- Аутентификация – односторонний TLS+пароль, двусторонний TLS



PKI Service и PKI Client: облачная подпись

- Возможность выполнения криптографических операций из интерфейса ViPNet PKI Client:
  1. Формирование запроса на сертификат с хранением ключа ЭП в ViPNet PKI Service
  2. Отображение сертификатов, ключи ЭП которых хранятся в сервере подписи
  3. Подписание документов



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