ViPNet HSM и ViPNet PKI Service: обзор новых версий продуктов

Бадмаева Римма

infotecs

Содержание вебинара

1. Назначение, взаимосвязь и различия ViPNet HSM и ViPNet PKI Service
2. ***ViPNet HSM 3.5:*** функциональные возможности сертифицированной версии
3. ***ViPNet PKI Service 2.3 и 2.4:*** функциональные возможности сертифицированных версий

Назначение и взаимосвязь ViPNet HSM и ViPNet PKI Service

ViPNet HSM

ViPNet
PKI Service

ViPNet HSM


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

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 КСЗ

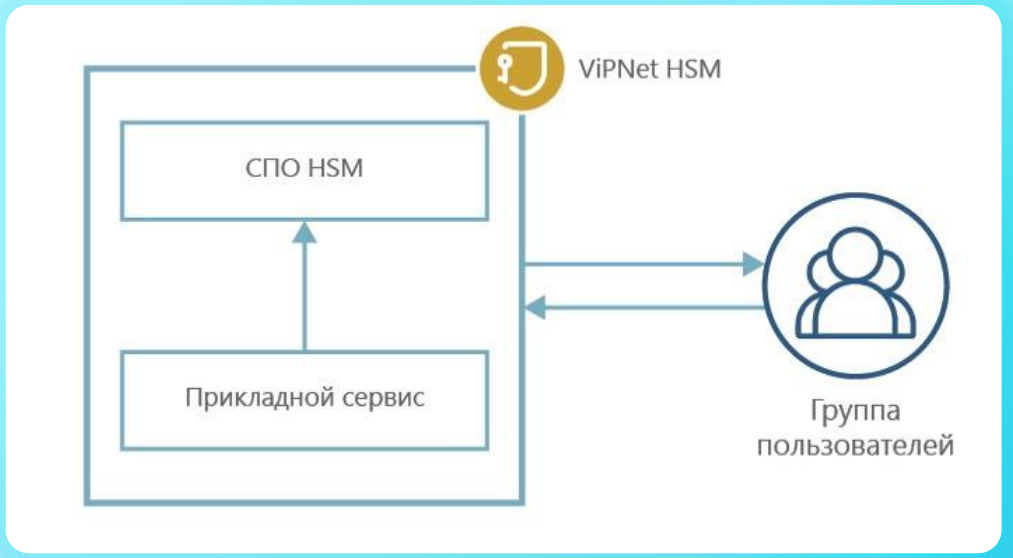
ViPNet HSM: внутренний прикладной сервис

Основные преимущества:

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

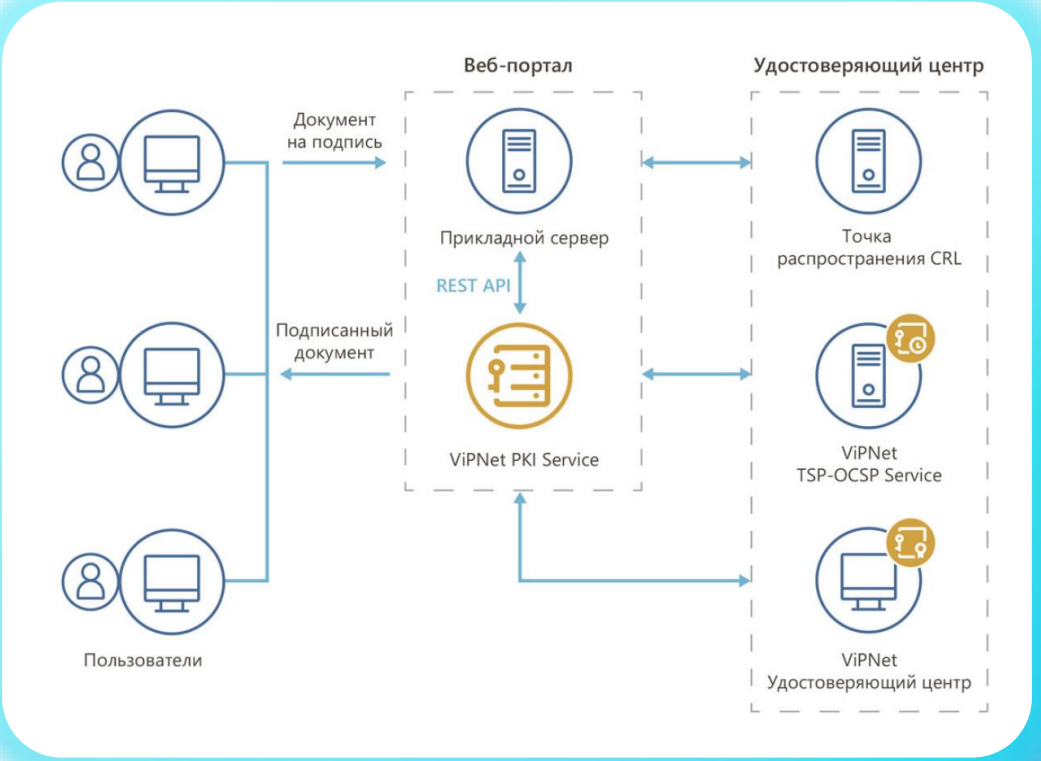
Например:

ViPNet
PKI Service



ViPNet PKI Service

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



Функциональные возможности и различия

- ViPNet HSM
- ViPNet PKI Service

Основные функции

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

Общие характеристики

- Поддерживаемые криптоалгоритмы: ГОСТ 28147-89, ГОСТ 34.12-2018, ГОСТ 34.13-2018, ГОСТ Р 34.10-2012, ГОСТ Р 34.11-2012
- Удаленное администрирование через Web-интерфейс по защищенному каналу с использованием ГОСТ TLS с АРМ с ViPNet PKI Client
- Кластер (до 10 узлов)
- Требуется оценка влияния
- Доступны версии в виде VA для тестирования (VirtualBox, VMWare, KVM)

Меры защиты

- 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

Встраивание ViPNet HSM и ViPNet PKI Service

- Необходимо провести оценку влияния
- Список белых функций, использование которых при разработке систем на основе ПАК ViPNet HSM и ПАК ViPNet PKI Service возможно без дополнительных тематических исследований, приводится в Правилах пользования.

Использование функций не из списка = разработка отдельного СКЗИ

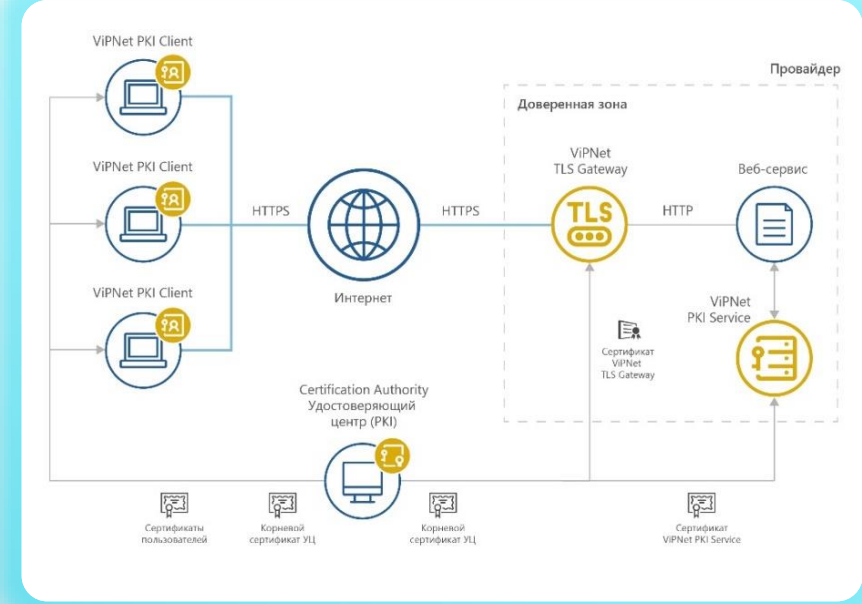
ViPNet HSM

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

ViPNet PKI Service

- API - REST
- Взаимодействие с другими PKI-продуктами
- Лицензирование

ViPNet PKI Service: дополнительные возможности



Взаимодействие с другими компонентами PKI:

- УЦ: ViPNet УЦ, КриптоПРО УЦ 2.0
- поддержка протокола TSP (метки времени)
- 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 (УНЭП)
- 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

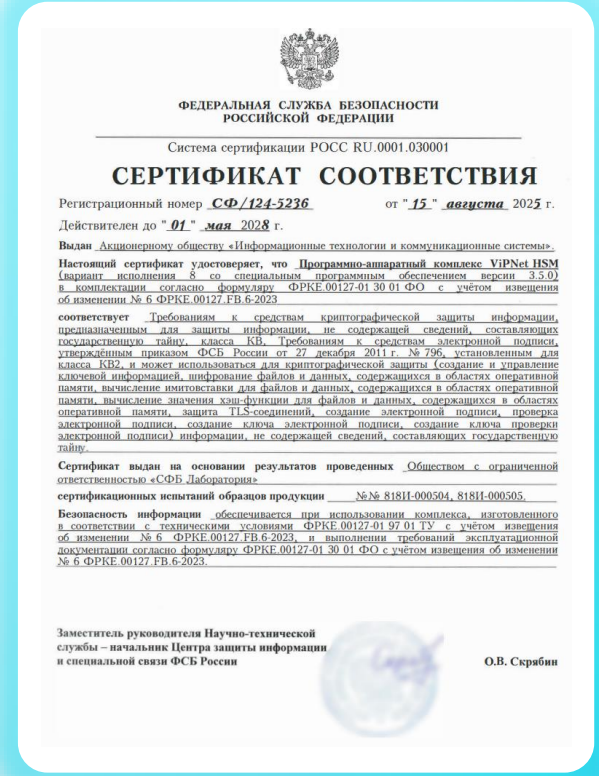
ViPNet PKI Service	
ViPNet PKI Service : Базовый продукт	
HC-237-PKI Service-2.X-(HSM5000 Q2)	ПАК ViPNet PKI Service (платформа HSM5000 Q2)
HC-237-PKI Service-HA-2.X-(HSM5000 Q2)	ПАК ViPNet PKI Service (дополнительный элемент кластера) (платформа HSM5000 Q2)
* Дополнительные лицензии на поддержку необходимого количества пользователей и необходимого количества сертификатов пользователей поставляютс	
** Поставка дополнительного элемента кластера ViPNet PKI Service возможна только к существующему ранее поставленному базовому ПАК ViPNet PKI Servi	
*** Для управления на АРМ администраторов PKI Service должен быть установлен ViPNet PKI Client 2.X, приобретается отдельно	
ViPNet PKI Service : Лицензии расширения	
HC-237-PKI Service-2.X-add-LIC-U-1000	Передача права на расширение функционала ViPNet PKI Service. Лицензия для 1000 пользователей
HC-237-PKI Service-2.X-add-LIC-U-10 000	Передача права на расширение функционала ViPNet PKI Service. Лицензия для 10 000 пользователей
HC-237-PKI Service-2.X-add-LIC-U-20 000	Передача права на расширение функционала ViPNet PKI Service. Лицензия для 20 000 пользователей
HC-237-PKI Service-2.X-add-LIC-U-30 000	Передача права на расширение функционала ViPNet PKI Service. Лицензия для 30 000 пользователей
HC-237-PKI Service-2.X-add-LIC-U-40 000	Передача права на расширение функционала ViPNet PKI Service. Лицензия для 40 000 пользователей
HC-237-PKI Service-2.X-add-LIC-U-50 000	Передача права на расширение функционала ViPNet PKI Service. Лицензия для 50 000 пользователей
HC-237-PKI Service-2.X-add-LIC-U-100 000	Передача права на расширение функционала ViPNet PKI Service. Лицензия для 100 000 пользователей
HC-237-PKI Service-2.X-add-LIC-U-200 000	Передача права на расширение функционала ViPNet PKI Service. Лицензия для 200 000 пользователей
HC-237-PKI Service-2.X-add-LIC-S-1000	Передача права на расширение функционала ViPNet PKI Service. Лицензия на 1000 сертификатов пользователей
HC-237-PKI Service-2.X-add-LIC-S-10 000	Передача права на расширение функционала ViPNet PKI Service. Лицензия на 10 000 сертификатов пользователей
HC-237-PKI Service-2.X-add-LIC-S-20 000	Передача права на расширение функционала ViPNet PKI Service. Лицензия на 20 000 сертификатов пользователей
HC-237-PKI Service-2.X-add-LIC-S-30 000	Передача права на расширение функционала ViPNet PKI Service. Лицензия на 30 000 сертификатов пользователей
HC-237-PKI Service-2.X-add-LIC-S-40 000	Передача права на расширение функционала ViPNet PKI Service. Лицензия на 40 000 сертификатов пользователей
HC-237-PKI Service-2.X-add-LIC-S-50 000	Передача права на расширение функционала ViPNet PKI Service. Лицензия на 50 000 сертификатов пользователей
HC-237-PKI Service-2.X-add-LIC-S-100 000	Передача права на расширение функционала ViPNet PKI Service. Лицензия на 100 000 сертификатов пользователей
HC-237-PKI Service-2.X-add-LIC-S-200 000	Передача права на расширение функционала ViPNet PKI Service. Лицензия на 200 000 сертификатов пользователей

ViPNet HSM 3.5

Обзор сертифицированной версии

Сертификат соответствия

- Сертификат №СФ/124-5236 от 15.08.25
- Вариант исполнения 8 (АП HSM5000 Q2)
- ФДСЧ - Гроссмейстер
- СПО 3.5.0
- Срок действия – до 01.05.28



ФЕДЕРАЛЬНАЯ СЛУЖБА БЕЗОПАСНОСТИ
РОССИЙСКОЙ ФЕДЕРАЦИИ

Система сертификации РОСС RU.0001.030001

СЕРТИФИКАТ СООТВЕТСТВИЯ

Регистрационный номер СФ/124-5236 от "15" августа 2025 г.

Действителен до "01" мая 2028 г.

Выдан Акционерному обществу «Информационные технологии и коммуникационные системы».

Настоящий сертификат удостоверяет, что Программно-аппаратный комплекс ViPNet HSM (вариант исполнения 8 со специальным программным обеспечением версии 3.5.0) в комплектации согласно формуляру ФРКЕ.00127-01 30 01 ФО с учётом извещения об изменении № 6 ФРКЕ.00127.FB.6-2023

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 №№ 818И-000504, 818И-000505.

Безопасность информации обеспечивается при использовании комплекса, изготовленного в соответствии с техническими условиями ФРКЕ.00127-01 97 01 ТУ с учётом извещения об изменении № 6 ФРКЕ.00127.FB.6-2023, и выполнении требований эксплуатационной документации согласно формуляру ФРКЕ.00127-01 30 01 ФО с учётом извещения об изменении № 6 ФРКЕ.00127.FB.6-2023.

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

ViPNet HSM 3.5: что нового

- Расширенная поддержка иностранных криптоалгоритмов
- Поддержка TLS версии 1.3
- Возможность перезагрузки и смены режима работы через web-интерфейс
- Возможность развертывания HSM VA на платформах виртуализации KVM

Расширенная поддержка иностранной криптографии*

- Создание асимметричных ключей, создание и проверка ЭП по FIPS 186-5
- 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.

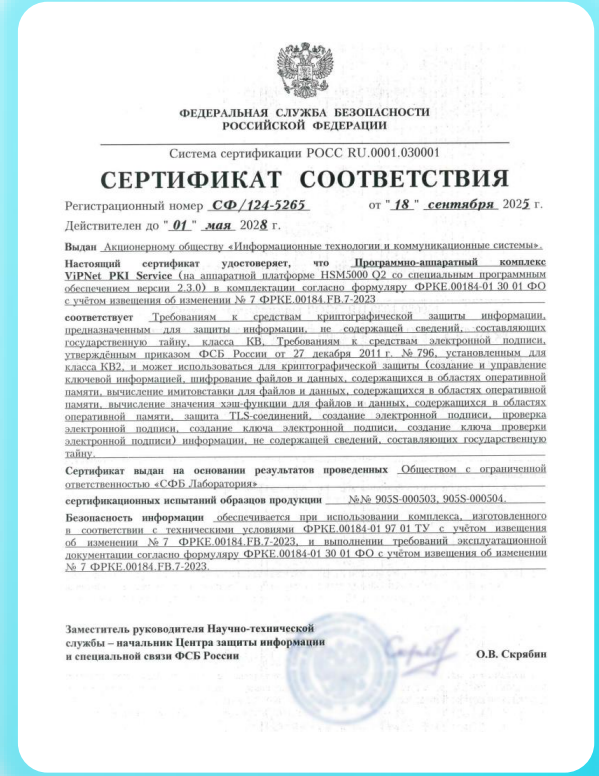
** по запросу список может быть расширен*

ViPNet PKI Service 2.3 и 2.4

Обзор сертифицированных версий

Сертификат соответствия (2.3)

- Сертификат №СФ/124-5265 от 18.09.25
- АП HSM5000 Q2
- ФДСЧ - Гроссмейстер
- СПО 2.3.0
- Срок действия – до 01.05.28



ФЕДЕРАЛЬНАЯ СЛУЖБА БЕЗОПАСНОСТИ
РОССИЙСКОЙ ФЕДЕРАЦИИ

Система сертификации РОСС RU.0001.030001

СЕРТИФИКАТ СООТВЕТСТВИЯ

Регистрационный номер СФ/124-5265 от "18" сентября 2025 г.

Действителен до "01" мая 2028 г.

Выдан Акционерному обществу «Информационные технологии и коммуникационные системы».

Настоящий сертификат удостоверяет, что Программно-аппаратный комплекс ViPNet PKI Service (на аппаратной платформе HSM5000 Q2 со специальным программным обеспечением версии 2.3.0) в комплектации согласно формуляру ФРКЕ.00184-01 30 01 ФО с учётом извещения об изменении № 7 ФРКЕ.00184.FB.7-2023

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 № 7 ФРКЕ.00184.FB.7-2023, и выполнении требований эксплуатационной документации согласно формуляру ФРКЕ.00184-01 30 01 ФО с учётом извещения об изменении № 7 ФРКЕ.00184.FB.7-2023.

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

ViPNet PKI Service 2.3: что нового

- Совместная работа с сервером аутентификации JaCarta Authentication Server (JAS) компании Аладдин
- Загрузка pfx-файлов в сервер подписи (сценарий миграции в облако)
- Проверка статусов сертификатов
- Поддержка TLS версии 1.3.

ViPNet PKI Service 2.3: что нового

- Возможность использования ViPNet TLS Gateway для аутентификации пользователей сервера подписи
- Возможность перезагрузки и смены режима работы через web-интерфейс
- Прекращена поддержка АП HSM2000 Q2

Прекращение поддержки АП HSM2000 Q2

- Актуально для ViPNet PKI Service, работающих с ДСДР
- Последний сертификат на ViPNet PKI Service на АП HSM2000 Q2 истек **31.10.2024.**
- Сертификат продлеваться не будет
- При необходимости запланировать закупку и ввод в эксплуатацию ViPNet PKI Service на АП HSM5000 Q2

ФЕДЕРАЛЬНАЯ СЛУЖБА БЕЗОПАСНОСТИ
РОССИЙСКОЙ ФЕДЕРАЦИИ

Система сертификации РОСС RU.0001.030001

СЕРТИФИКАТ СООТВЕТСТВИЯ

Регистрационный номер СФ/124-4825 от "03" апреля 2024 г.

Действителен до "31" октября 2024 г.

Выдан Акционерному обществу «Информационные технологии и коммуникационные системы».

Настоящий сертификат удостоверяет, что Программно-аппаратный комплекс ViPNet PKI Service (на аппаратной платформе HSM2000 Q2) в комплектации согласно формуляру ФРКЕ.00184-01 30 01 ФО с учётом извещения об изменении № 6 ФРКЕ.00184.FB.6-2022

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»

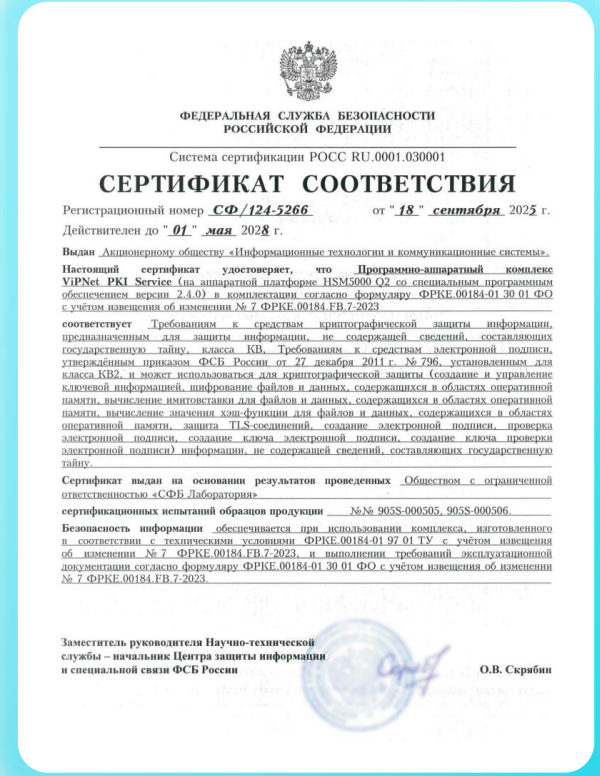
сертификационных испытаний образца продукции № 905S-000502.

Безопасность информации обеспечивается при использовании комплекса, изготовленного в соответствии с техническими условиями ФРКЕ.00184-01 97 01 ТУ с учётом извещения об изменении № 6 ФРКЕ.00184.FB.6-2022, и выполнении требований эксплуатационной документации согласно формуляру ФРКЕ.00184-01 30 01 ФО с учётом извещения об изменении № 6 ФРКЕ.00184.FB.6-2022.

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

Сертификат соответствия (2.4)

- Сертификат №СФ/124-5266 от 18.09.25
- АП HSM5000 Q2
- ФДСЧ - Гроссмейстер
- СПО 2.4.0
- Срок действия – до 01.05.28



ФЕДЕРАЛЬНАЯ СЛУЖБА БЕЗОПАСНОСТИ
РОССИЙСКОЙ ФЕДЕРАЦИИ

Система сертификации РОСС RU.0001.030000

СЕРТИФИКАТ СООТВЕТСТВИЯ

Регистрационный номер СФ/124-5266 от "18" сентября 2025 г.

Действителен до "01" мая 2028 г.

Выдан Акционерному обществу «Информационные технологии и коммуникационные системы».

Настоящий сертификат удостоверяет, что Программно-аппаратный комплекс ViPNet PKI Service (на аппаратной платформе HSM5000 Q2 со специальным программным обеспечением версии 2.4.0) в комплектации согласно формуляру ФРКЕ.00184-01 30 01 ФО с учётом извещения об изменении № 7 ФРКЕ.00184.FB.7-2023

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-000505, 905S-000506.

Безопасность информации обеспечивается при использовании комплекса, изготовленного в соответствии с техническими условиями ФРКЕ.00184-01 97 01 ТУ с учётом извещения об изменении № 7 ФРКЕ.00184.FB.7-2023, и выполнении требований эксплуатационной документации согласно формуляру ФРКЕ.00184-01 30 01 ФО с учётом извещения об изменении № 7 ФРКЕ.00184.FB.7-2023.

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

ViPNet PKI Service 2.4: что нового

- Версия для использования в Контуре контроля, Контуре обработки в инфраструктуре цифрового рубля финансовых посредников (коммерческих банков)

- Добавлена поддержка ViPNet УЦ 5

Телеграм-канал

Криптография в финтехе

Подписывайтесь
на наши соцсети,
там много интересного

infotecs

Спасибо за внимание!