Знакомьтесь: ViPNet Удостоверяющий центр 5

Бадмаева Римма

Руководитель продуктового направления

инфотекс ТЕХНОДЕСТ

Белый поток

Назначение УЦ

Удостоверяющий центр предназначен для выполнения функций УЦ в соответствии с требованиями ФЗ-63 «Об электронной подписи»:

- издание сертификатов
- аннулирование сертификатов
- ведение реестра сертификатов и т.д.

Эволюция УЦ: от версии 4.6 до версии 5

инфотекс

ViPNet УЦ 4.6: состав

ViPNet Administrator

УКЦ выступает в качестве Центра сертификации

ViPNet Registration Point или ViPNet CA Web Service

Выступают в качестве Центра регистрации

ViPNet CA Informing

Сервис информирования

ViPNet Publication Service

Сервис публикации

ViPNet TSP-OCSP Service

Сервис выдачи меток (штампов) времени и проверки статусов сертификатов в онлайн-режиме

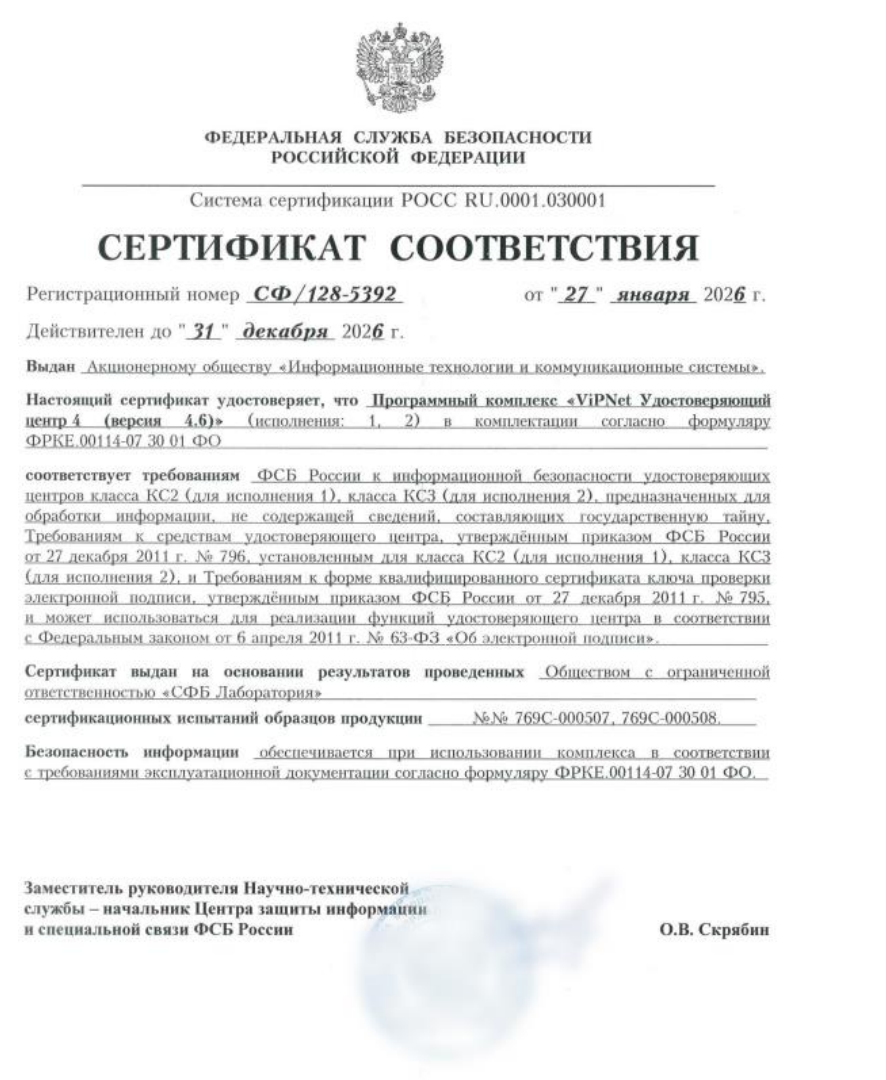
ViPNet УЦ 4.6: детали

Совместная работа с ViPNet HSM
(позволяет увеличить срок действия ключа ЭП УЦ до 5 лет)

минцифры_

Используется аккредитованными УЦ
(для издания квалифицированных сертификатов)

Используется для выдачи сертификатов
(для Госключа)



ФЕДЕРАЛЬНАЯ СЛУЖБА БЕЗОПАСНОСТИ
РОССИЙСКОЙ ФЕДЕРАЦИИ

Система сертификации РОСС RU.0001.030001

СЕРТИФИКАТ СООТВЕТСТВИЯ

Регистрационный номер СФ/128-5392 от "27" января 2026 г.

Действителен до "31" декабря 2026 г.

Выдан Акционерному обществу «Информационные технологии и коммуникационные системы».

Настоящий сертификат удостоверяет, что Программный комплекс «ViPNet Удостоверяющий центр 4 (версия 4.6)» (исполнения: 1, 2) в комплектации согласно формуляру ФРКЕ.00114-07 30 01 ФО

соответствует требованиям ФСБ России к информационной безопасности удостоверяющих центров класса КС2 (для исполнения 1), класса КС3 (для исполнения 2), предназначенных для обработки информации, не содержащей сведений, составляющих государственную тайну. Требованиям к средствам удостоверяющего центра, утверждённым приказом ФСБ России от 27 декабря 2011 г. № 796, установленным для класса КС2 (для исполнения 1), класса КС3 (для исполнения 2), и Требованиям к форме квалифицированного сертификата ключа проверки электронной подписи, утверждённым приказом ФСБ России от 27 декабря 2011 г. № 795, и может использоваться для реализации функций удостоверяющего центра в соответствии с Федеральным законом от 6 апреля 2011 г. № 63-ФЗ «Об электронной подписи».

Сертификат выдан на основании результатов проведенных Обществом с ограниченной ответственностью «СФБ Лаборатория»

сертификационных испытаний образцов продукции №№ 769С-000507, 769С-000508.

Безопасность информации обеспечивается при использовании комплекса в соответствии с требованиями эксплуатационной документации согласно формуляру ФРКЕ.00114-07 30 01 ФО.

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

инфотекс

ViPNet УЦ 4.6: сертификация

- Два исполнения: средство УЦ КС2 и КС3 для ОС Windows
- Текущий сертификат действует до 31.12.2026

Предпосылки разработки УЦ 5

- Импортозамещение
- Ключ ЭП УЦ должен храниться в неизвлекаемом виде (HSM или токен-СКЗИ)
- Удобство размещения

ViPNet УЦ 5: состав

Центр сертификации

- **ПАК ViPNet Certification Authority 5**
- АРМ администратора УЦ с **СКЗИ ViPNet PKI Client 2.0** для подключения к web-интерфейсу ViPNet CA

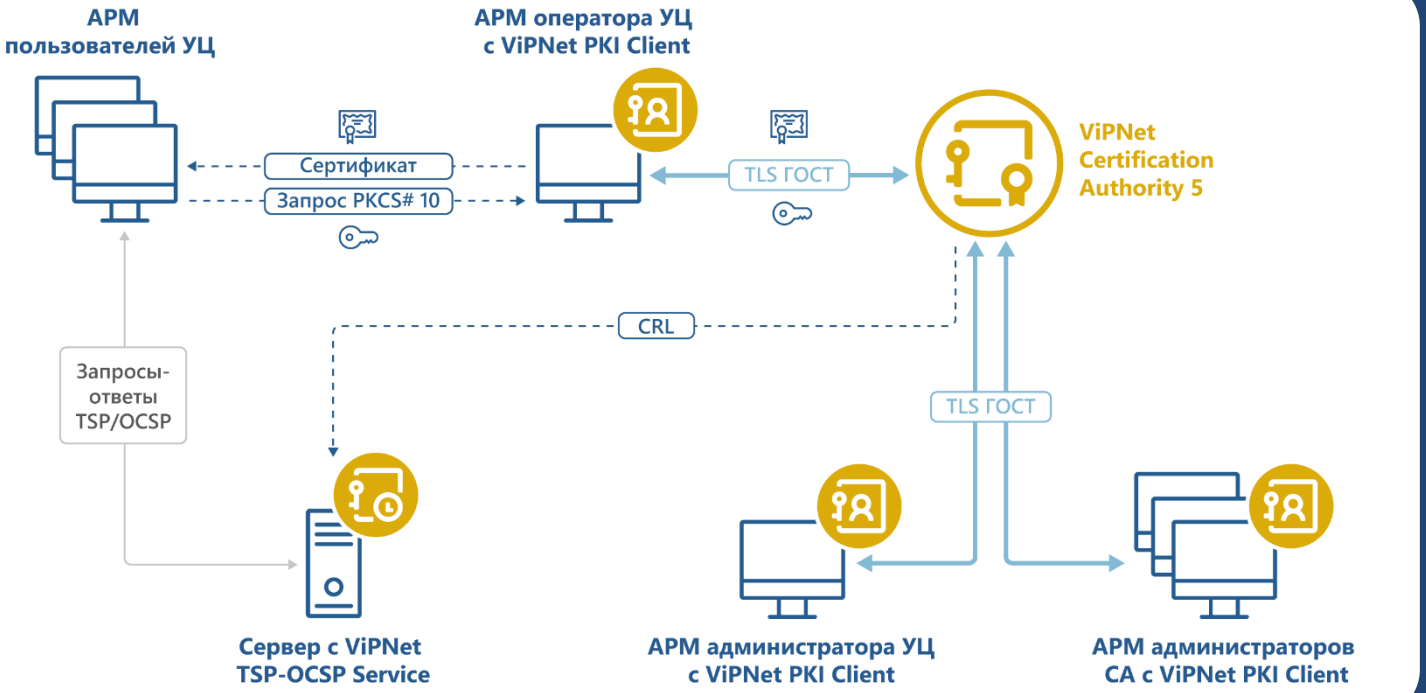
Центр регистрации

АРМ оператора УЦ с **СКЗИ ViPNet PKI Client 2.0** для подключения к web-интерфейсу ViPNet CA

ViPNet TSP-OCSP Service 5

Сервис выдачи меток (штампов) времени и проверки статусов сертификатов в онлайн-режиме

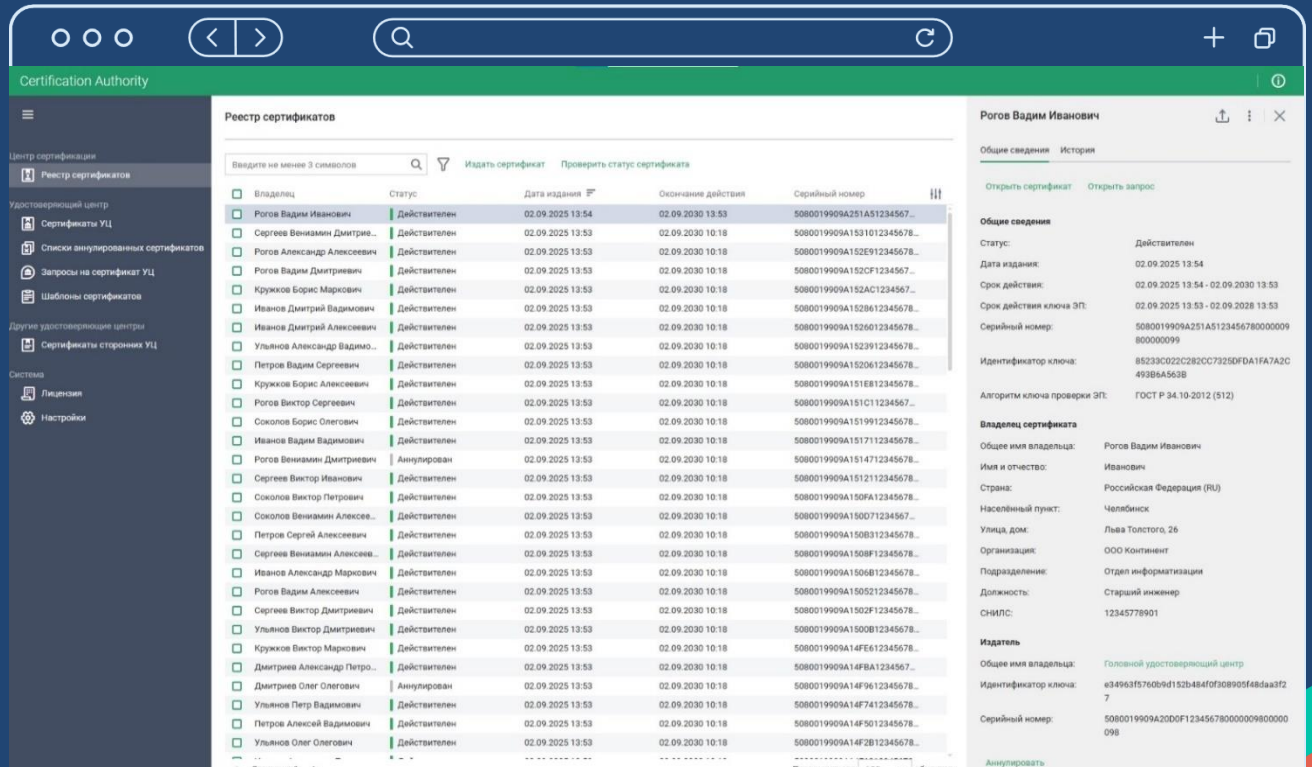
Схема работы УЦ



ViPNet Certification Authority 5

- Разрабатывается на базе криптографической платформы ViPNet HSM (как, например, сервер подписи ViPNet PKI Service)
- Для тестирования доступна версия в виде VA (VirtualBox, VMWare, KVM)
- Аппаратная платформа – **HSM 5000 Q2**
- СКЗИ и средство ЭП класса КВ/КВ2

ViPNet Certification Authority 5



ViPNet CA 5: основные функции

Издание пользовательских сертификатов:

- по запросу (pkcs#10)
- с формированием ключевой пары

Издание корневых сертификатов УЦ

Формирование запросов в вышестоящий УЦ, запросов на кросс-сертификат

Аннулирование сертификатов, выпуск CRL и т.д.

Выдача сертификатов, в т.ч. в печатной форме

Ведение реестра сертификатов

Основные отличия УЦ 5 от УЦ 4

- Отдельный продукт, не связан с ViPNet-сетями и VPN
- Ядро УЦ – ПАК с ОС Linux
- ОС для АРМ администраторов и операторов УЦ – Linux (СКЗИ ViPNet PKI Client, исп. 6)
- Возможность одновременного использования нескольких сертификатов УЦ для выпуска сертификатов

Переход с УЦ 4 на УЦ 5

ViPNet УЦ 4

перестает выпускать сертификаты пользователей, только отзыв, вплоть до выпуска финального CRL

ViPNet УЦ 5

обеспечивает выпуск пользовательских сертификатов и управляет их жизненным циклом (отзыв, хранение)

Про миграцию

- Возможен импорт реестра сертификатов из УЦ 4 в УЦ 5
- **Есть ограничения:**
  - **юридические:** в квалифицированном сертификате указано название средства УЦ и средства ЭП, у УЦ 4 и УЦ 5 они будут разные
  - **технические:** ключ ЭП УЦ 4 неэкспортируемый, его нельзя перенести в УЦ 5

ViPNet УЦ 5: производительность

Параметр	Значение
Средняя скорость издания сертификатов	**~270 шт/сек**
Средняя скорость издания сертификатов при смешанной нагрузке (издание и аннулирование без выпуска CRL)	**~172 шт/сек**
Средняя скорость аннулирования сертификатов при смешанной нагрузке	**~24 шт/сек**
Количество издаваемых сертификатов	**Макс – 100 млн**
Размер CRL с 1 млн отозванных сертификатов	**50 Мб**
Время издания CRL с 1 млн отозванных сертификатов	**50 сек**

ViPNet УЦ: планы развития

Расширение перечня поддерживаемых АП

Разработка исполнений КВ2 и КС1 (VA)

Поддержка западных алгоритмов

инфотекс

Криптография в финтехе теперь в MAX!

САНКТ ПЕТЕРБУРГ

инфотекс

ТЕХНОФЕСТ

Академия инфотекс · Учебный центр инфотекс · AMPIRE · TELEOFIS · КОМФОРТЕЛ оператор связи бизнес-класса · РУТОКЕН · Актив · TS Solution · AXOFT

Подписывайтесь на наши соцсети