

# Знакомьтесь: ViPNet Удостоверяющий центр 5

Бадмаева Римма  
Ведущий менеджер продуктов



## 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

# 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

*\* Обязательный компонент для сертификации по КСЗ, но не необходим УЦ. Требуется ViPNet CSP, может использоваться совместно с ViPNet HSM*

# VipNet УЦ 4.6: детали



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



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/128-4946 от "17" июля 2024 г.

Действителен до "28" февраля 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 комплексе согласно формуляру ФРКБ.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, утвержденным 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, утвержденным 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 ФРКБ.00114-07.30.01 ФО.

Временно исполняющий обязанности  
начальника Центра защиты информации  
и специальной связи ФСБ России



В.А. Шуринов

# ViPNet УЦ 4.6: сертификация

Два исполнения: средство УЦ КС2  
и КС3 для ОС Windows

Текущий сертификат действует  
до 28.02.2026

## 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

- ПAK **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

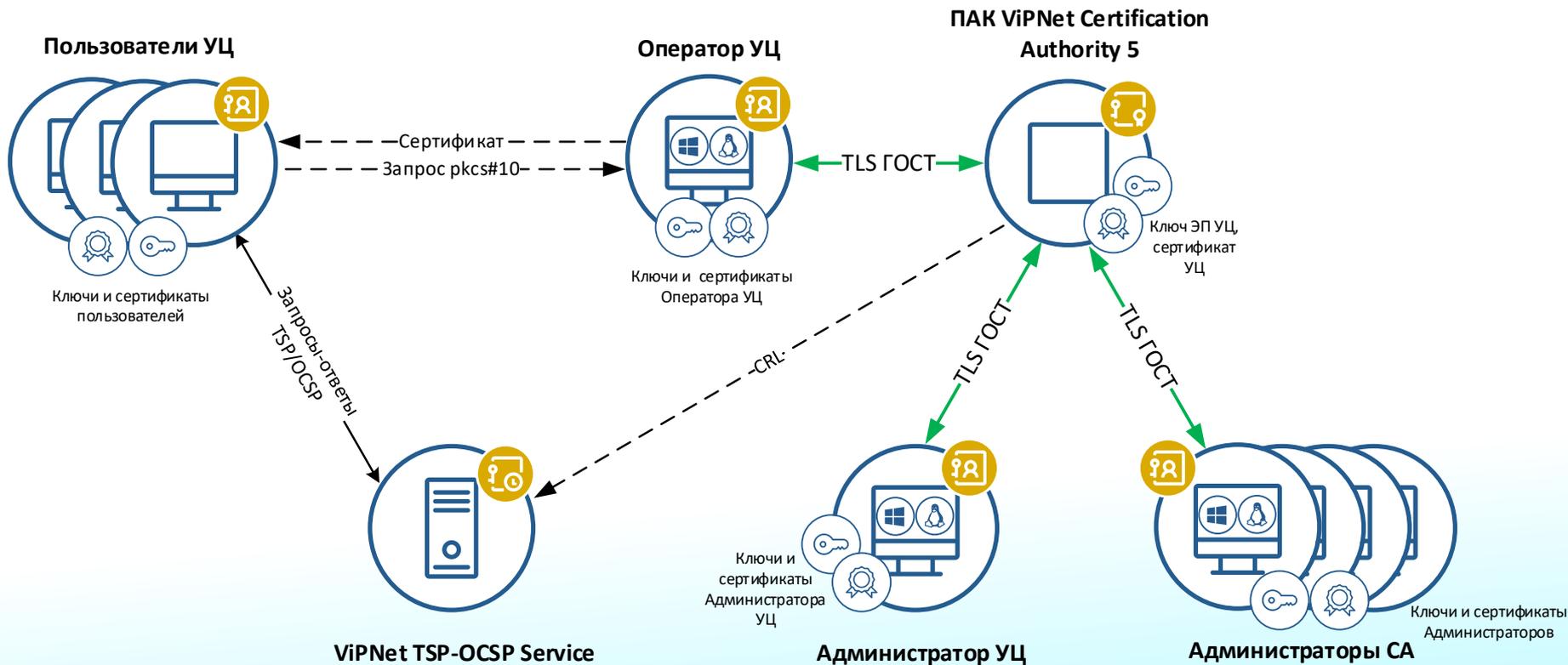


## VIPNet TSP-OCSP Service\*

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

*Без изменений*

# Схема работы УЦ



# VIPNet Certification Authority 5



Разрабатывается на базе криптографической платформы VIPNet HSM (как, например, сервер подписи VIPNet PKI service)



Аппаратная платформа –  
**HSM 5000 Q2**



СКЗИ и средство ЭП  
класса КВ/КВ2



Для тестирования доступна версия  
в виде VA (VirtualBox, VMWare, KVM)



# VIPNet Certification Authority 5



### ViPNet Certification Authority

- Центр сертификации
  - Реестр сертификатов**
  - Списки аннулированных сертификатов...
  - Запросы на сертификат УЦ
- Другие удостоверяющие центры
  - Сертификаты сторонних УЦ
- Система
  - Лицензия
  - Настройки

### Реестр сертификатов

Введите не менее 3 символов

[Издать сертификат](#) [Проверить статус сертификата](#)

Владелец	Статус	Дата издания	Окончание действия	Серийный номер
Соколов Сергей Маркович	Действителен	04.11.2024 13:32	04.02.2026 13:33	50400192F6BBD25F1234567...
Рогов Сергей Олегович	Действителен	04.11.2024 13:30	04.02.2026 13:31	50400192F6BA3C2E1234567...
Рогов Сергей Олегович	Действителен	04.11.2024 13:30	04.02.2026 13:31	50400192F6B9B38C1234567...
Request - 1177825 (Отсутств...	Действителен	04.11.2024 13:29	04.02.2026 13:30	50400192F6B90A1B1234567...
Request - 1177825 (Отсутств...	Действителен	04.11.2024 13:28	04.02.2026 13:29	50400192F6B8779B12345678...
123	Действителен	02.11.2024 16:04	02.11.2042 16:05	50400192ECFA351D1234567...
5_2 (hsm 1024)	Действителен	02.11.2024 15:19	10.09.2029 13:43	50400192ECD0B7981234567...
4_2 (файл1024)	Действителен	02.11.2024 15:08	10.09.2029 13:43	50400192ECC688221234567...
7(hsm512)	Действителен	01.11.2024 19:51	01.11.2042 19:52	50400192E8A3A5801234567...
6(файл512)	Действителен	01.11.2024 19:51	01.11.2027 19:52	50400192E8A3683612345678...
5 (hsm1024)	Действителен	01.11.2024 19:40	01.11.2042 19:40	50400192E899195512345678...
4 (файл1024)	Действителен	01.11.2024 19:39	01.11.2042 19:40	50400192E898BA3212345678...
3	Действителен	01.11.2024 19:33	01.11.2042 19:34	50400192E8934CED1234567...
2	Действителен	01.11.2024 19:10	01.11.2042 19:10	50400192E87DAD951234567...
12_подпись	Действителен	01.11.2024 12:35	01.11.2027 12:36	50400192E714394212345678...
Test Sub_CA	Действителен	01.11.2024 09:42	01.11.2027 09:43	50400192E6766C6712345678...
Соколов Алексей Иванович	Действителен	30.10.2024 07:46	30.10.2027 07:47	50400192DBBF2D951234567...
Петров Иван Иванович	Действителен	28.10.2024 16:26	28.10.2027 16:27	50400192D34E70A51234567...
Соколов Алексей Сергеевич	Срок действия истек	28.10.2024 09:33	28.10.2024 22:00	50400192D1D476861234567...
Рогов Вениамин Петрович	Срок действия истек	28.10.2024 09:31	28.10.2024 22:00	50400192D1D258BC1234567...
pendll512	Срок действия истек	28.10.2024 09:29	28.10.2024 09:30	50400192D1D066EE1234567...

### Соколов Сергей Маркович

Общие сведения История

[Открыть сертификат](#) [Открыть запрос](#)

#### Общие сведения

Статус: Действителен

Дата издания: 04.11.2024 13:32

Срок действия: 04.11.2024 13:33 - 04.02.2026 13:33

Серийный номер: 50400192F6BBD25F123456780000004F000000F4

Идентификатор ключа: 6FFC0C3A7D39A83F303D84AA72E44B876DEDF4D

Алгоритм ключа проверки ЭП: ГОСТ Р 34.10-2012 (512)

Параметры ключа проверки ЭП: Набор параметров А

#### Владелец сертификата

Общее имя владельца: Соколов Сергей Маркович

#### Издатель

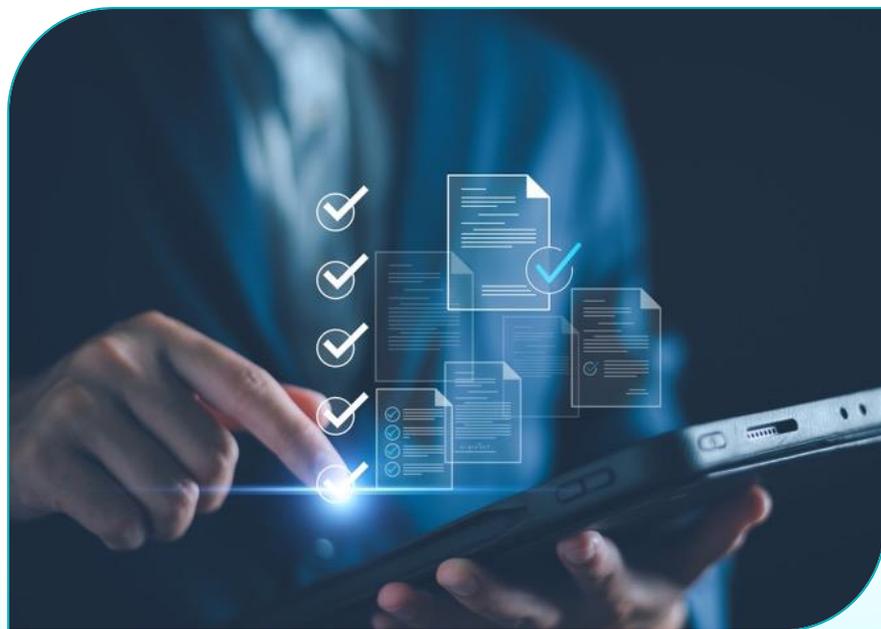
Общее имя владельца: Корневой УЦ

Идентификатор ключа: 8c1678acdc642f187e643d700f2ff1dbd022b1f

Серийный номер: 50400191FEC37F6C12345678000004F0000004F

[Аннулировать](#)

# VIPNet CA 5: основные функции



- Издание корневых сертификатов УЦ
- Формирование запросов в вышестоящий УЦ, запросов на кросс-сертификат
- Издание пользовательских сертификатов:
  - по запросу (pkcs#10)
  - с формированием ключевой пары
- Выдача сертификатов, в т.ч. в печатной форме
- Ведение реестра сертификатов
- Аннулирование сертификатов, выпуск CRL и т.д.

# Основные отличия от 4 поколения



-  Отдельный продукт, не связан с VipNet-сетями и VPN
-  Ядро УЦ – ПАК с ОС Linux
-  ОС для АРМ администраторов и операторов УЦ – Windows и Linux (СКЗИ VipNet PKI Client, исп. 3 и 6)
-  Возможность одновременного использования нескольких сертификатов УЦ для выпуска сертификатов

# 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

# 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)

# ViPNet УЦ 5: производительность

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

# Планы развития



ViPNet УЦ

Расширение перечня поддерживаемых АП

Поддержка западных алгоритмов

Разработка исполнений KB2 и KC1 (VA)

Кластер

TSP-OCSP Service  
(импортозамещение)

# ТЕХНО infotecs Фест

Подписывайтесь  
на наши соцсети,  
там много интересного

