

# Знакомьтесь: ViPNet Удостоверяющий центр 5



**Бадмаева Римма**

Руководитель продуктового направления

## 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

# VipNet УЦ 4.6: детали

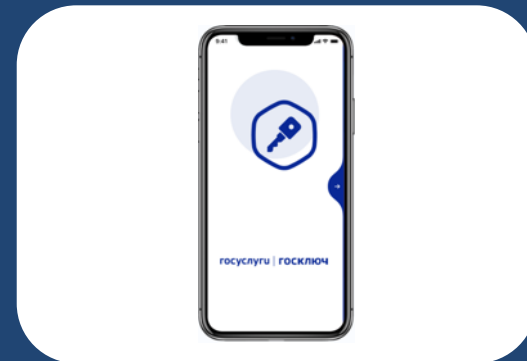


## Совместная работа с VipNet HSM

(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/128-5392 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, 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 ФРКЕ.00114-07 30 01 ФО.

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

О.В. Скрыбин

# 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

- Импортзамещение
- 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

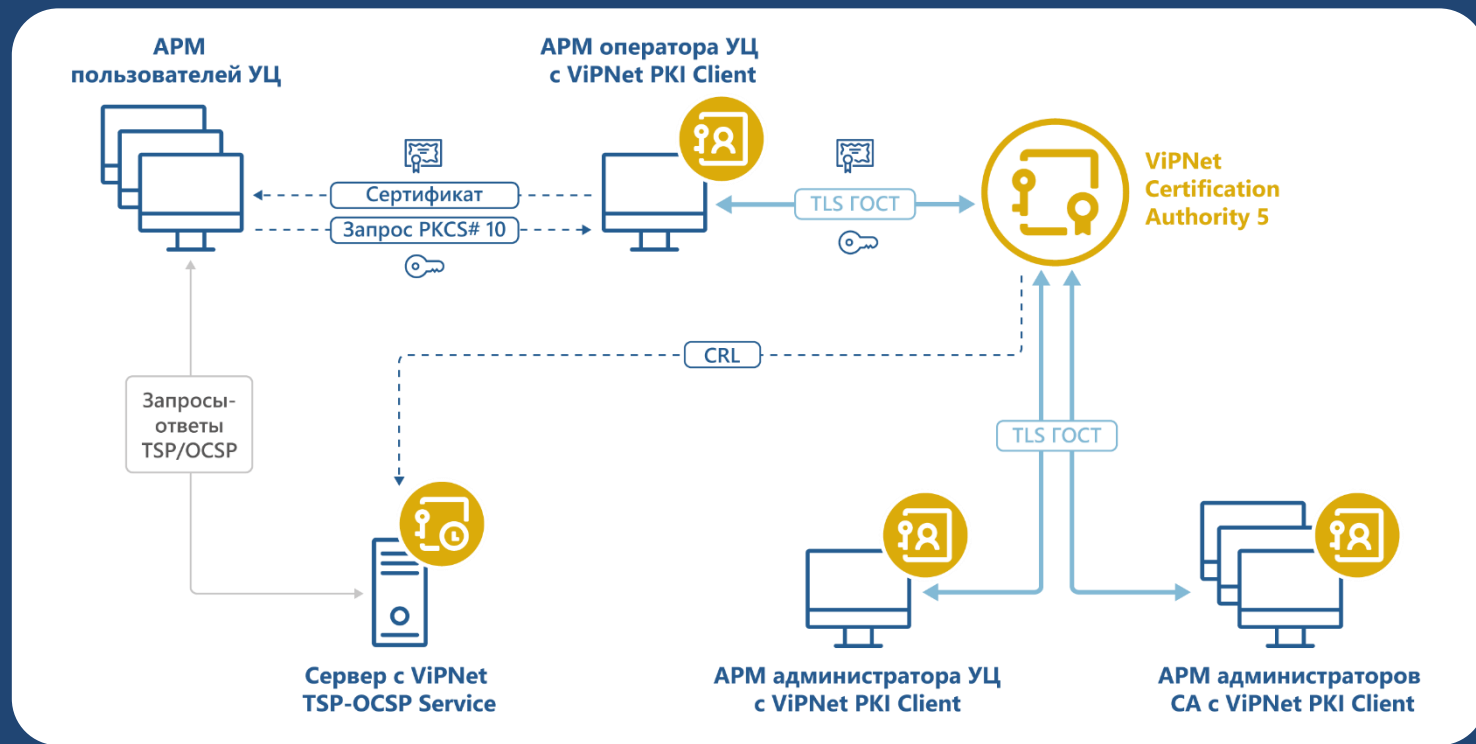
АРМ оператора УЦ с **СКЗИ VIPNet PKI Client 2.0** для подключения к web-интерфейсу **VIPNet CA**



## **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

The screenshot displays the 'Реестр сертификатов' (Certificate Registry) section of the VIPNet Certification Authority 5. The interface includes a search bar at the top with the text 'Введите не менее 3 символов' and buttons for 'Исдать сертификат' and 'Проверить статус сертификата'. Below the search bar is a table listing certificates with columns for 'Владелец' (Owner), 'Статус' (Status), 'Дата издания' (Issue Date), 'Окончание действия' (Expiration Date), and 'Серийный номер' (Serial Number). The first entry is for 'Рогов Вадим Иванович' with a status of 'Действителен' (Valid).

Владелец	Статус	Дата издания	Окончание действия	Серийный номер
Рогов Вадим Иванович	Действителен	02.09.2025 13:54	02.09.2030 13:53	5080019909A251A51234567...
Сергеев Вениамин Дмитри...	Действителен	02.09.2025 13:53	02.09.2030 10:18	5080019909A1531012345678...
Рогов Александр Алексеевич	Действителен	02.09.2025 13:53	02.09.2030 10:18	5080019909A152E912345678...
Рогов Вадим Дмитриевич	Действителен	02.09.2025 13:53	02.09.2030 10:18	5080019909A152CF1234567...
Кружков Борис Маркович	Действителен	02.09.2025 13:53	02.09.2030 10:18	5080019909A152AC1234567...
Иванов Дмитрий Вадимович	Действителен	02.09.2025 13:53	02.09.2030 10:18	5080019909A1528612345678...
Иванов Дмитрий Алексеевич	Действителен	02.09.2025 13:53	02.09.2030 10:18	5080019909A1526012345678...
Ульянов Александр Вадимо...	Действителен	02.09.2025 13:53	02.09.2030 10:18	5080019909A1523912345678...
Петров Вадим Сергеевич	Действителен	02.09.2025 13:53	02.09.2030 10:18	5080019909A1520612345678...
Кружков Борис Алексеевич	Действителен	02.09.2025 13:53	02.09.2030 10:18	5080019909A151E812345678...
Рогов Виктор Сергеевич	Действителен	02.09.2025 13:53	02.09.2030 10:18	5080019909A151C11234567...
Соколов Борис Олегович	Действителен	02.09.2025 13:53	02.09.2030 10:18	5080019909A1519912345678...
Иванов Вадим Вадимович	Действителен	02.09.2025 13:53	02.09.2030 10:18	5080019909A1517112345678...
Рогов Вениамин Дмитриевич	Аннулирован	02.09.2025 13:53	02.09.2030 10:18	5080019909A1514712345678...
Сергеев Виктор Иванович	Действителен	02.09.2025 13:53	02.09.2030 10:18	5080019909A1512112345678...
Соколов Виктор Петрович	Действителен	02.09.2025 13:53	02.09.2030 10:18	5080019909A1509A12345678...
Соколов Вениамин Алексее...	Действителен	02.09.2025 13:53	02.09.2030 10:18	5080019909A150071234567...
Петров Сергей Алексеевич	Действителен	02.09.2025 13:53	02.09.2030 10:18	5080019909A1508312345678...
Сергеев Вениамин Алексее...	Действителен	02.09.2025 13:53	02.09.2030 10:18	5080019909A1508F12345678...
Иванов Александр Маркович	Действителен	02.09.2025 13:53	02.09.2030 10:18	5080019909A1504B12345678...
Рогов Вадим Алексеевич	Действителен	02.09.2025 13:53	02.09.2030 10:18	5080019909A1505212345678...
Сергеев Виктор Дмитриевич	Действителен	02.09.2025 13:53	02.09.2030 10:18	5080019909A1502F12345678...
Ульянов Виктор Дмитриевич	Действителен	02.09.2025 13:53	02.09.2030 10:18	5080019909A1500B12345678...
Кружков Виктор Маркович	Действителен	02.09.2025 13:53	02.09.2030 10:18	5080019909A14FE612345678...
Дмитриев Александр Петро...	Действителен	02.09.2025 13:53	02.09.2030 10:18	5080019909A14FBA1234567...
Дмитриев Олег Олегович	Аннулирован	02.09.2025 13:53	02.09.2030 10:18	5080019909A14F9E12345678...
Ульянов Петр Вадимович	Действителен	02.09.2025 13:53	02.09.2030 10:18	5080019909A14F7412345678...
Петров Алексей Вадимович	Действителен	02.09.2025 13:53	02.09.2030 10:18	5080019909A14F5012345678...
Ульянов Олег Олегович	Действителен	02.09.2025 13:53	02.09.2030 10:18	5080019909A14F2B12345678...

On the right side, the details for the selected certificate are shown for 'Рогов Вадим Иванович'. The 'Общие сведения' (General Information) section includes fields for 'Статус' (Status: Действителен), 'Дата издания' (Issue Date: 02.09.2025 13:54), 'Срок действия' (Validity Period: 02.09.2025 13:54 - 02.09.2030 13:53), 'Срок действия ключа ЭП' (Signature Key Validity Period: 02.09.2025 13:53 - 02.09.2028 13:53), 'Серийный номер' (Serial Number: 5080019909A251A512345678000000980000099), and 'Идентификатор ключа' (Key Identifier: 852330C2C282CC7250FDA1FA7A2C493B6A5638). The 'Владелец сертификата' (Certificate Owner) section lists 'Рогов Вадим Иванович' with his full name, address (Льва Толстого, 26), organization (ООО Континент), and position (Старший инженер). The 'Издатель' (Issuer) section identifies the issuer as 'Головной удостоверяющий центр' (Main Certification Center) with key identifier 'e34963f5760b9d152b484f0308905f48d3a3f27'.

# ViPNet CA 5: основные функции

Издание пользовательских сертификатов:

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

Аннулирование сертификатов, выпуск CRL и т.д.

Ведение реестра сертификатов

Издание корневых сертификатов УЦ

Формирование запросов в вышестоящий УЦ, запросов на кросс-сертификат

Выдача сертификатов, в т.ч. в печатной форме

# 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 отзыванных сертификатов	50 Мб
Время издания CRL с 1 млн отзыванных сертификатов	50 сек

# VIPNet УЦ: планы развития



---

Расширение  
перечня  
поддержива  
емых АП



---

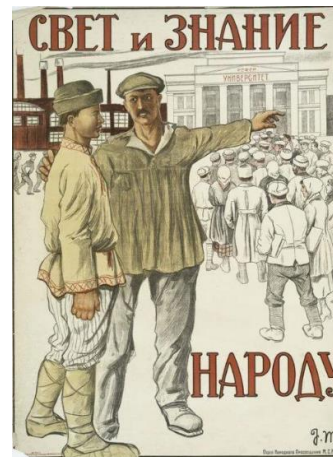
Разработка  
исполнений  
KB2 и KC1  
(VA)



---

Поддержка  
западных  
алгоритмов

# Криптография в финтехе теперь в МАХ!



САНКТ  
ПЕТЕРБУРГ

инфотекс  
ТЕХНОДЕСТ

Подписывайтесь  
на наши соцсети



инфотекс  
Академия



AMPIRE

TELEOFIS

КОМФОРТЕЛ  
оператор связи бизнес-клинов

РУТОНЕН  
оператор связи бизнес-клинов

TS Solution

AXOFT