САЙФЕР

Технологія хмарного підпису

Сучасні підходи

ТОВ “Сайфер ПРО”:
Влад Ковтун, Андрій Охріменко
Микола Байбуз, Олександр Стокіпний

Agenda

- Задача
- Варіанти рішення
- Рішення від Сайфера
  - Шифр-CKS
  - Шифр-HSM
- Переваги
- Питання ...

Задача

- Зберігати ключі у Засобі КЕП
- Ставити швидко ЕП і швидко узгоджувати ключі
- Ставити багато ЕП і багато разів узгоджувати ключі
- Висока надійність - працювати безперервно більше ніж 8 годин кожен день

- ID-Card
- Smart Card & USB-Token
- Sim Card

- Hardware Secure Module

Нормативні вимоги

- Закон України Про електронні довірчі послуги
- Закон України Про електронні документи і електронний документообіг
- REGULATION (EU) No 910/2014 OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL of 23 July 2014 on electronic identification and trust services for electronic transactions in the internal market and repealing Directive 1999/93/EC

Нормативні специфікації

- **CEN/EN 419 241-1 Trustworthy Systems Supporting Server Signing - Part 1: General System Security Requirements**
- **CEN/EN 419 241-2 Trustworthy Systems Supporting Server Signing Part 2, Protection Profile for QSCD for Server Signing**
- CEN/EN 419 221-1 Protection profiles for secure signature creation device - Part 1: Overview
- CEN/EN 419 221-2 Protection profiles for secure signature creation device - Part 2: Device with key generation
- CEN EN 419 221-5 Protection profiles for secure signature creation device - Part 5: Extension for device with key generation and trusted channel to signature creation application
- **ETSI TS 119 431 ESI; Policy and security requirements for trust service providers; Part 1: TSP service components operating a remote QSCD / SCDev**
- ETSI TS 119 431 ESI; Policy and security requirements for trust service providers; Part 2: TSP service components supporting AdES digital signature creation
- ETSI TS 119 432 ESI; Protocols for remote digital signature creation

Нормативні специфікації

- ETSI EN 319 411-1 Policy and security requirements for Trust Service Providers issuing certificates. Part 1: General requirements
- ETSI EN 319 401 ESI; General Policy Requirements for Trust Service Providers
- ETSI TS 119 101 ESI; Policy and security requirements for applications for signature creation and signature validation
- ETSI TS 119 102-1 ESI; Procedures for Creation and Validation of AdES Digital Signatures; Part 1: Creation and Validation
- Cloud Signature Consortium (CSC) specification

Що пропонується?

Шифр-Cloud Key Storage

* - Наявні експертні висновки Держспецзв'язку України

Шифр-CKS

- Централізована система
- Мікросервісна архітектура
- Контейнеризація і стекування мікросервісів
- Системи оркестрації (Docker Swarm, OpenShift, Kubernetes, інші)
- REST API (JSON)
- HTTPS/TLS v1.2
- Додаткове шифрування чутливих параметрів

- ДСТУ 4145:2002+ГОСТ 34.311-95+ДСТУ ГОСТ 28147:2009
- ECDSA+SHA+AES
- RSA+SHA+AES
- ДСТУ 4145:2002+ДСТУ 7564:2014+ДСТУ 7624:2014 – **у роботі (тестування на сумісність)**

Шифр-CKS: Управління

- Користувачами (Auth)
  - Створення
  - Видалення
  - Блокування
  - Відновлення
  - Зміна паролю
  - Інформація
  - Другий фактор
    - Google Authenticator
    - Email
    - Push+SMS
    - Інші на вимогу
- Віртуальними носіями (vTMS)
  - Створення і ініціалізація (PIN+PUK)
  - Видалення
  - Блокування (на рівні vTMS)
  - Відновлення (на рівні vTMS)
  - Зміна PIN (за відомим PIN)
  - Відновлення PIN (за відомим PUK)
  - Генерація ключів
  - Видалення об’єктів (особистий ключ, сертифікат, запит на сертифікат)

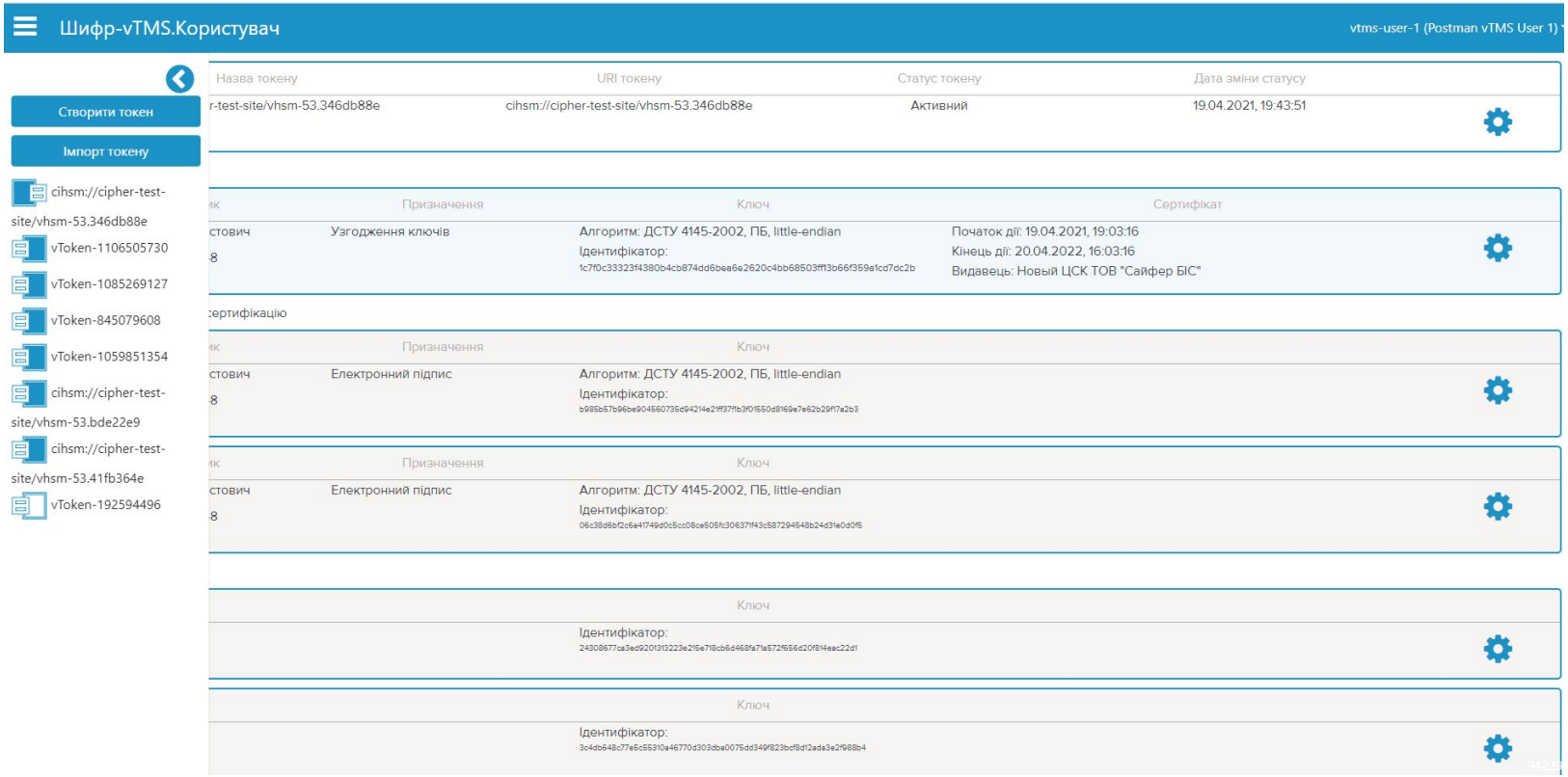
Шифр-CKS: Криптографічні операції

- Разові операції (дані*, хеш)
  - Підписання
  - Зашифрування
  - Розшифрування
- Пакетні операції (дані*, хеш)
  - Підписання
  - Зашифрування
  - Розшифрування
- Безпека
  - HTTPS/TLS
  - Дані шифруються симетричним шифром (**AES**, ДСТУ 7624) на випадковому ключі
  - Випадковий симетричний ключ шифрується публічним **RSA**/ECDH ключем сервісу
  - Обмеження строку дії шифрованих даних на симетричному ключі
  - Обмеження строку дії ключа **RSA**/ECDH

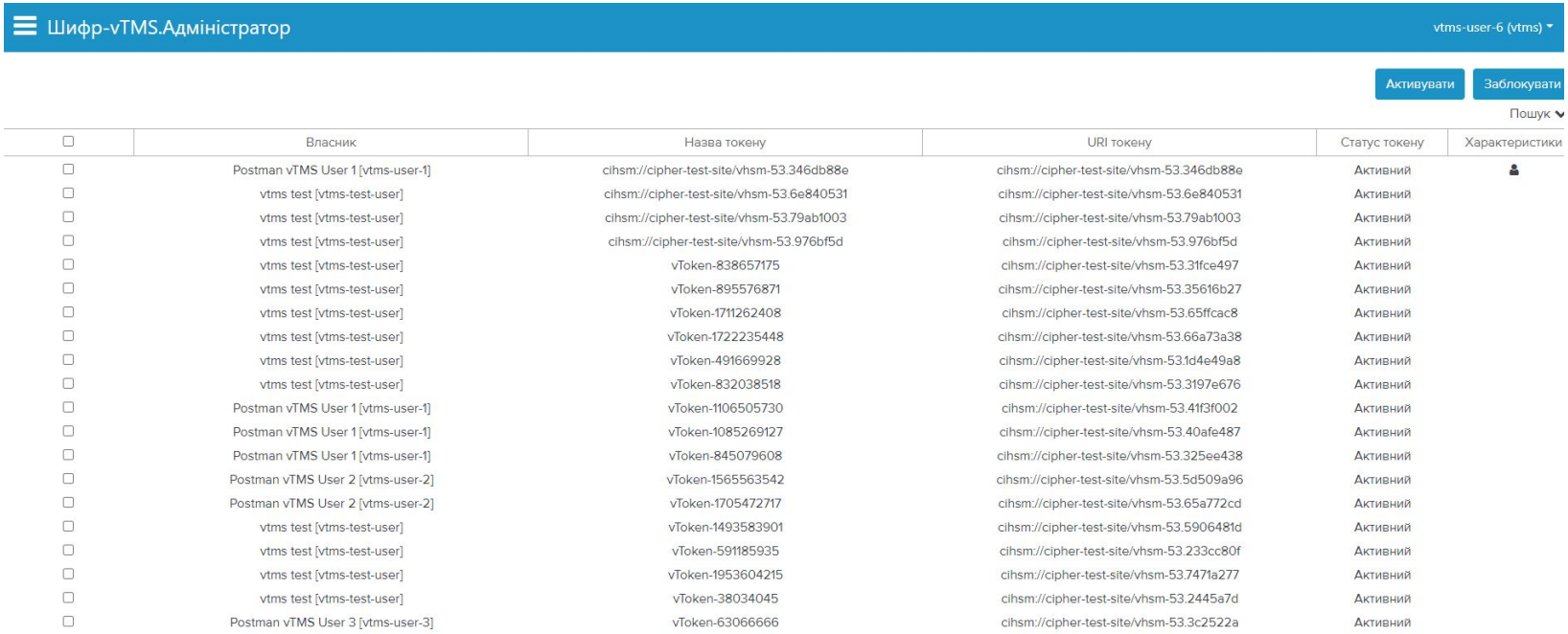
* - невеликі за обсягом дані, закодовані у Base64

САЙФЕР

Шифр-CKS: Обслуговування

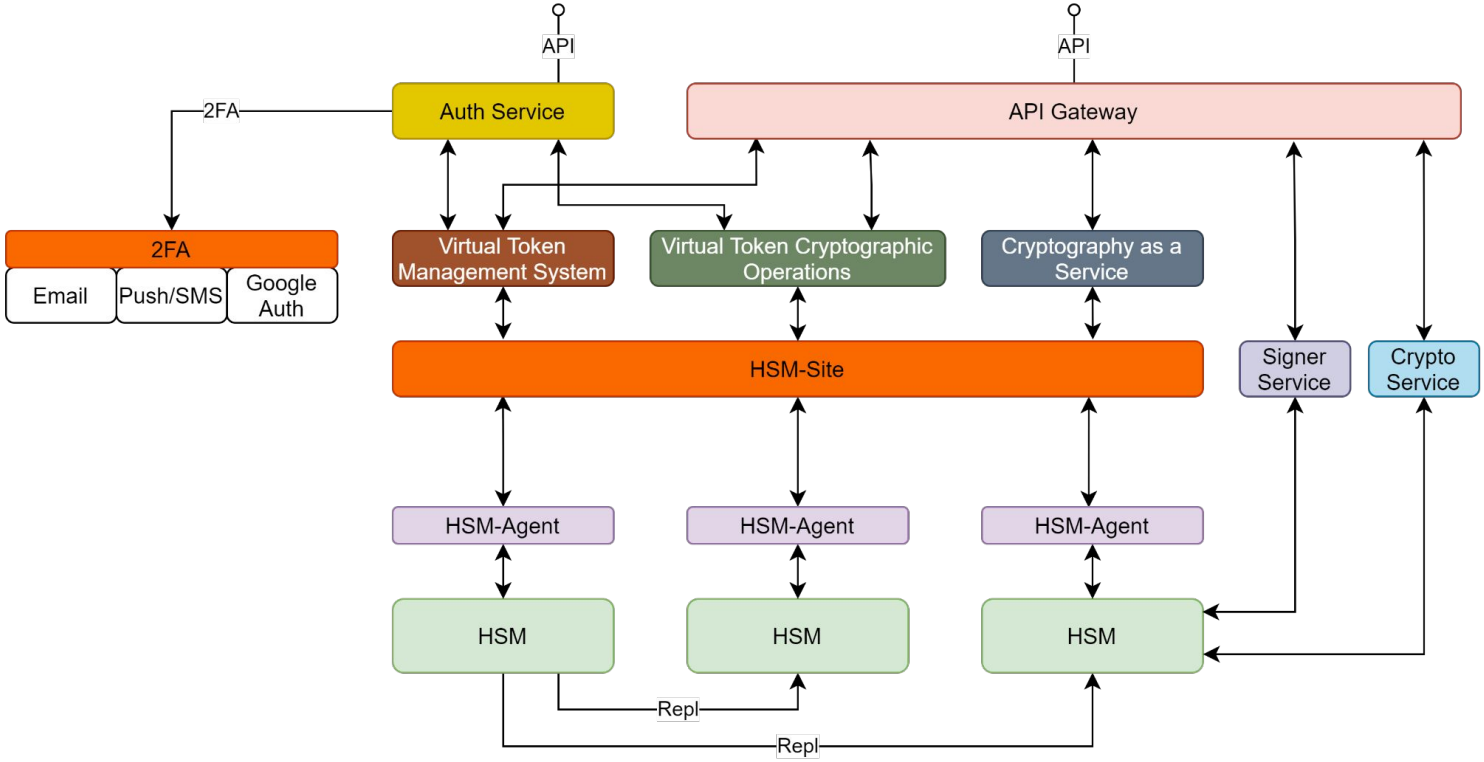


Шифр-CKS: Обслуговування



Власник	Назва токену	URI токену	Статус токену	Характеристики
Postman vTMS User 1 [vtms-user-1]	cihsm://cipher-test-site/vhsm-53.346db88e	cihsm://cipher-test-site/vhsm-53.346db88e	Активний	
vtms test [vtms-test-user]	cihsm://cipher-test-site/vhsm-53.6e840531	cihsm://cipher-test-site/vhsm-53.6e840531	Активний	
vtms test [vtms-test-user]	cihsm://cipher-test-site/vhsm-53.79ab1003	cihsm://cipher-test-site/vhsm-53.79ab1003	Активний	
vtms test [vtms-test-user]	cihsm://cipher-test-site/vhsm-53.976bf5d	cihsm://cipher-test-site/vhsm-53.976bf5d	Активний	
vtms test [vtms-test-user]	vToken-838657175	cihsm://cipher-test-site/vhsm-53.31fce497	Активний	
vtms test [vtms-test-user]	vToken-895576871	cihsm://cipher-test-site/vhsm-53.35616b27	Активний	
vtms test [vtms-test-user]	vToken-1711262408	cihsm://cipher-test-site/vhsm-53.65ffcac8	Активний	
vtms test [vtms-test-user]	vToken-1722235448	cihsm://cipher-test-site/vhsm-53.66a73a38	Активний	
vtms test [vtms-test-user]	vToken-491669928	cihsm://cipher-test-site/vhsm-53.1d4e49a8	Активний	
vtms test [vtms-test-user]	vToken-832038518	cihsm://cipher-test-site/vhsm-53.3197e676	Активний	
Postman vTMS User 1 [vtms-user-1]	vToken-1106505730	cihsm://cipher-test-site/vhsm-53.41f3f002	Активний	
Postman vTMS User 1 [vtms-user-1]	vToken-1085269127	cihsm://cipher-test-site/vhsm-53.40afe487	Активний	
Postman vTMS User 1 [vtms-user-1]	vToken-845079608	cihsm://cipher-test-site/vhsm-53.325ee438	Активний	
Postman vTMS User 2 [vtms-user-2]	vToken-1565563542	cihsm://cipher-test-site/vhsm-53.5d509a96	Активний	
Postman vTMS User 2 [vtms-user-2]	vToken-1705472717	cihsm://cipher-test-site/vhsm-53.65a772cd	Активний	
vtms test [vtms-test-user]	vToken-1493583901	cihsm://cipher-test-site/vhsm-53.5906481d	Активний	
vtms test [vtms-test-user]	vToken-591185935	cihsm://cipher-test-site/vhsm-53.233cc80f	Активний	
vtms test [vtms-test-user]	vToken-1953604215	cihsm://cipher-test-site/vhsm-53.7471a277	Активний	
vtms test [vtms-test-user]	vToken-38034045	cihsm://cipher-test-site/vhsm-53.2445a7d	Активний	
Postman vTMS User 3 [vtms-user-3]	vToken-63066666	cihsm://cipher-test-site/vhsm-53.3c2522a	Активний	

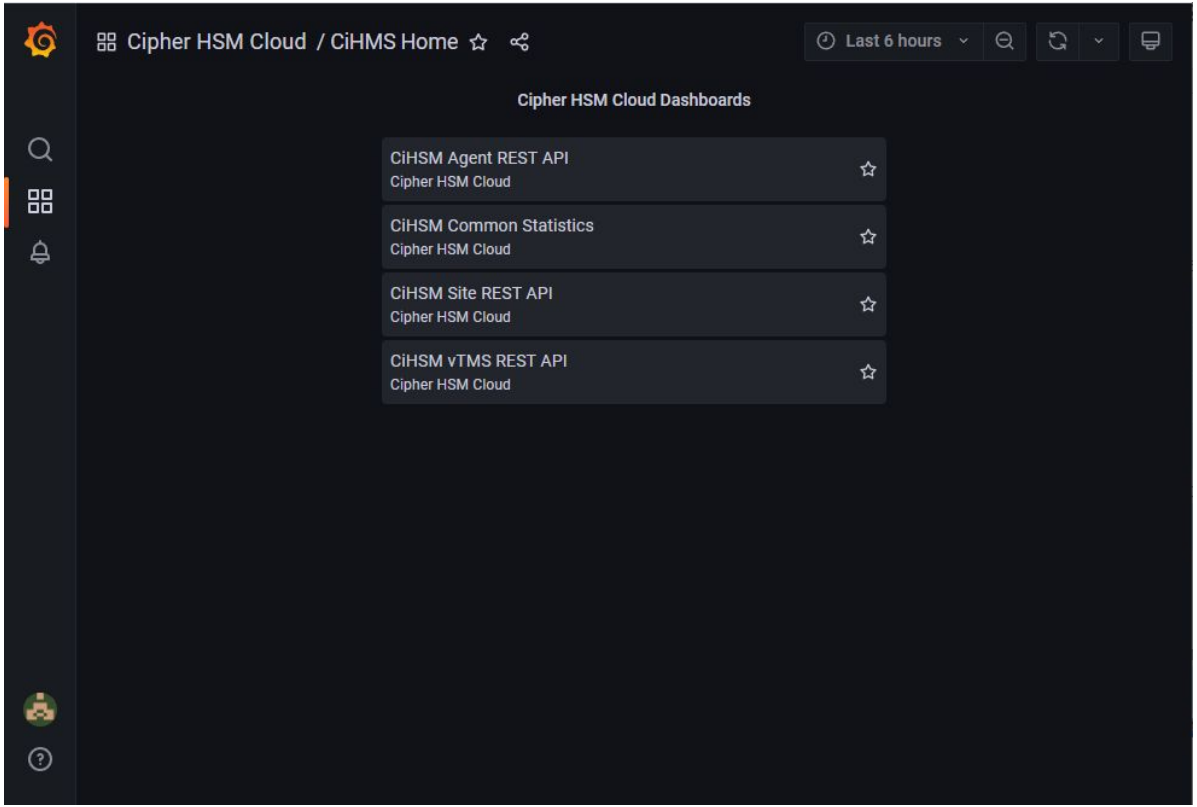
Шифр-CKS: Архітектура



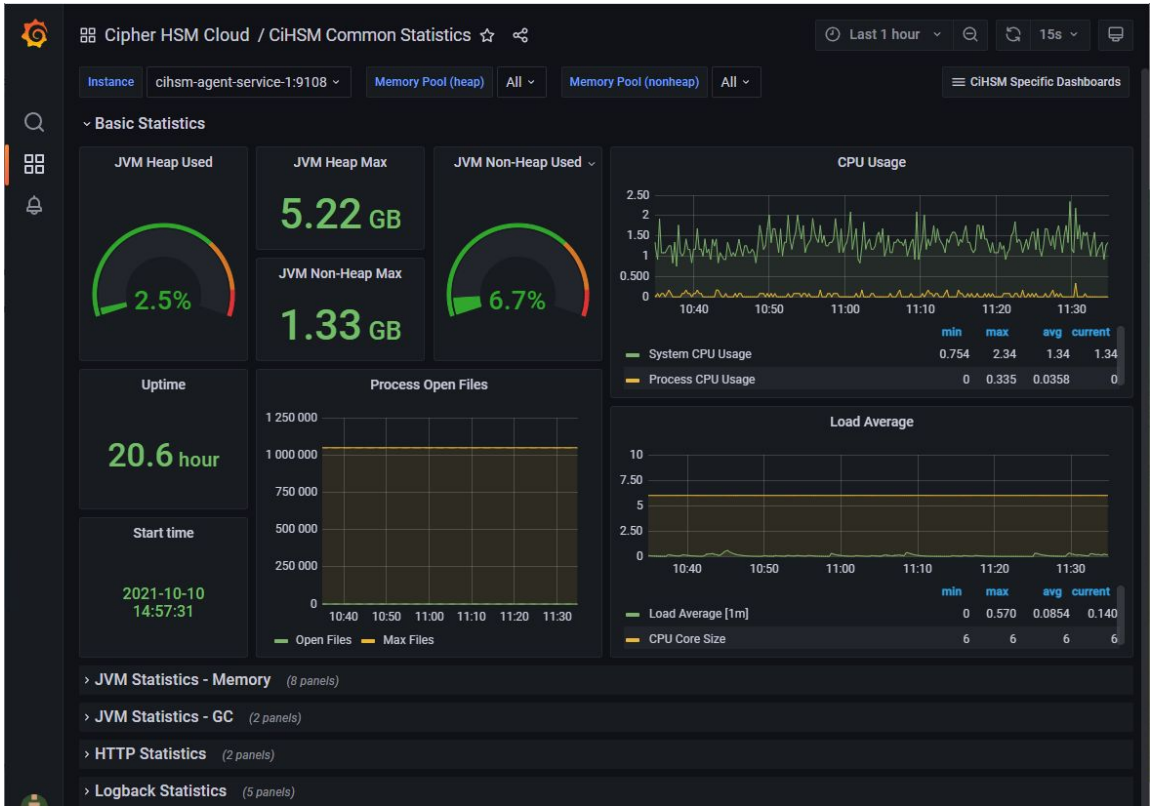
Сайфер Шифр-CKS

Моніторинг

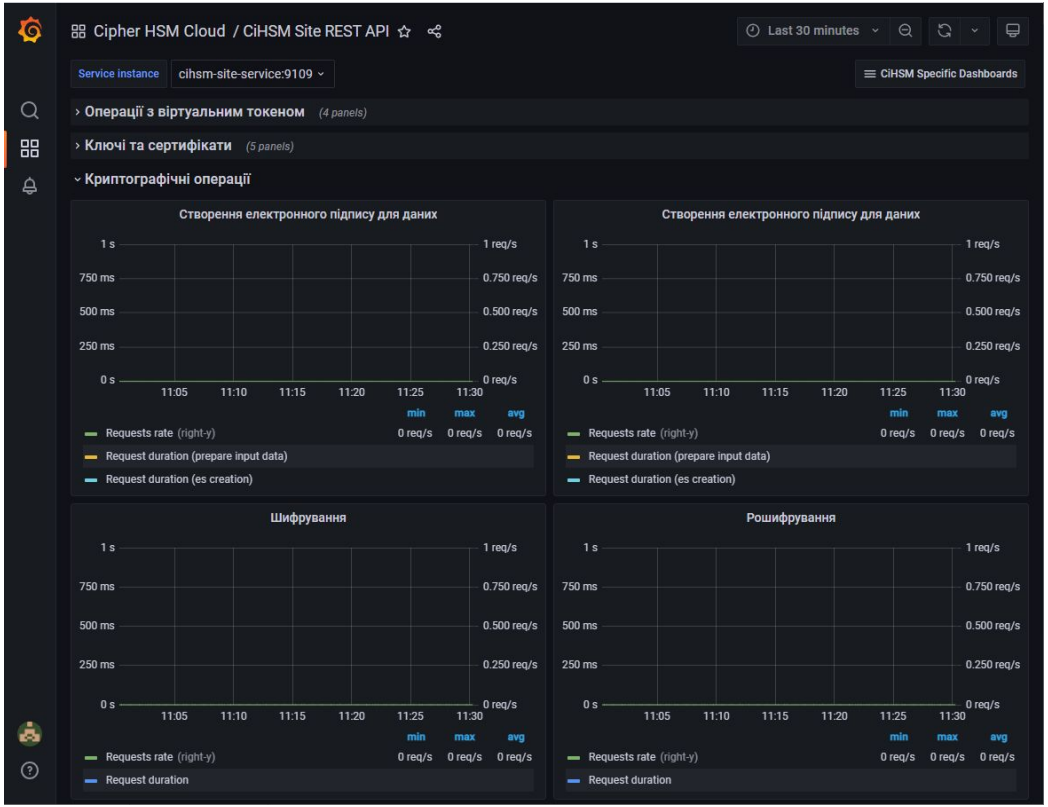
Моніторинг: всі підсистеми



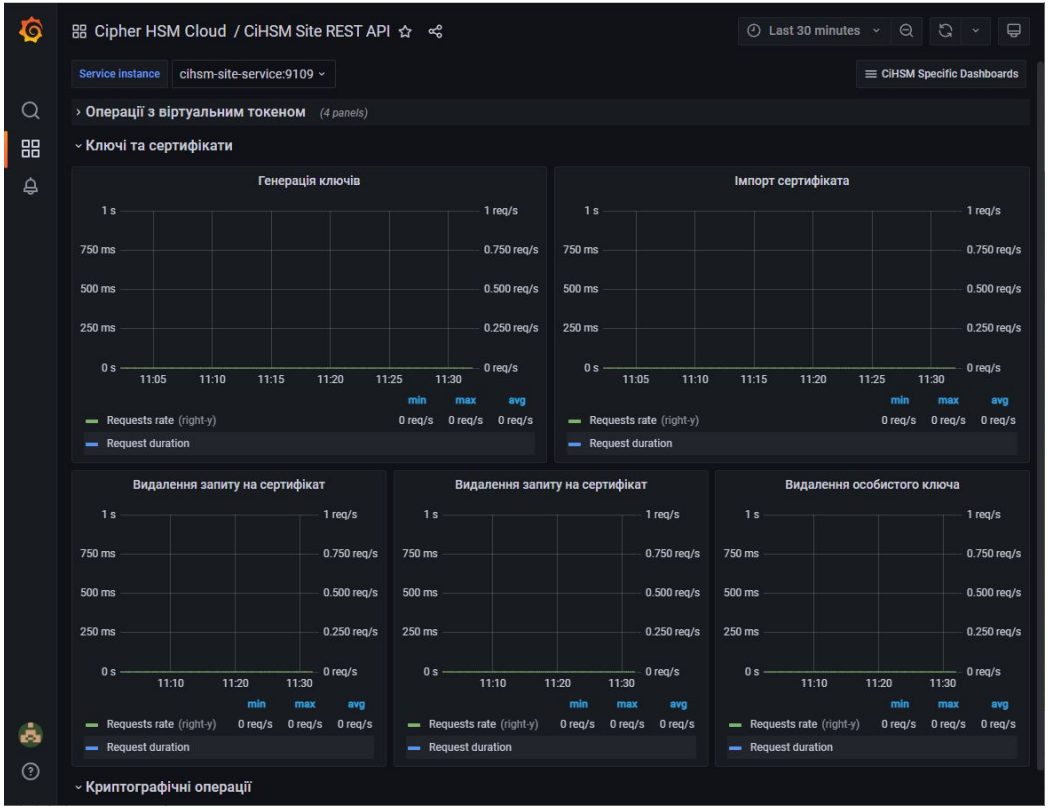
Моніторинг: загальна стстистика



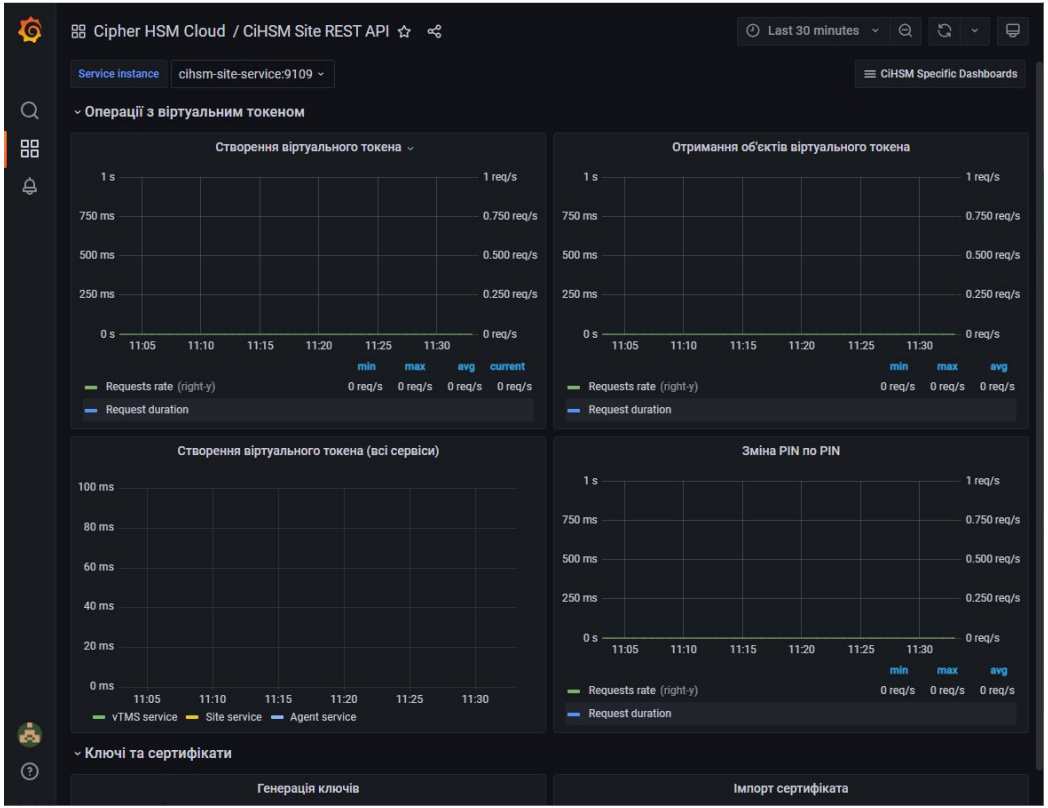
Моніторинг: Сайфер-HSM-Site: Криптоопераці



Моніторинг: Сайфер-HSM-Site: Об’єкти



Моніторинг: Сайфер-HSM-Site: Носії



Що пропонується?

Мережний криптомодуль Шифр-HSM

* - Наявні експертні висновки Держспецзв'язку України

Переваги від HSM

- Відповідність вимогам КЕП
- Висока швидкодія криптографічних операцій
- Паралельна обробка запитів
- Підтримка великої кількості криптографічних алгоритмів (вітчизняних і міжнародних)
- Безпека зберігання ключів та іншої секретної інформації
- Можливість резервування та реплікація стану
- Інтеграція з великою кількістю систем:
  - Через бібліотеку PKCS#11
  - Через інтеграційний модуль Шифр-HSM-Agent, Шифр-HSM-Site
  - Через інтеграційний модуль Шифр-Signer, Шифр-Crypto
- Висока надійність
- Горизонтальне масштабування (розподілення ключів - CiHSM vTMS, маршрутизація - CiHSM-Site)
- Балансування запитів між кількома HSM (маршрутизація CiHSM-Site)

Переваги від HSM

- Віддалене управління і моніторинг
- Віддалена ініціалізація і запуск (без необхідності фізичного контакту)
- Захист каналів зв'язку:
  - Реплікації
  - Управління
  - Резервного копіювання
  - Використання
- Розподіл ключа шифрування секретних даних між кількома адміністраторами
- Можливість змін у комплектації

Мережний криптомодуль Шифр-HSM

Опис

- Форм-фактор: Rack Mount 19”, 1U
- Фізичний захист корпусу
- Внутрішній замок
- Датчики проникнення і вскриття
- Фізичне знищення сховища
- Автономна робота від акумуляторів засобу захисту
- Безпечне завантаження (Secure Boot)
- БП: 1/2
- Network (1/10 Gigabit Ethernet): RJ-45/SFP

Підтримка клієнтських платформ

- Windows x86/x86-64
- Linux x86/x86-64
- MacOS x86-64 (планується)
- Linux ARMv7/ARMv8 (планується)

Комплектність: Базова

Комплектність	Ключів, тис. шт	Одночасних сесій	Захищене сховище, ГБ
Початковий	30	256	256
Стандартний	60	512	256
Продуктивний	90	1024	256

Комплектність: Внутрішня

Комплектність	Ключів, тис. шт	Одночасних сесій	Захищене сховище, ТБ
Початковий	300	1536	0,5
Стандартний	500	2048	1
Продуктивний	900	4096	1

Продуктивність ЕП (Базовий-Стандартний)

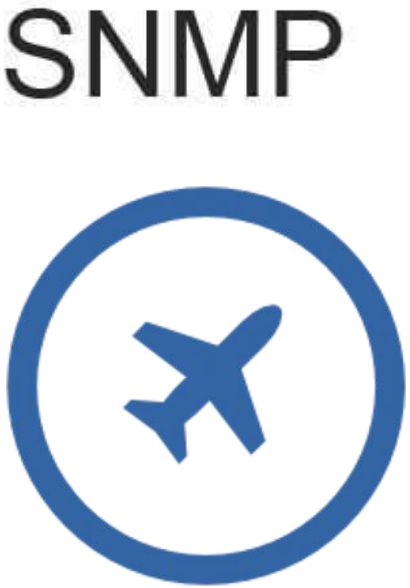
Операція	Довжина ключа, біт	Швидкість, ЕП/с
Формування (ДСТУ 4145-2002)	257	5000
Формування (ECDSA)	256	4000
Формування (RSA)	2048	1000
Формування (RSA)	4096	650

Продуктивність ЕП (Внутрішній-Стандартний)

Операція	Довжина ключа, біт	Швидкість, ЕП/с
Формування (ДСТУ 4145-2002)	257	10000
Формування (ECDSA)	256	8500
Формування (RSA)	2048	2000
Формування (RSA)	4096	1390

Моніторинг: Сайфер Шифр-HSM

- SNMP
- Cockpit



Запитання?

ТОВ “Сайфер ПРО”

Влад Ковтун: vk@cipher.com.ua

Андрій Охріменко: ao@cipher.com.ua

Микола Байбуз: nb@cipher.com.ua

Олександр Стокіпний: as@cipher.com.ua

www: https://cipher.com.ua