САЙФЕР

Хмарна платформа Сайфер для комплексної роботи з електронним підписом

Мережний криптографічний модуль

ТОВ “Сайфер ПРО”:
Влад Ковтун

Agenda

- Задачі
- Можливе рішення – хмарна платформа
  - Сайфер Шифр-CaaS
  - Сайфер Шифр-HSM
- Token-over-IP
- Питання ...

Задача: Розмаїття

- Захищених носіїв
- Форматів ключів різних виробників
  - АТ ІІТ, ТОВ Сайфер, ТОВ Автор, ТОВ НОКК, ТОВ АЦСК Украина
- Провайдерів MobileID
  - Vodafone, LifeCell, KyivStar
- КНЕДП побудованих на технологіях
  - АТ ІІТ, ТОВ Сайфер, ТОВ Автор, ТОВ НОКК, ТОВ АЦСК Украина
- Сервісів роботи з захищеними хмарними сховищами ключій (АТ ІІТ, ТОВ Сайфер)
- Систем і технологій для впровадження і інтеграцій

Задача: Середовище

- Зміни у нормативній базі
- Кожний розробник засобів КЗІ вносить свій внесок до розмаїття реалізацій
- Зворотна сумісність
- Швидкі зміни вимоги бізнес-замовників - швидкі оновлення
- Развиток технологій
- Високі навантаження і необхідність у масштабуванні
- Висока доступність
- Кілька датацентрів
- Середовища віртуалізації (публічні, приватні та гибридні хмари)

Задачі: Дуже прості

- Генерація і зберігання ключів (у вигляді, що унеможливлює вилучення з пристрою)
- Генерація запитів на сертифікат і видання сертифікатів
- Можливість зберігати кілька ключів для цілого спектру алгоритмів
- Захист ключів від несанкціонованого доступу
- Виконання криптографічних перетворень (багато, швидко і паралельно)
- Контроль за використанням і адміністрування

Чи існують рішення в таких умовах?

Так! Існує! **Шифр-CaaS**

Рішення існує! Шифр-CaaS

- Централізована система
- Агенти на робочих місцях користувачів
- Микросервисна архитектура
- Пакування мікросервісів у контейнер
- Системи оркестрації (Docker Swarm, Kubernetis)
- REST API (JSON)
- HTTPS/TLS v1.2 (на базі Шифр+ v2.5)

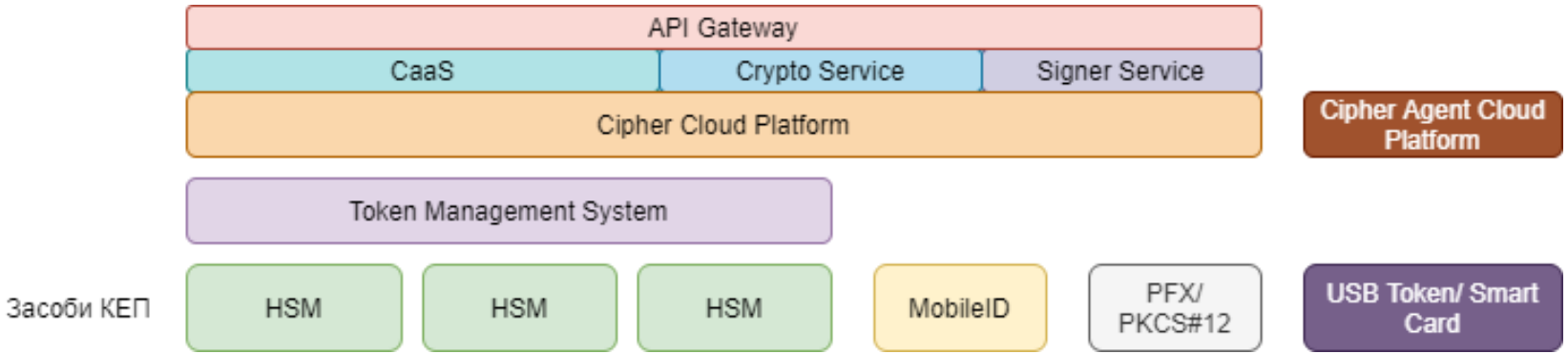
Переваги від Шифр-CaaS

- Централізована система
- Микросервисная архитектура
- Пакування мікросервісів у контейнер
- Системи оркестрації (Docker Swarm, Kubernetis,…)
  - Масштабування
  - Відмовостійкість
  - Ефективність використання ресурсів
  - Гнучкість
  - CI/CD
- REST API (JSON)
  - Легкість інтеграції
- HTTPS/TLS v1.2 (на базі Шифр+ v2.5)
  - Автентифікація і конфіденційність
- Агенти на робочих місцях користувачів

Алгоритми:

- 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

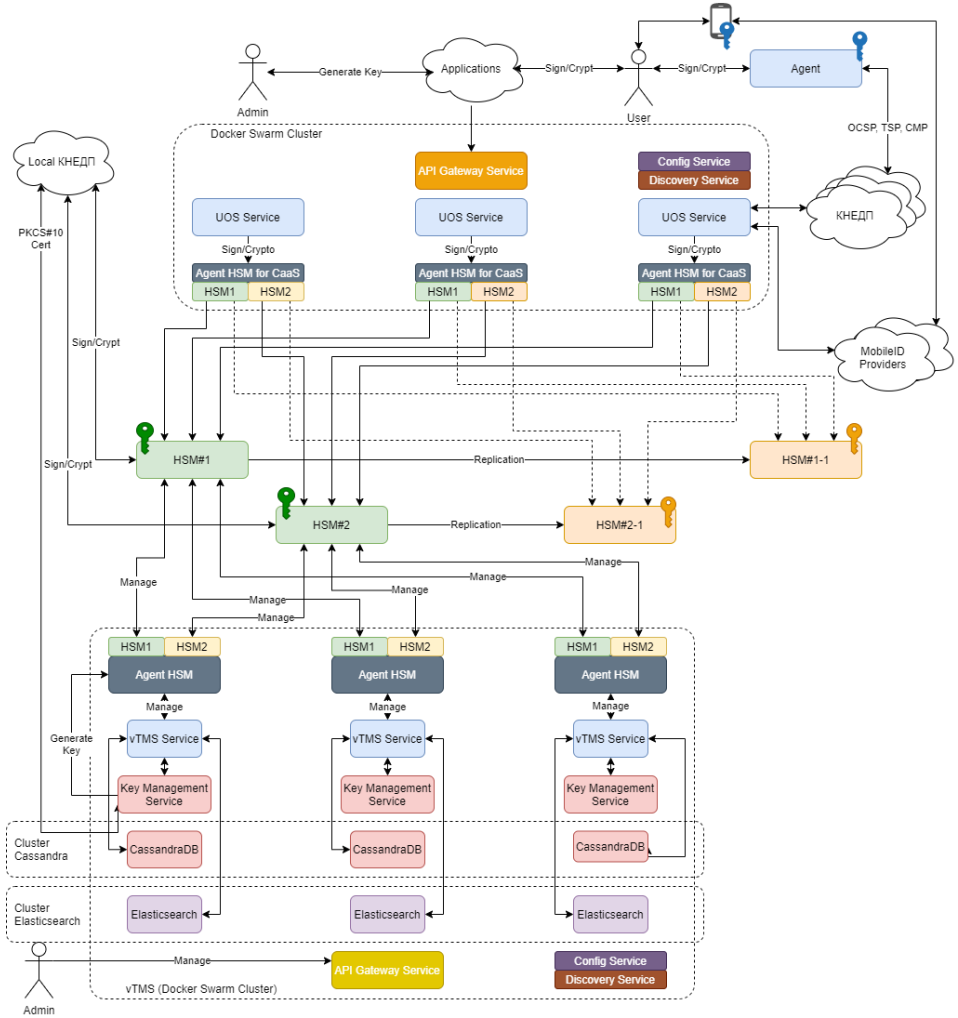
Рішення існує



САЙФЕР

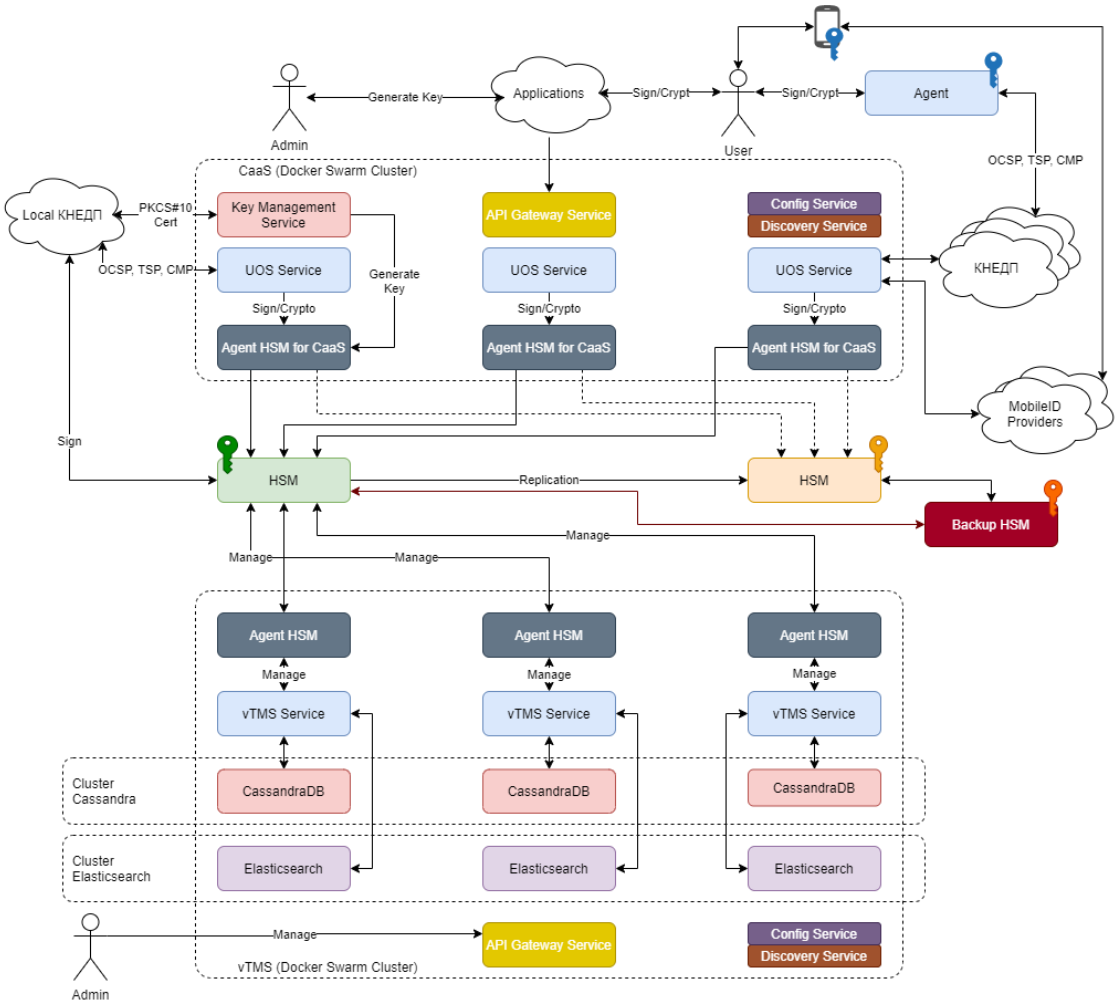
Рішення існує

- Шифр-HSM
- Шифр-CaaS/ Agent Шифр-CaaS
- Шифр-vTMS
- Шифр-Signer
- Шифр-Crypto



САЙФЕР

Рішення існує: Спрощене



- Шифр-HSM
- Шифр-CaaS/ Agent Шифр-CaaS
- Шифр-vTMS
- Шифр-Signer
- Шифр-Crypto

Чи існують рішення в таких умовах?

Так! Існує! **Шифр-HSM**

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
- Ключі не вилучаються з HSM
- Можливість резервування та реплікація стану
- Інтеграція з великою кількістю систем:
  - Через бібліотеку PKCS#11
  - Через інтеграційний модуль Шифр-CaaS
  - Через інтеграційний модуль Шифр-Signer, Шифр-Crypto
- Висока надійність
- Горизонтальне масштабування (через vTMS)
- Балансування запитів між кількома HSM (через vTMS)

Опис

Апаратна реалізація

- Форм-фактор: Rack Mount 19”, 1U
- Наявність датчиків НСД
- Наявність датчиків проникнення і вскриття
- Шифрування фізичної пам'яті
- Безпечне завантаження (Secure Boot)
- Network (1/10 Gigabit Ethernet): RJ-45/SFP

Характеристики

- Багатопоточна реалізація (до 1000 одночасних підключень)
- Захищений довірений канал між бібліотекою PKCS#11 та самим мережним HSM (TLS v1.2-Шифр+ v2.5)
- Розподіл секрету між адміністраторами для запуску (на захищених носіях)
- Підтримка TPM 2.0 + MED
- SNMP

Підтримка клієнтських платформ

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

Комплектність:

Комплектність-Base	Ключів, тис. шт	Одночасних сесій	
Початковий	30	128	
Стандартний	60	256	
Продуктивний	90	512	

Комплектність-Internal	Ключів, тис. шт	Одночасних сесій	
Початковий	30	256	
Стандартний	60	512	
Продуктивний	90	1024	

Продуктивність ЕП (Базовий-Стандартний)

Операція	Довжина ключа, біт	Швидкість, ЕП/с
Формування (ДСТУ 4145-2002)	257	5000
Формування (ECDSA)	256	4000
Формування (RSA PKCS#1 v1.5)	2048	1000
Формування (RSA PKCS#1 v1.5)	4096	650
Формування спільного секрету (ДСТУ ISO/IEC 15946-3+ДСТУ 4145-2002)	431	4500
Формування спільного секрету (ДСТУ ISO/IEC 15946-3+ECDSA)	256	3500

Запитання?

ТОВ “Сайфер ПРО”

Влад Ковтун: vk@cipher.com.ua

www: https://cipher.com.ua