2014 CEE-SEC(R) РазработкаПО

Технология виртуализации аппаратных модулей безопасности в контейнерах Linux

Кирилл Кринкин,
Дмитрий Карташов

Академический Университет РАН, Санкт-Петербург
Лаборатория Parallels

Parallels

Мотивация

- Аппаратные HSM – зарекомендовавшие себя средства защиты, имеющие высокую стоимость;
- Контейнеры Linux – надежные и защищенные окружения
- Реализация функций HSM в контейнере – разумный компромисс защищенности и функциональности

Что такое HSM

Hardware Security Module – физическое устройство для управления цифровыми ключами и выполнения криптофункций:

- физическая (аппаратная) изоляция;
- отсутствие интерфейсов доступа к памяти
- средства защиты от проникновения

Контейнеры в Linux

Штатное средство виртуализации в ядре Linux:

- изоляция пространств имен
- ограничение ресурсов
- защита

«Доступные» решения

AWS CloudHSM Pricing

You will be charged a one-time upfront fee for each CloudHSM provisioned to you and an hourly fee f
HSM while it remains provisioned and available for your use.

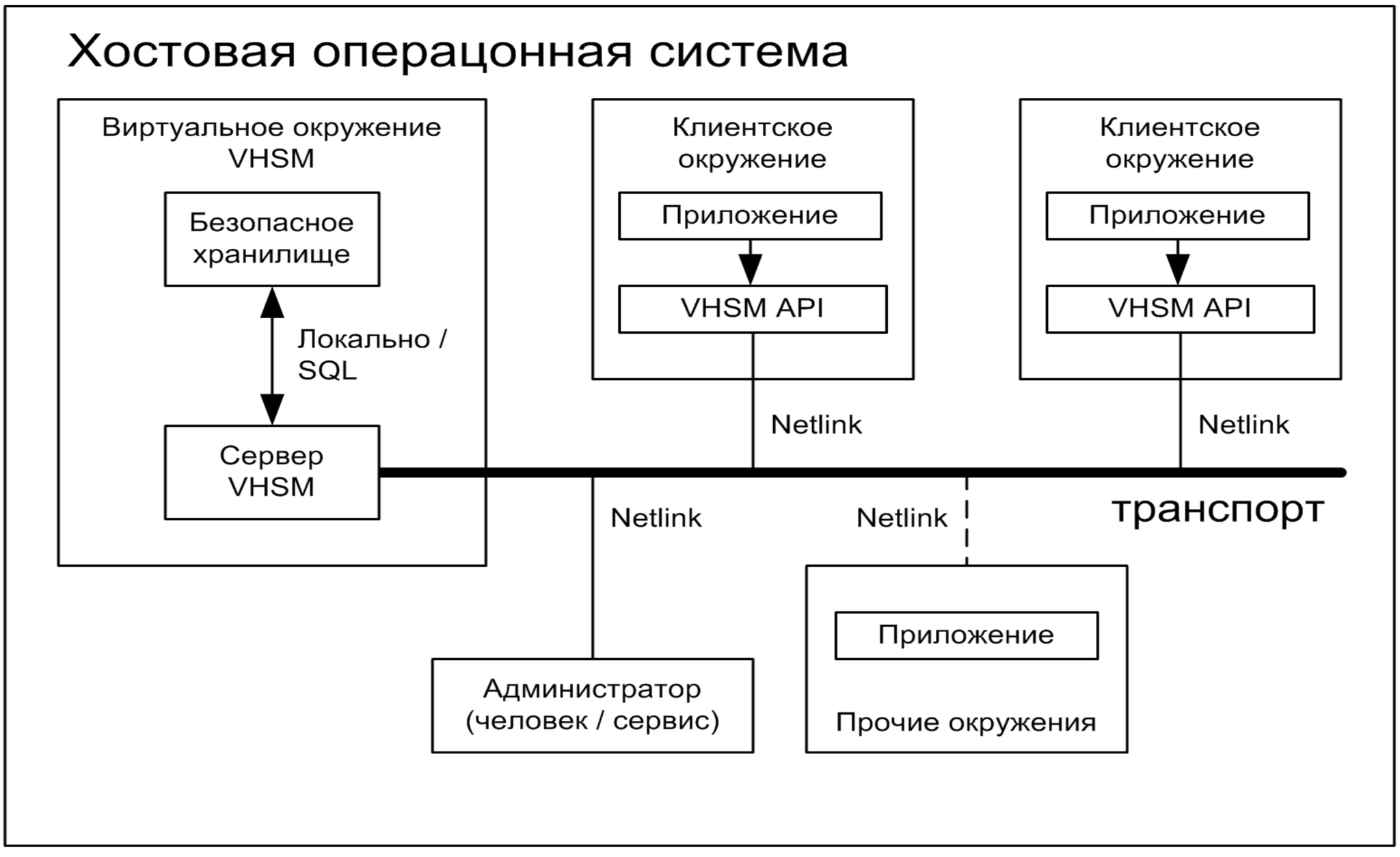
Region: US East (N. Virginia)

AWS CloudHSM Type	Upfront	Hourly
AWS CloudHSM service with Dedicated SafeNet Luna SA	$5,000	$1.88 per Hour
		$1,373 (on average per m

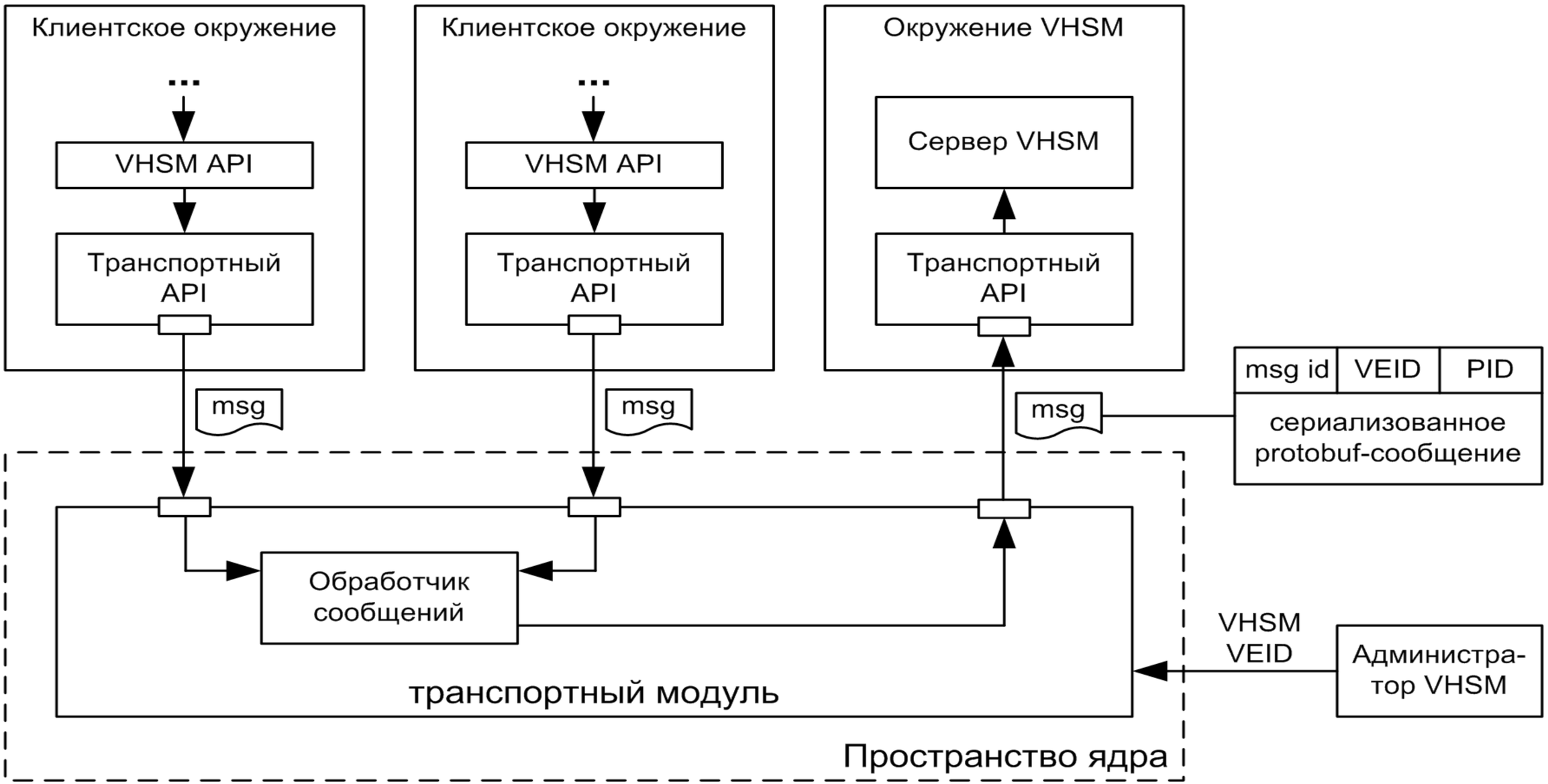
Except as otherwise noted, our prices are exclusive of applicable taxes and duties, including VAT and applicable sales t
customers with a Japanese billing address, use of the Asia Pacific (Tokyo) Region is subject to Japanese Consumption
more.

Наименование	Цена
Программно-аппаратный криптографический модуль "КриптоПро HSM". Вариант исполнения 1 Параметр устройства: • Процессор (64 разр.): **2 x Xeon E5630** ого): **16** а): **2U/72 см** : **3 шт. (оптика)** ество пользователей (ключевых контейнеров): **10000** ество одновременно работающих пользователей (сессий): **1500** водительность (ЭЦП/сек.): **15000** нный с горячей заменой po HSM"	900 000,00р.
тографический модуль "КриптоПро HSM". Вариант исполнения 2 **1 x Core2Duo** ого): **2** а): **2U/48 см** : **2 шт. (оптика)** ество пользователей (ключевых контейнеров): **1500** ество одновременно работающих пользователей (сессий): **1000** водительность (ЭЦП/сек.): **1500** ой po HSM"	600 000,00р.
тографический модуль "Атликс-HSM"	600 000,00р.
ческую поддержку ПАКМ "КриптоПро HSM"	60 000,00р.

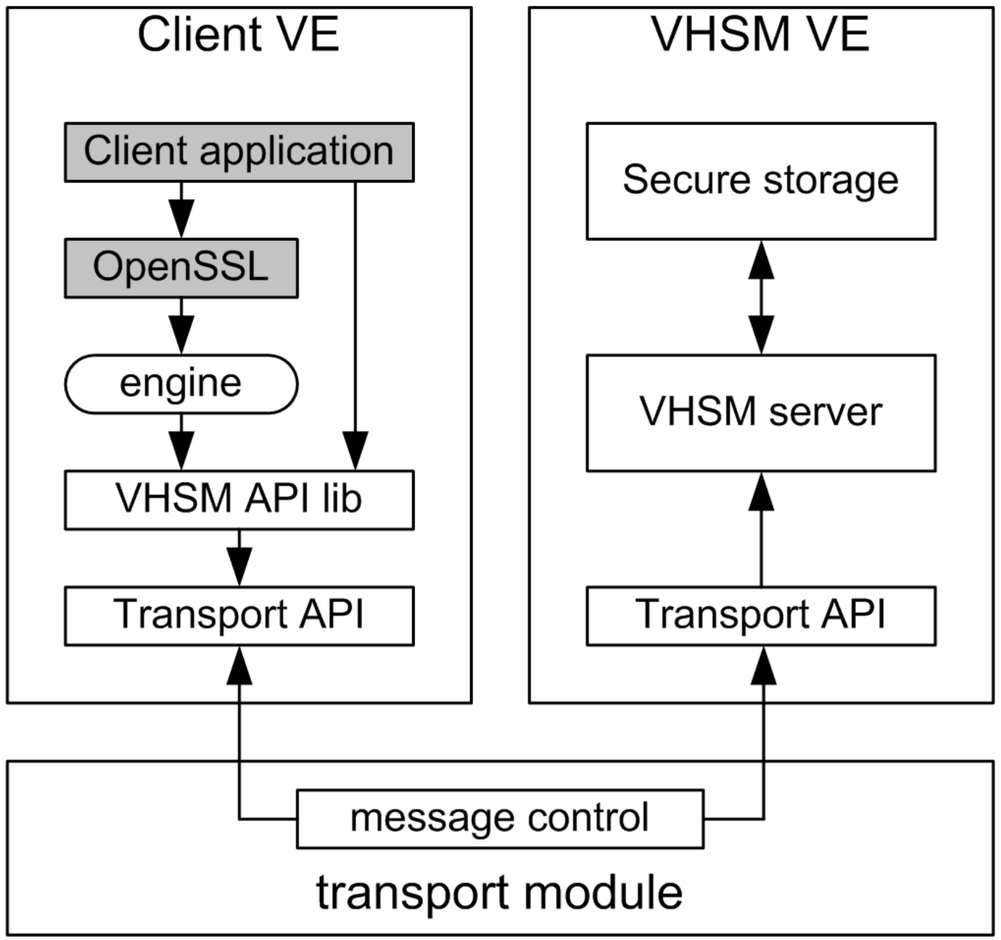
Архитектура Virtual-HSM



VHSM транспорт

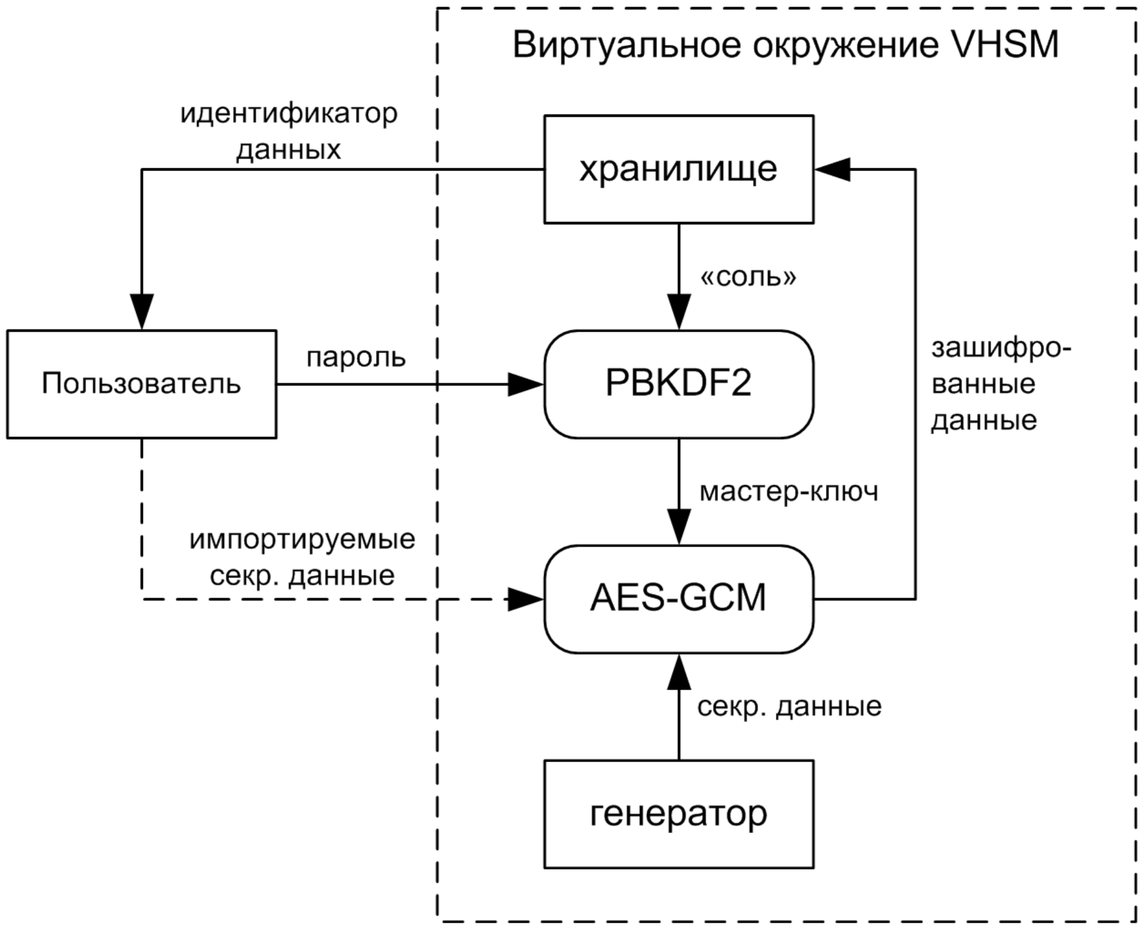


VHSM для пользователя



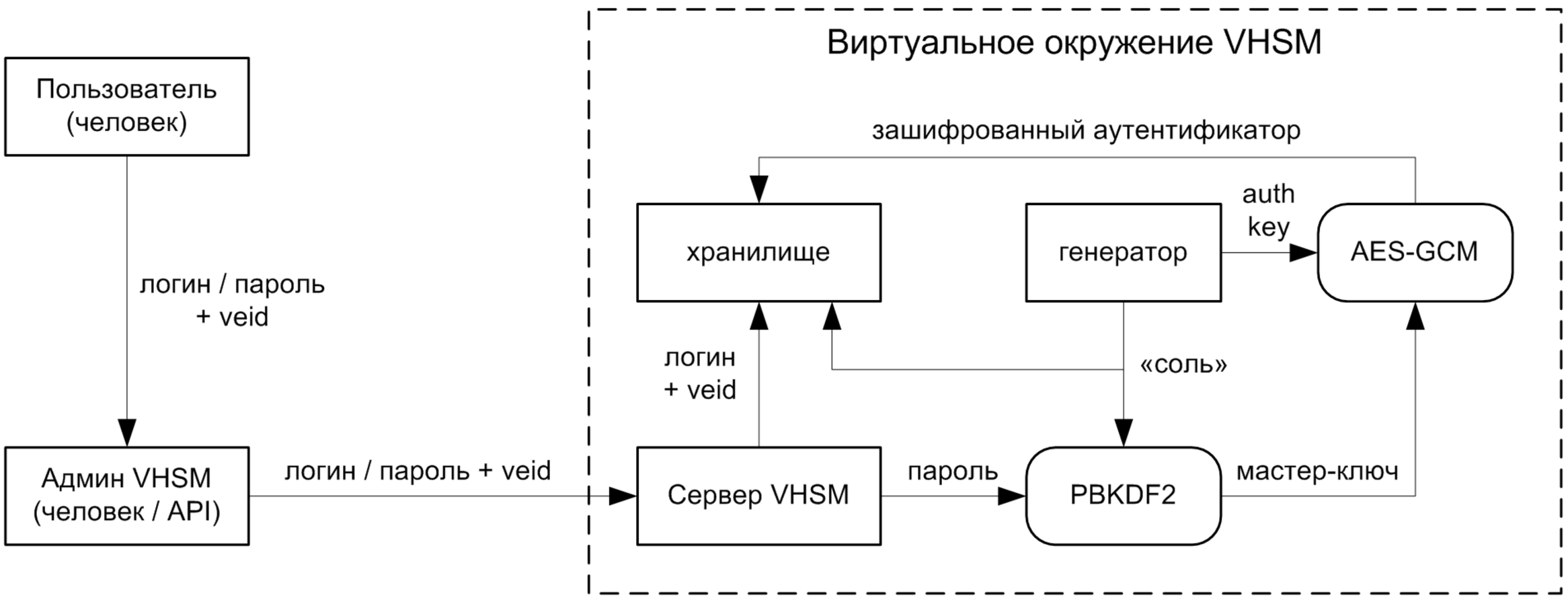
- интерфейс OpenSSL
- crypto-engine
- клиент vhsm в контейнере

Организация хранилища

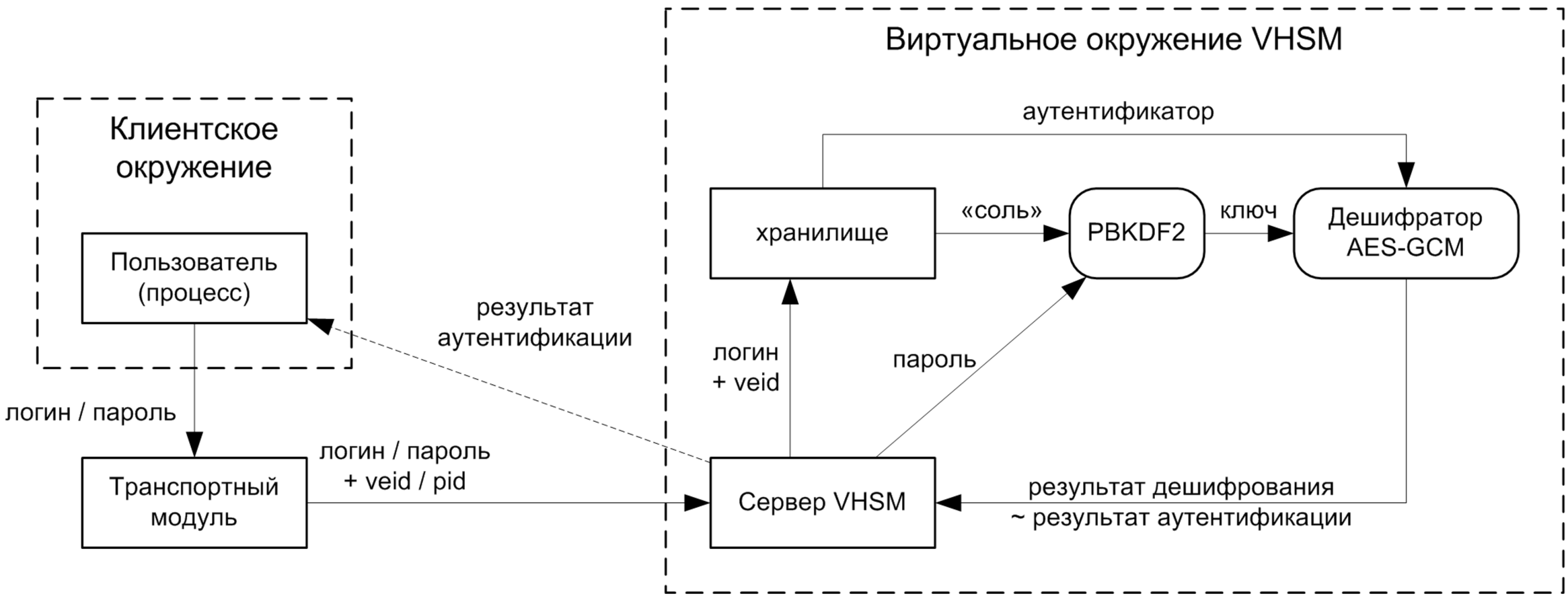


- SQL DB
- AES GCM
- только ID (pin)

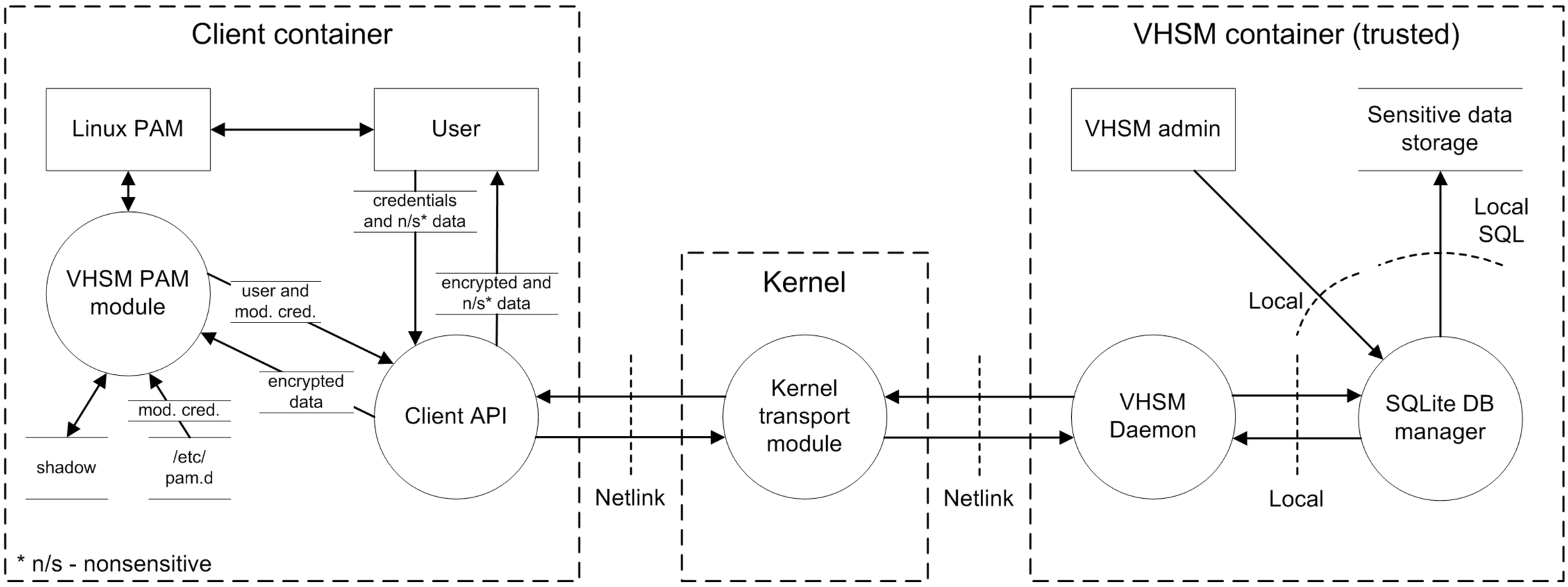
Администрирование



Аутентификация, авторизация



Анализ угроз



Производительность

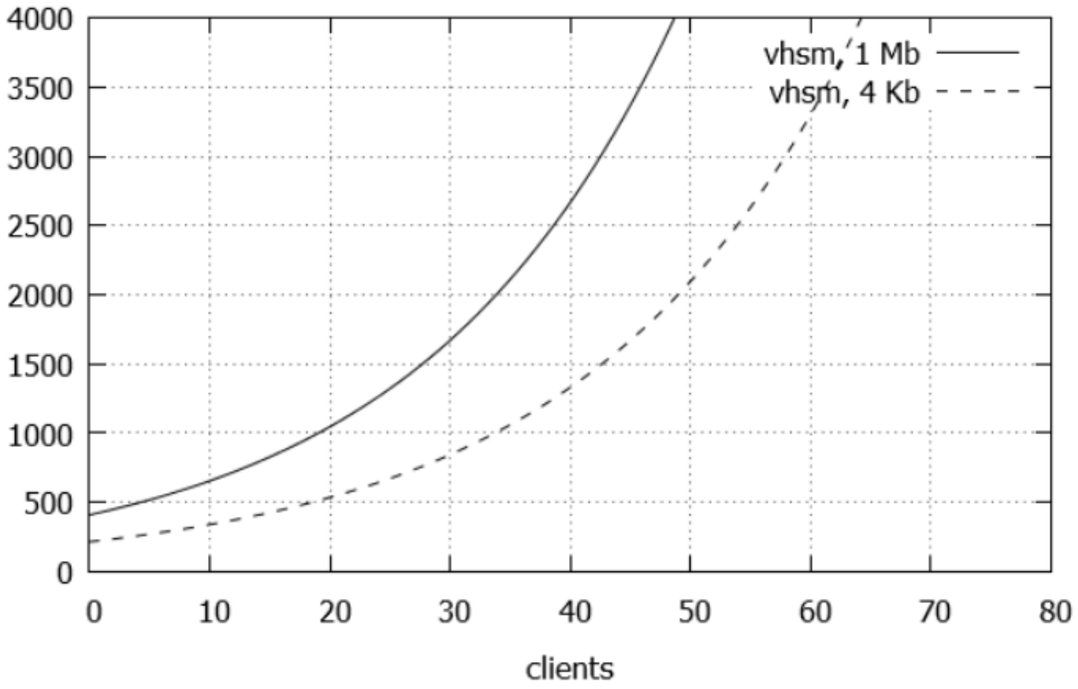


Рис. 1: HMAC-SHA1: VHSM, 4 Кб и 1 Мб

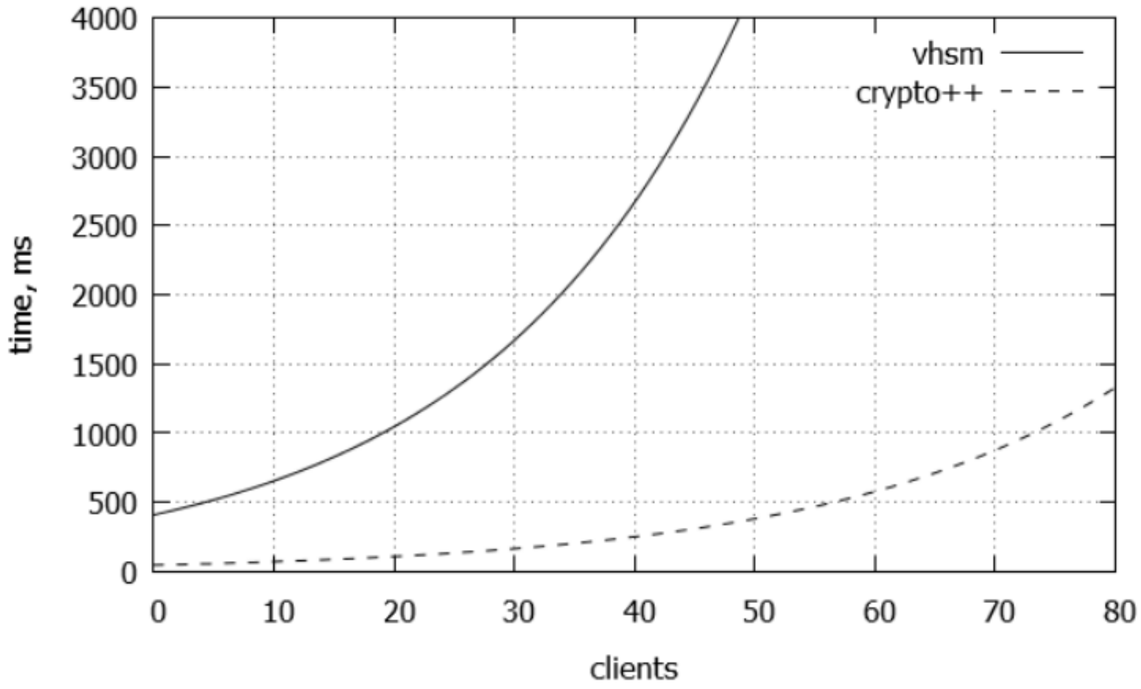


Рис. 2: HMAC-SHA1: VHSM и Crypto++, 1 Мб

Ссылки и ресурсы

- http://openvz.org/Virtual_HSM
- http://git.openvz.org/?p=vhsm

Спасибо

- Кирилл Кринкин *kirill.krinkin@gmail.com*
- Дмитрий Карташов *mapseamoff@mail.ru*