



# Технология виртуализации аппаратных модулей безопасности в контейнерах Linux

Кирилл Кринкин,  
Дмитрий Карташов

*Академический Университет РАН, Санкт-Петербург  
Лаборатория 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 for each CloudHSM while it remains provisioned and available for your use.

Region: US East (N. Virginia) ▾

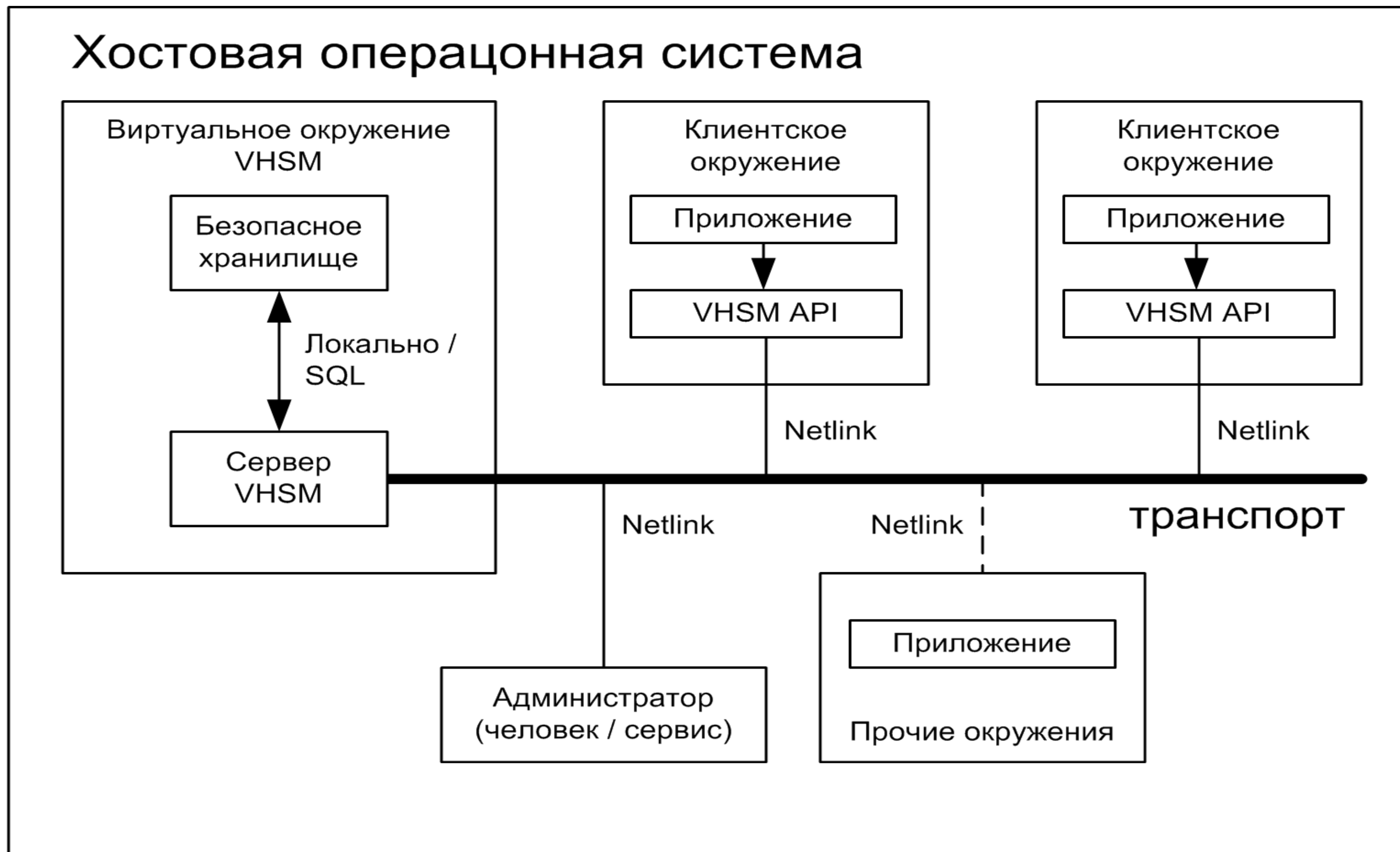
AWS CloudHSM Type	Upfront	Hourly	Цена
Программно-аппаратный криптографический модуль "КриптоПро HSM". Вариант исполнения 1			900 000,00р.
Программно-аппаратный криптографический модуль "КриптоПро HSM". Вариант исполнения 2			600 000,00р.
AWS CloudHSM service with Dedicated SafeNet Luna SA	\$5,000	\$1.88 per Hour	\$1,373 (on average per month)
Программно-аппаратный криптографический модуль "Атликс-HSM"			600 000,00р.
Техническую поддержку ПАКМ "КриптоПро HSM"			60 000,00р.

Наименование	Цена
Программно-аппаратный криптографический модуль "КриптоПро HSM". Вариант исполнения 1 Параметр устройства: • Процессор (64 разр.): 2 x Xeon E5630 • Память (ГБ): 16 • Высота (мм): 2U/72 см • Оптика: 3 шт. (оптика) • Количество пользователей (ключевых контейнеров): 10000 • Количество одновременно работающих пользователей (сессий): 1500 • Пропускная способность (ЭЦП/сек.): 15000 • Гарантийный срок: 3 года • Сервис: 24/7 • Доставка: по HSM"	900 000,00р.
Программно-аппаратный криптографический модуль "КриптоПро HSM". Вариант исполнения 2 Параметр устройства: • Процессор (64 разр.): 1 x Core2Duo • Память (ГБ): 2 • Высота (мм): 2U/48 см • Оптика: 2 шт. (оптика) • Количество пользователей (ключевых контейнеров): 1500 • Количество одновременно работающих пользователей (сессий): 1000 • Пропускная способность (ЭЦП/сек.): 1500 • Гарантийный срок: 3 года • Сервис: 24/7 • Доставка: по HSM"	600 000,00р.
Программно-аппаратный криптографический модуль "Атликс-HSM"	600 000,00р.
Техническую поддержку ПАКМ "КриптоПро HSM"	60 000,00р.

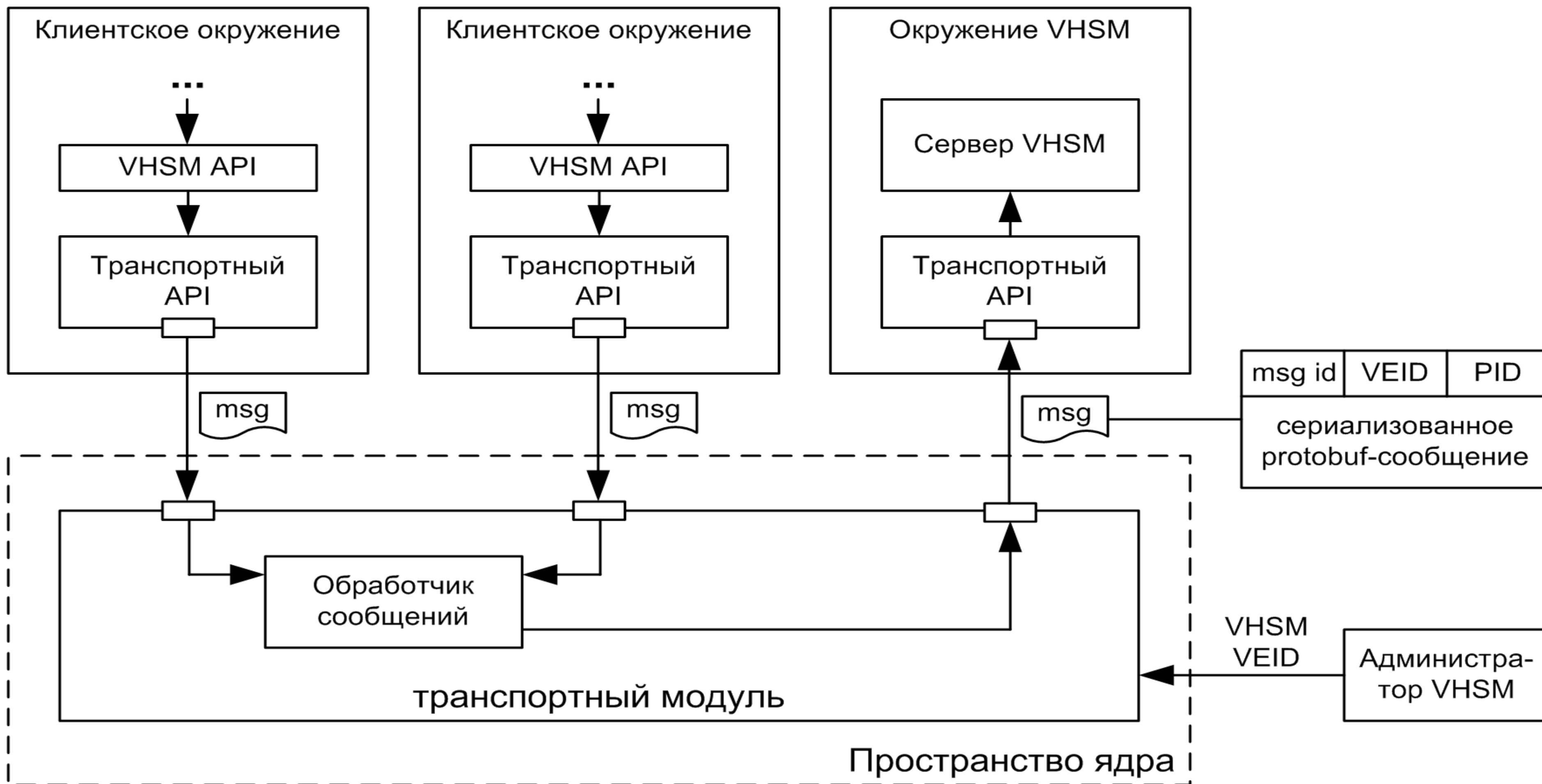
Create Free Account

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

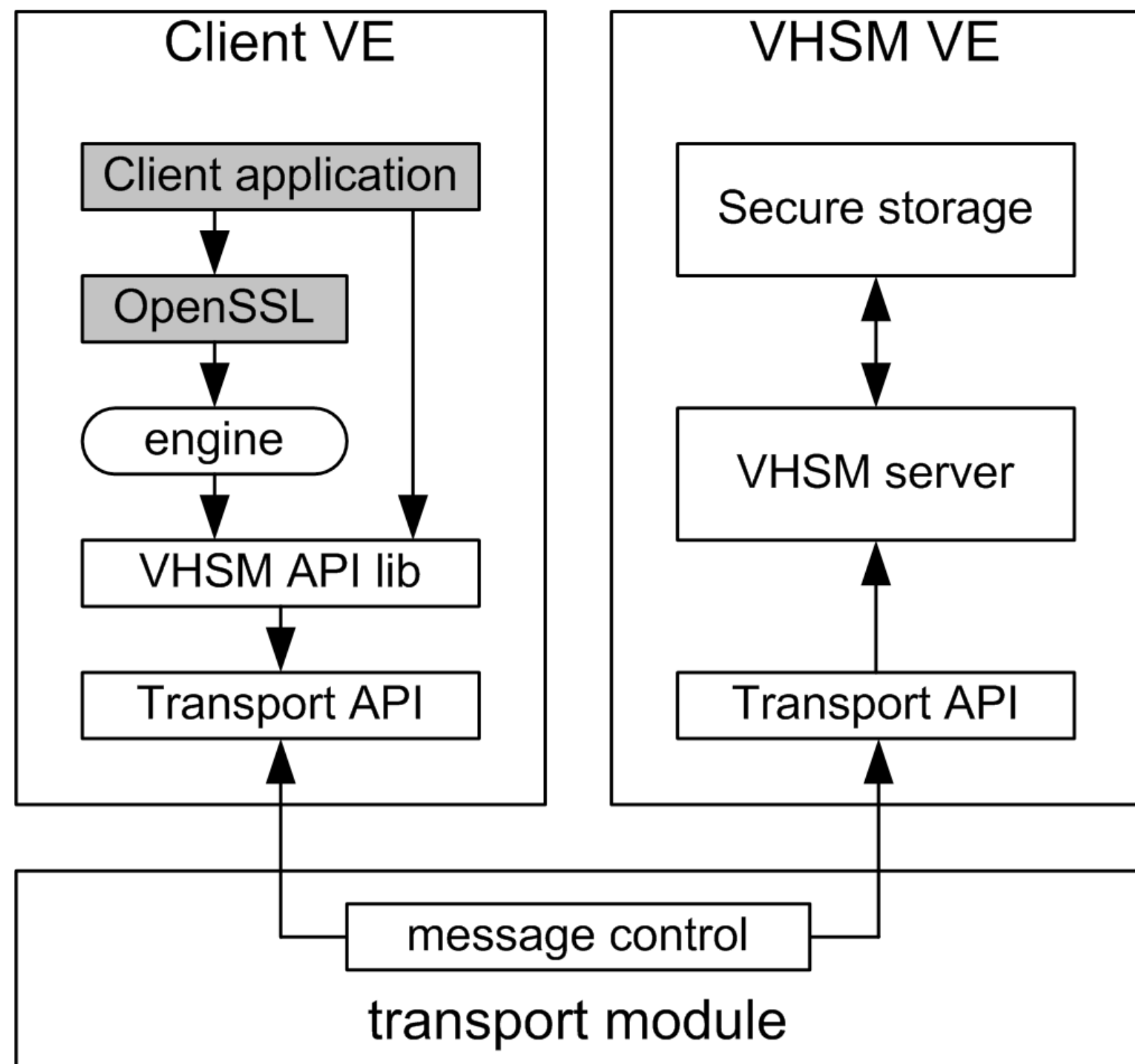
# Архитектура Virtual-HSM



# VHSM транспорт



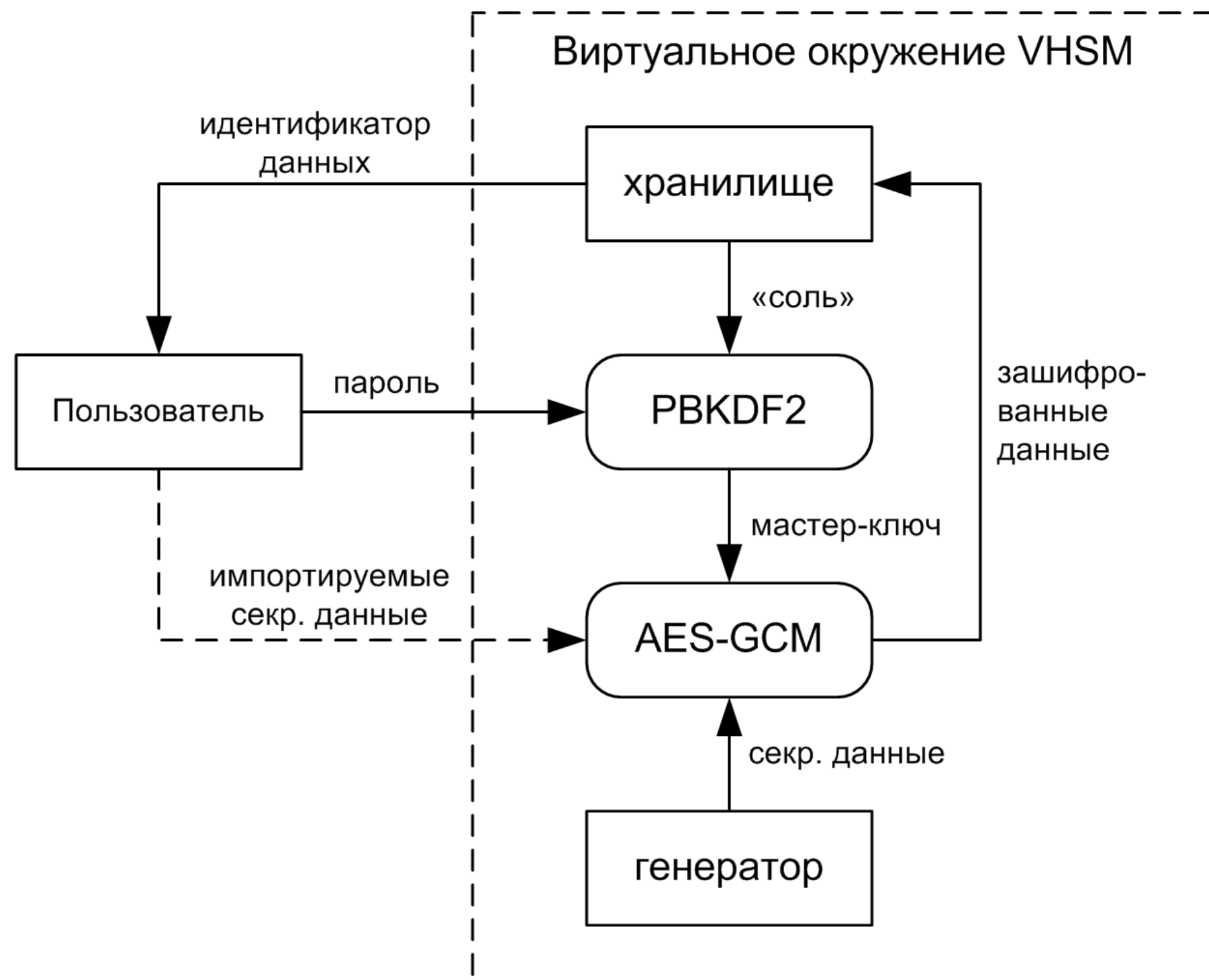
# VHSM для пользователя



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

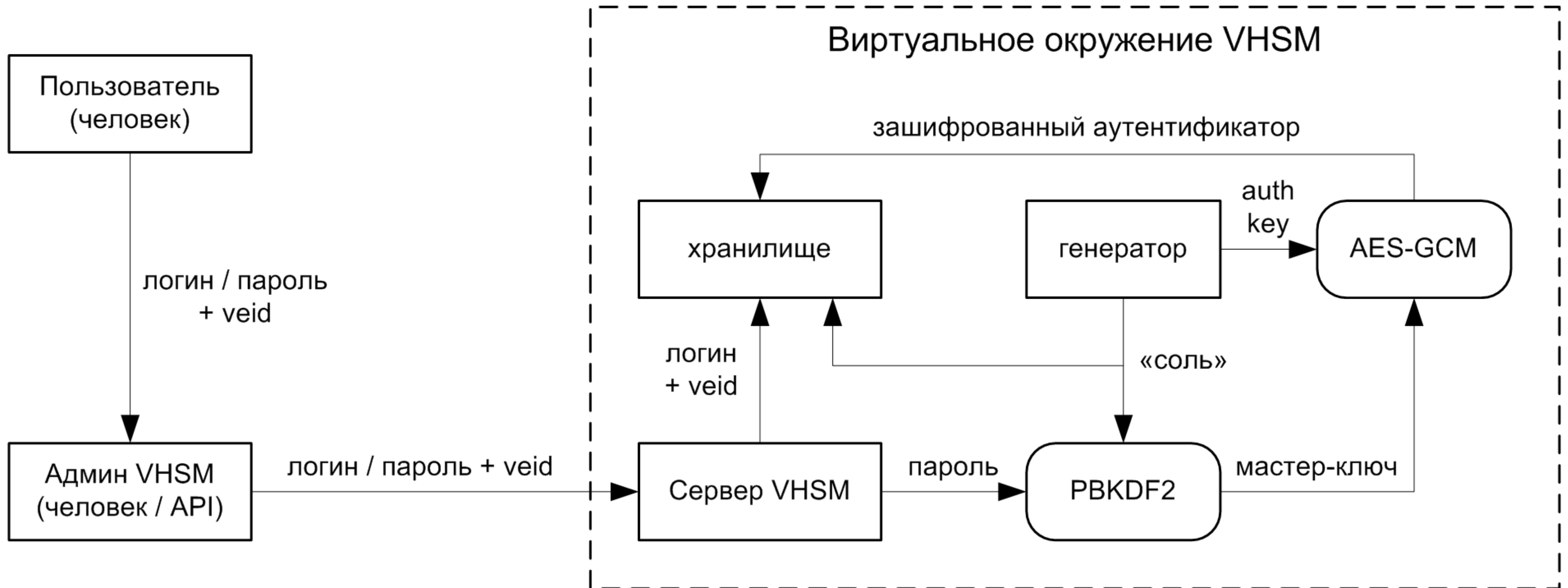


# Организация хранилища

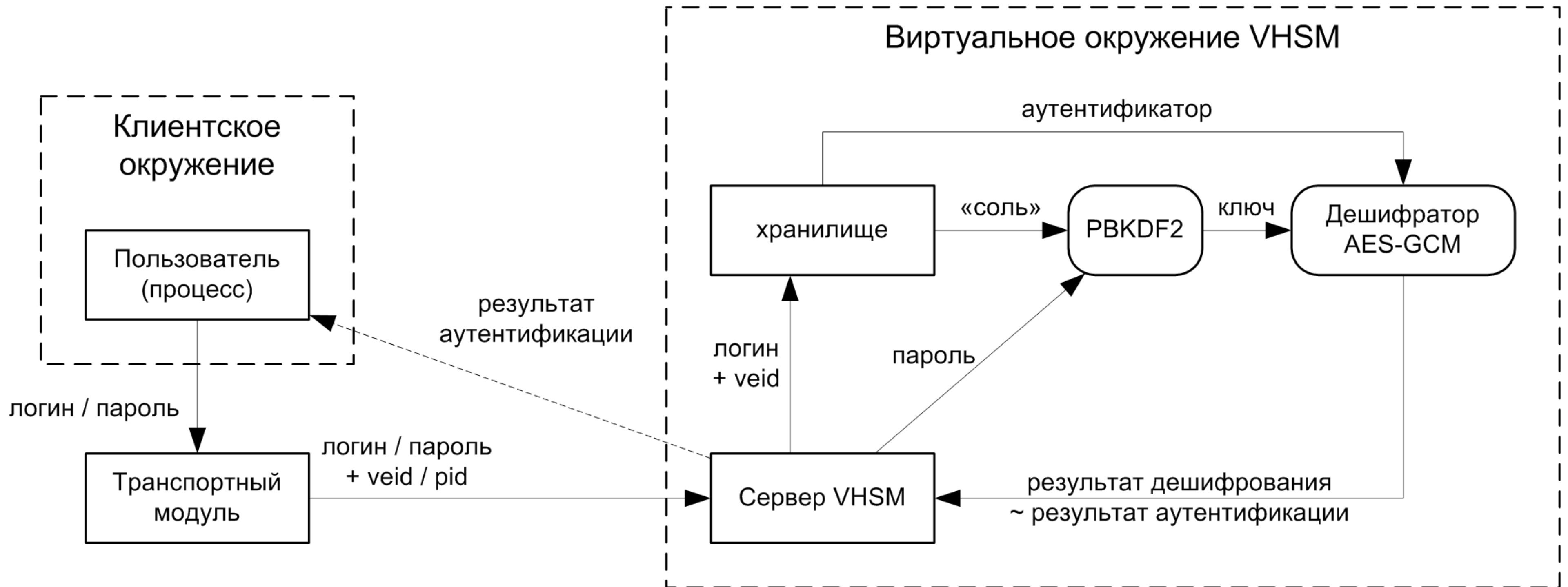


- SQL DB
- AES GCM
- ТОЛЬКО ID (pin)

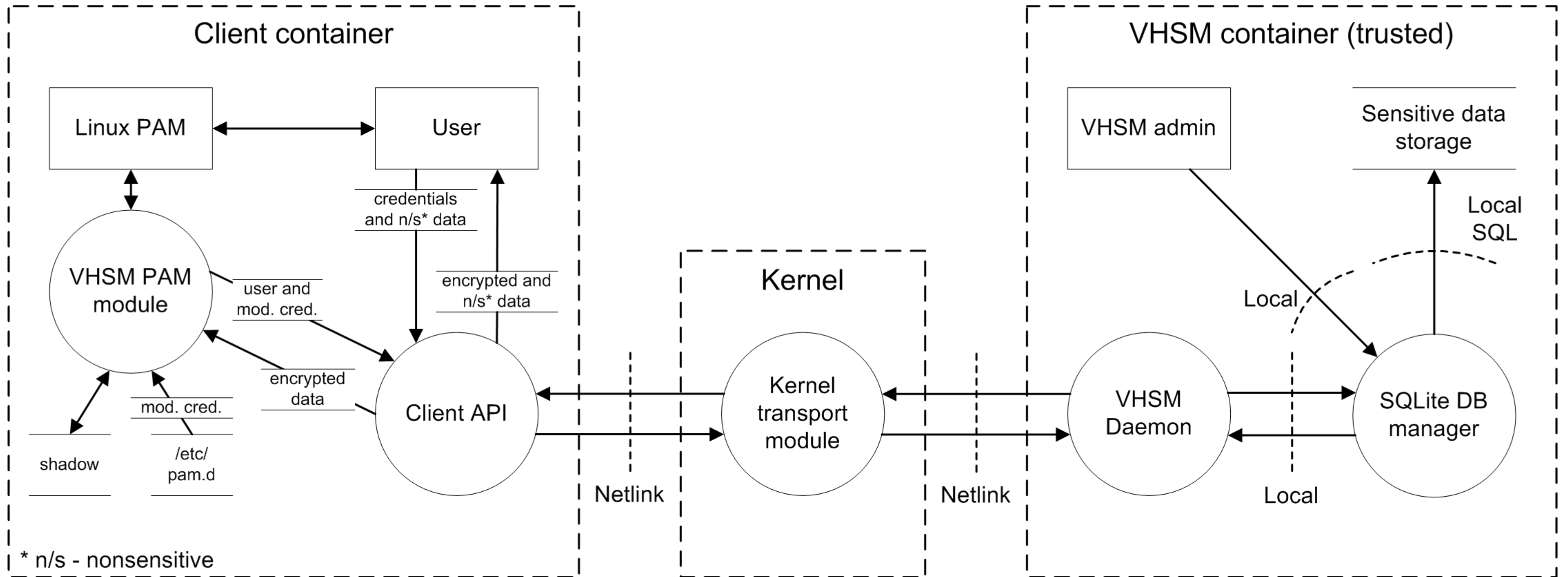
# Администрирование



# Аутентификация, авторизация



# Анализ угроз



# Производительность

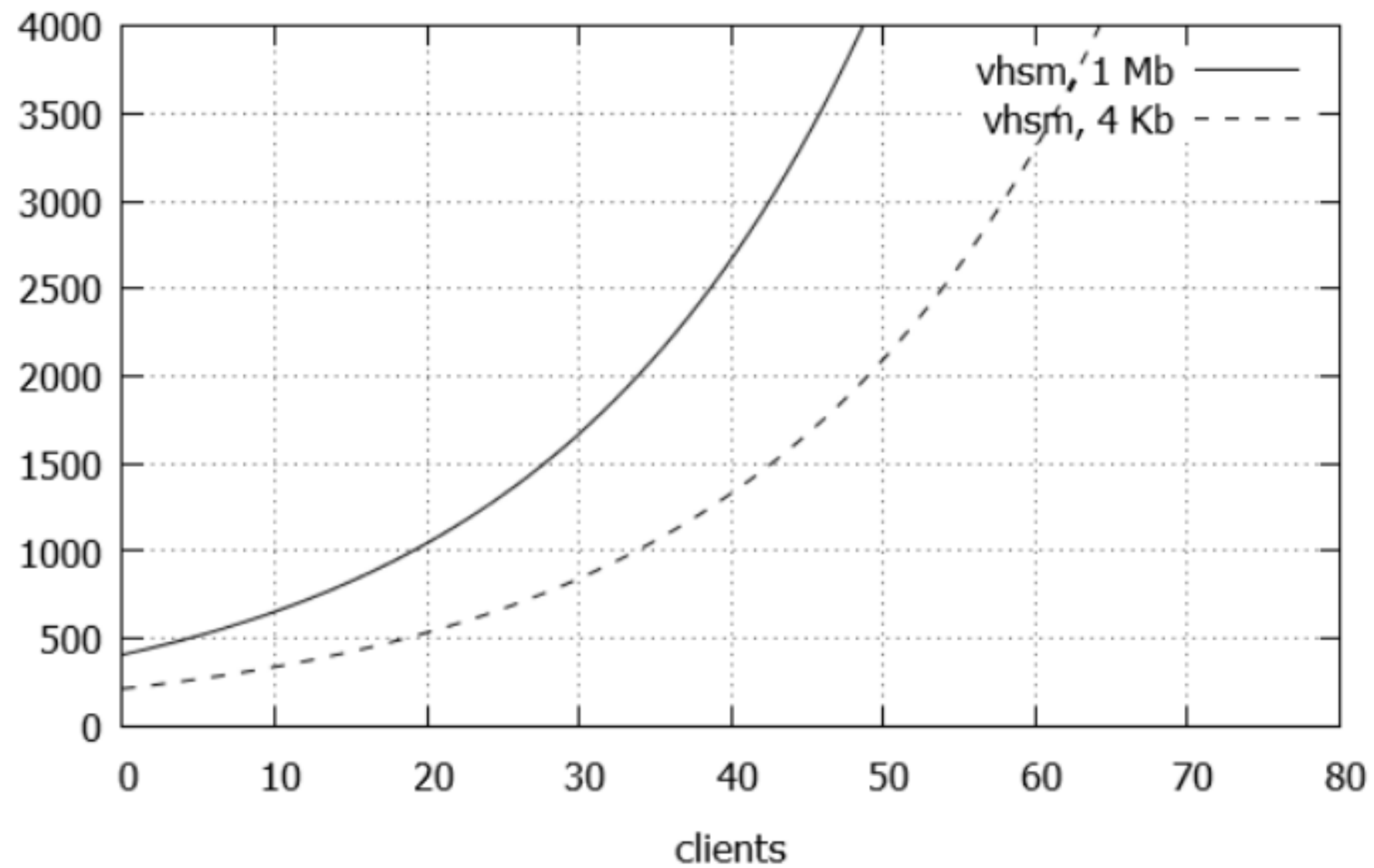


Рис. 1: HMAC-SHA1: VHSM, 4 Кб и 1 Мб

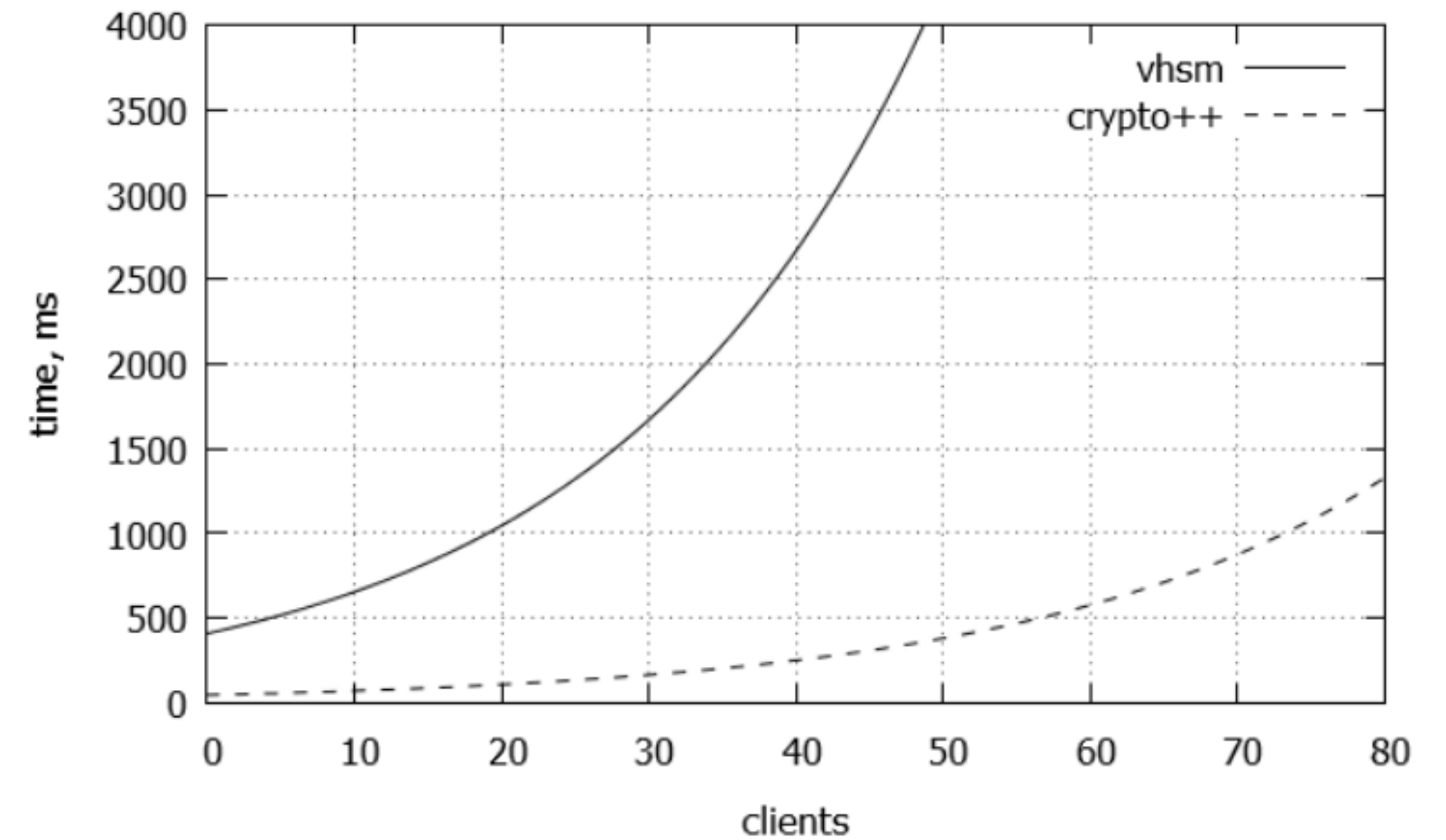
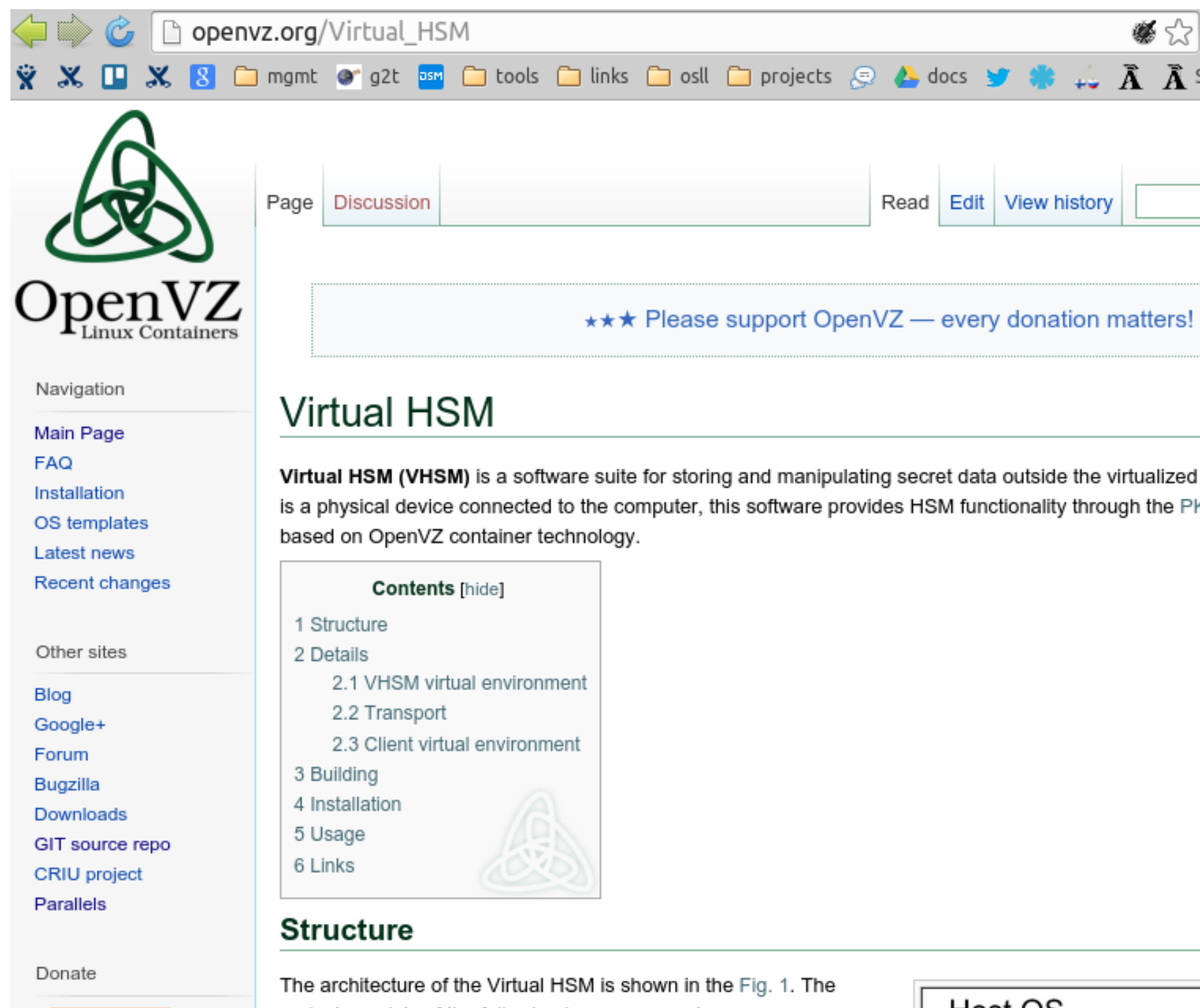


Рис. 2: HMAC-SHA1: VHSM и Crypto++, 1 Мб

# Ссылки и ресурсы



The screenshot shows a web browser window with the URL `openvz.org/Virtual_HSM`. The page features the OpenVZ logo and navigation menu on the left. The main content area includes a "Discussion" tab, a donation notice, and a section titled "Virtual HSM". The text describes Virtual HSM (VHSM) as a software suite for storing and manipulating secret data outside the virtualized environment. A table of contents is provided, listing sections from Structure to Links. The "Structure" section is currently expanded, showing a diagram of the architecture.

Page **Discussion**

\*\*\* Please support OpenVZ — every donation matters! \*\*\*

## Virtual HSM

**Virtual HSM (VHSM)** is a software suite for storing and manipulating secret data outside the virtualized environment. If a physical device connected to the computer, this software provides HSM functionality through the PKI based on OpenVZ container technology.

**Contents** [hide]

- 1 Structure
- 2 Details
  - 2.1 VHSM virtual environment
  - 2.2 Transport
  - 2.3 Client virtual environment
- 3 Building
- 4 Installation
- 5 Usage
- 6 Links

### Structure

The architecture of the Virtual HSM is shown in the Fig. 1. The diagram consists of the following components:

- Host OS

- [http://openvz.org/Virtual\\_HSM](http://openvz.org/Virtual_HSM)
- <http://git.openvz.org/?p=vhsm>

# Спасибо

- Кирилл Кринкин [\*kirill.krinkin@gmail.com\*](mailto:kirill.krinkin@gmail.com)
- Дмитрий Карташов [\*mapseamoff@mail.ru\*](mailto:mapseamoff@mail.ru)