РОССИЙСКАЯ ФЕДЕРАЦИЯ

(19) **RU** (11) **2016 143 088**(13) **A**

(51) МПК
H04L 9/08 (2006.01)

ФЕДЕРАЛЬНАЯ СЛУЖБА
ПО ИНТЕЛЛЕКТУАЛЬНОЙ СОБСТВЕННОСТИ

(12) ЗАЯВКА НА ИЗОБРЕТЕНИЕ

(21)(22) Заявка: **2016143088, 04.05.2015**

Приоритет(ы):
(30) Конвенционный приоритет:
05.05.2014 US 61/988,786;
09.09.2014 US 14/481,399

(43) Дата публикации заявки: **03.05.2018** Бюл. № 13

(85) Дата начала рассмотрения заявки PCT на национальной фазе: **02.11.2016**

(86) Заявка PCT:
US 2015/028991 (04.05.2015)

(87) Публикация заявки PCT:
WO 2015/171476 (12.11.2015)

Адрес для переписки:
129090, Москва, ул. Б.Спасская, 25, строение 3, ООО "Юридическая фирма Городисский и Партнеры"

(71) Заявитель(и):
МАЙКРОСОФТ ТЕКНОЛОДЖИ ЛАЙСЕНСИНГ, ЭлЭлСи (US)

(72) Автор(ы):
НОВАК Марк Фишел (US),
БЕН-ЗВИ Нир (US),
ФЕРГЮСОН Нильс Т. (US)

(54) БЕЗОПАСНЫЙ ТРАНСПОРТ ЗАШИФРОВАННЫХ ВИРТУАЛЬНЫХ МАШИН С НЕПРЕРЫВНЫМ ДОСТУПОМ ВЛАДЕЛЬЦА

(57) Формула изобретения

1. Способ управления зашифрованными наборами данных в компьютерном окружении, содержащий этапы, на которых:

получают первый ключ дешифрирования, причем первый ключ дешифрирования сконфигурирован для использования для дешифрирования зашифрованного набора данных, который был зашифрован с использованием первого механизма шифрования, при этом первый механизм шифрования ассоциирован с первым ключом дешифрирования, который может быть использован для дешифрирования этого набора данных;

шифруют первый ключ дешифрирования посредством второго механизма шифрования, причем второй механизм шифрования ассоциирован со вторым ключом дешифрирования, используемым первым субъектом, так что второй ключ дешифрирования может быть использован первым субъектом для дешифрирования упомянутого набора данных путем дешифрирования сначала первого ключа с использованием второго ключа дешифрирования и затем с использованием дешифрированного первого ключа для дешифрирования этого набора данных;

шифруют первый ключ дешифрирования посредством третьего механизма шифрования, причем третий механизм шифрования ассоциирован с третьим ключом

RU 2016143088 A
RU 2016143088 A

дешифрирования, используемым вторым субъектом, так что третий ключ дешифрирования может быть использован вторым субъектом для дешифрирования упомянутого набора данных путем дешифрирования сначала первого ключа с использованием третьего ключа дешифрирования и затем с использованием первого дешифрированного ключа для дешифрирования этого набора данных;

создают пакет, содержащий, по меньшей мере, первый ключ дешифрирования, зашифрованный посредством второго механизма шифрования, и первый ключ дешифрирования, зашифрованный посредством третьего механизма шифрования;

подписывают пакет защитной подписью; и

подписывают пакет подписью, созданной из первого ключа дешифрирования;

при этом упомянутый набор данных содержит части виртуальной машины;

при этом первый субъект является провайдером услуг размещения данной виртуальной машины и второй субъект является арендатором этого провайдера;

при этом выстраивается иерархия ключей, где корнем этой иерархии является первый ключ дешифрирования, и части виртуальной машины шифруются с использованием ключей из этой иерархии.

2. Способ по п.1, в котором первый ключ является мастер-ключом для vTPM для виртуальной машины.

3. Способ по п. 1, в котором набор данных содержит информацию подготовки для VM.

4. Способ по п. 1, в котором упомянутый набор данных содержит состояние vTPM.

5. Способ по п. 1, в котором упомянутый пакет содержит множество копий первого ключа дешифрирования, зашифрованных разными механизмами шифрования для множества разных хранителей.

6. Система для управления зашифрованными наборами данных в компьютерном окружении, содержащая

один или более процессоров; и

один или более машиночитаемых носителей информации, каковые один или более машиночитаемых носителей содержат машиноисполняемые инструкции, которые при их исполнении по меньшей мере одним из упомянутых одного или более процессоров предписывают системе выполнять этапы по п. 1.

7. Один или более физических машиночитаемых носителей информации, содержащих машиноисполняемые инструкции, которые при их исполнении по меньшей мере одним из одного или более процессоров предписывают системе выполнять этапы по п. 1.

RU 2016143088 A

RU 2016143088 A