



ФЕДЕРАЛЬНАЯ СЛУЖБА
ПО ИНТЕЛЛЕКТУАЛЬНОЙ СОБСТВЕННОСТИ

(12) **ЗАЯВКА НА ИЗОБРЕТЕНИЕ**

(21)(22) Заявка: 2017105800, 25.08.2015

Приоритет(ы):

(30) Конвенционный приоритет:
25.09.2014 US 14/495,959

(43) Дата публикации заявки: 22.08.2018 Бюл. № 24

(85) Дата начала рассмотрения заявки РСТ на
национальной фазе: 22.02.2017(86) Заявка РСТ:
US 2015/046815 (25.08.2015)(87) Публикация заявки РСТ:
WO 2016/048535 (31.03.2016)Адрес для переписки:
109012, Москва, ул. Ильинка, 5/2, ООО
"Союзпатент"

(71) Заявитель(и):

МАКАФИ, ИНК. (US)

(72) Автор(ы):

**НАЙШТУТ Алекс (IL),
СМИТ Нед (US),
ШАРАГА Авишай (IL),
ПОГОРЕЛИК Олег (IL),
БХАРГАВ-СПАНТЗЕЛ Абхилаша (US),
РАЗИЕЛ Майкл (IL),
ПРИЕВ Ави (IL),
ШАЛИВ Ади (IL),
МУТТИК Игорь (GB)**(54) **АРХИТЕКТУРА ИДЕНТИЧНОСТИ ПЛАТФОРМЫ С ВРЕМЕННОЙ ИДЕНТИЧНОСТЬЮ
ПОД ПСЕВДОНИМОМ**

(57) Формула изобретения

1. Устройство клиент идентичности платформы, содержащее:
сетевой интерфейс; и
один или более логических элементов аппаратных и/или программных средств,
содержащих механизм клиента идентичности платформы (PIC), выполненный с
возможностью функционирования для:
обнаружения доступной услуги по указанному сетевому интерфейсу;
генерирования временной идентичности на основе псевдонима (TPI); и
передачи TPI на доступную услугу по указанному сетевому интерфейсу.
2. Устройство по п. 1, в котором механизм PIC дополнительно содержит доверенную
исполнительную среду (TEE), при этом механизм PIC дополнительно выполнен с
возможностью функционирования для защищенного подписания TPI в TEE.
3. Устройство по п. 2, в котором этап генерирования TPI содержит подэтап, на
котором смешивают случайное или псевдослучайное начальное значение с основным
названием и истечением срока действия.
4. Устройство по п. 2, в котором TEE содержит защищенную область памяти или
защищенные аппаратные средства.
5. Устройство по п. 1, в котором механизм PIC дополнительно выполнен с
возможностью функционирования для установки истечения срока действия для TPI.
6. Устройство по п. 5, в котором механизм PIC дополнительно выполнен с

возможностью функционирования для уничтожения ТРІ после истечения срока действия.

7. Устройство по п. 6, в котором механизм РІС дополнительно выполнен с возможностью функционирования для генерирования второго ТРІ после уничтожения ТРІ.

8. Устройство по п. 1, в котором этап обнаружения доступной услуги содержит подэтап, на котором осуществляют идентификацию онлайн услуги.

9. Устройство по п. 1, в котором этап обнаружения доступной услуги содержит подэтап, на котором осуществляют идентификацию доступного беспроводного сетевого соединения для физического места предоставления услуги.

10. Устройство по п. 1, в котором этап обнаружения доступной услуги содержит подэтап, на котором осуществляют соединение, с возможностью связи, с провайдером общественной услуги.

11. Устройство по п. 1, в котором механизм РІС дополнительно выполнен с возможностью функционирования для предоставления не идентифицирующих персонально демографических данных в ТРІ.

12. Устройство по п. 1, в котором механизм РІС дополнительно выполнен с возможностью функционирования для предоставления данных телеметрии для доступной услуги.

13. Устройство по п. 1, в котором механизм РІС дополнительно выполнен с возможностью функционирования для:

обнаружения второй доступной услуги по сетевому интерфейсу, причем вторая доступная услуга отличается от первой доступной услуги;

генерирования второй ТРІ, причем второй ТРІ отличается от первого ТРІ; и передачи второй ТРІ на вторую доступную услугу по указанному сетевому интерфейсу.

14. Один или более считываемых компьютером носителей информации, хранящий инструкции, вызывающие выполнение процессором предоставления механизма клиента идентичности платформы (РІС), функционирования для:

обнаружения доступной сетевой услуги;

генерирования временной идентичности на основе псевдонима (ТРІ); и передачи ТРІ на доступную сетевую услугу.

15. Один или более считываемых компьютером носителей информации по п. 14, в котором механизм РІС дополнительно содержит доверенную исполнительную среду (ТЕЕ), при этом механизм РІС дополнительно выполнен с возможностью функционирования для безопасной подписи ТРІ в ТЕЕ.

16. Один или более считываемых компьютером носителей информации по п. 15, в котором этап генерирования ТРІ содержит подэтап, на котором: смешивают случайное или псевдослучайное значение с основным наименованием и временем истечения срока действия.

17. Один или более считываемых компьютером носителей информации по п. 14, в котором механизм РІС дополнительно выполнен с возможностью установки времени истечения срока действия для ТРІ.

18. Один или более считываемых компьютером носителей информации по п. 14, в котором этап обнаружения доступной услуги содержит подэтап, на котором идентифицируют онлайн услугу.

19. Один или более считываемых компьютером носителей информации по п. 14, в котором этап обнаружения доступной услуги содержит подэтап, на котором: идентифицируют доступное беспроводное сетевое соединение для физического места предоставления услуги.

20. Один или более считываемых компьютером носителей информации по п. 14, в

котором этап обнаружения доступной услуги содержит подэтап, на котором осуществляют соединение, с возможностью связи, с публичным провайдером услуги.

21. Один или более считываемых компьютером носителей информации по п. 14, в котором механизм РИС дополнительно выполнен с возможностью функционирования для предоставления не идентифицирующих персонально демографических данных в ТРІ.

22. Один или более считываемых компьютером носителей информации по п. 14, в котором механизм РИС дополнительно выполнен с возможностью функционирования для предоставления данных телеметрии для доступной услуги.

23. Один или более считываемых компьютером носителей информации по п. 14, в котором механизм РИС дополнительно выполнен с возможностью функционирования для:

обнаружения второй доступной услуги по сетевому интерфейсу, причем вторая доступная услуга отличается от первой доступной услуги;

генерирования второго ТРІ, причем второй ТРІ отличается от первого ТРІ; и передачи второго ТРІ на вторую доступную услугу по сетевому интерфейсу.

24. Сервер идентичности платформы, содержащий:

сетевой интерфейс; и

один или более логических элементов, содержащих механизм сервера идентичности платформы, выполненный с возможностью функционирования для:

приема запроса на установку соединения от клиента идентичности платформы (РИС) через сетевой интерфейс;

согласования политики услуги с РИС;

получения временной идентичности на основе псевдонима (ТРІ) из РИС;

запроса данных телеметрии из РИС;

приема данных телеметрии из РИС; и

предоставления целевого содержания в РИС, при этом целевое содержание основано на телеметрии.

25. Сервер идентичности платформы по п. 24, в котором РИС дополнительно выполнено с возможностью функционирования для:

предоставления ТРІ в сервер аттестации; и

приема проверки аттестации от сервера аттестации.