РОССИЙСКАЯ ФЕДЕРАЦИЯ

(19) **RU** (11) **2013 101 768** (13) **A**

(51) МПК
H04W 12/04 (2009.01)

ФЕДЕРАЛЬНАЯ СЛУЖБА
ПО ИНТЕЛЛЕКТУАЛЬНОЙ СОБСТВЕННОСТИ

(12) ЗАЯВКА НА ИЗОБРЕТЕНИЕ

(21)(22) Заявка: **2013101768/08, 16.06.2011**

Приоритет(ы):
(30) Конвенционный приоритет:
16.06.2010 US 61/355,423;
15.06.2011 US 13/161,336

(43) Дата публикации заявки: **27.07.2014** Бюл. № **21**

(85) Дата начала рассмотрения заявки PCT на национальной фазе: **16.01.2013**

(86) Заявка PCT:
US 2011/040777 (16.06.2011)

(87) Публикация заявки PCT:
WO 2011/159952 (22.12.2011)

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

(71) Заявитель(и):
КВЭЛКОММ ИНКОРПОРЕЙТЕД (US)

(72) Автор(ы):
ЭСКОТТ Эдриан Эдвард (US),
ПАЛАНИГОУНДЕР Ананд (US)

(54) СПОСОБ И УСТРОЙСТВО ДЛЯ СВЯЗЫВАНИЯ АУТЕНТИФИКАЦИИ АБОНЕНТА И АУТЕНТИФИКАЦИИ УСТРОЙСТВА В СИСТЕМАХ СВЯЗИ

(57) Формула изобретения

1. Способ, действующий в устройстве, содержащий:

выполнение аутентификации абонента с сетевым объектом;

выполнение аутентификации устройства с сетевым объектом для упомянутого устройства;

генерацию защитного ключа, связывающего аутентификацию абонента и аутентификацию устройства; и

использование защитного ключа, чтобы обезопасить связь между устройством и обслуживающей сетью.

2. Способ по п. 1, в котором аутентификация абонента основана на обмене данными соглашения о ключе аутентификации между устройством и сетевым объектом.

3. Способ по п. 1, в котором аутентификация устройства основана на обмене данными по схеме «запрос-ответ» между устройством и сетевым объектом.

4. Способ по п. 1, в котором аутентификация абонента выполняется первым сервером аутентификации, который является частью сетевого объекта, и аутентификация устройства выполняется вторым сервером аутентификации, который является частью сетевого объекта.

5. Способ по п. 1, в котором аутентификация устройства выполняется посредством:

приема данных от сетевого объекта, которые зашифрованы с помощью открытого

RU 2013101768 A

RU 2013101768 A

ключа устройства;

использования соответствующего секретного ключа, чтобы расшифровать зашифрованные данные; и

последующего доказательства сетевому объекту того, что упомянутое устройство обладает сведениями о данных.

6. Способ по п. 1, дополнительно содержащий:

отправку запроса о присоединении от устройства к сетевому объекту, при этом запрос о присоединении включает в себя индикацию возможностей аутентификации устройства у упомянутого устройства.

7. Способ по п. 1, в котором аутентификация устройства защищена по меньшей мере одним ключом, сгенерированным во время аутентификации абонента.

8. Способ по п. 1, в котором аутентификация абонента и аутентификация устройства выполняются одновременно в обменах комбинированными сообщениями.

9. Способ по п. 1, в котором аутентификация абонента выполняется при более раннем и отдельном от аутентификации устройства защищенном обмене данными.

10. Способ по п. 1, в котором защитный ключ генерируется как функция от по меньшей мере первого ключа, полученного при аутентификации абонента, и второго ключа, полученного при аутентификации устройства.

11. Способ по п. 10, в котором защитный ключ также представляет собой функцию одноразового слова шифрования сети и одноразового слова шифрования устройства.

12. Способ по п. 1, в котором устройство представляет собой ретрансляционный узел, который выступает как терминал доступа к сетевому объекту, а также выступает как сетевое устройство для одного или нескольких терминалов доступа.

13. Способ по п. 1, в котором защитный ключ отдельно генерируется устройством и сетевым объектом.

14. Способ по п. 1, дополнительно содержащий:

обеспечение специфического для абонента ключа как части соглашения на обслуживание, при этом специфический для абонента ключ используется для аутентификации абонента; и

обеспечение специфического для устройства ключа в устройстве при производстве, при этом специфический для устройства ключ используется для аутентификации устройства.

15. Устройство, содержащее:

интерфейс связи; и

схему обработки, соединенную с интерфейсом связи, при этом схема обработки сконфигурирована, чтобы:

выполнять аутентификацию абонента с сетевым объектом;

выполнять аутентификацию устройства с сетевым объектом для упомянутого устройства;

генерировать защитный ключ, связывающий аутентификацию абонента и аутентификацию устройства; и

использовать защитный ключ, чтобы обезопасить связь между устройством и обслуживающей сетью.

16. Устройство по п. 15, в котором аутентификация абонента основана на обмене данными соглашения о ключе аутентификации между устройством и сетевым объектом.

17. Устройство по п. 15, в котором аутентификация устройства основана на обмене данными по схеме «запрос-ответ» между устройством и сетевым объектом.

18. Устройство по п. 15, в котором аутентификация устройства выполняется посредством:

приема данных от сетевого объекта, которые зашифрованы с помощью открытого

RU 2013101768 A

RU 2013101768 A

ключа устройства;

использования соответствующего секретного ключа, чтобы расшифровать зашифрованные данные; и

последующего доказательства сетевому объекту того, что устройство обладает сведениями о данных.

19. Устройство по п. 15, дополнительно содержащее:

отправку запроса о присоединении от устройства к сетевому объекту, при этом запрос о присоединении включает в себя индикацию возможностей аутентификации устройства у упомянутого устройства.

20. Устройство по п. 15, в котором аутентификация устройства защищена по меньшей мере одним ключом, сгенерированным во время аутентификации абонента.

21. Устройство по п. 15, в котором аутентификация абонента и аутентификация устройства выполняются одновременно в обменах комбинированными сообщениями.

22. Устройство по п. 15, в котором аутентификация абонента выполняется при более раннем и отдельном от аутентификации устройства защищенном обмене данными.

23. Устройство по п. 15, в котором защитный ключ генерируется как функция от по меньшей мере первого ключа, полученного при аутентификации абонента, и второго ключа, полученного при аутентификации устройства.

24. Устройство по п. 15, причем устройство представляет собой ретрансляционный узел, который выступает как терминал доступа к сетевому объекту, а также выступает как сетевое устройство для одного или нескольких терминалов доступа.

25. Устройство по п. 15, дополнительно содержащее:

съемное запоминающее устройство, соединенное со схемой обработки и хранящее специфический для абонента ключ, используемый для аутентификации абонента; и

защищенное запоминающее устройство, соединенное со схемой обработки и хранящее специфический для устройства ключ, используемый для аутентификации устройства.

26. Устройство, содержащее:

средство для выполнения аутентификации абонента с сетевым объектом;

средство для выполнения аутентификации устройства с сетевым объектом для упомянутого устройства;

средство для генерации защитного ключа, связывающего аутентификацию абонента и аутентификацию устройства; и

средство для использования защитного ключа, чтобы обезопасить связь между устройством и обслуживающей сетью.

27. Устройство по п. 26, дополнительно содержащее:

средство для хранения специфического для абонента ключа, используемого для аутентификации абонента; и

средство для хранения специфического для устройства ключа, используемого для аутентификации устройства.

28. Считываемый процессором носитель, содержащий инструкции, действующие в устройстве, которые при исполнении процессором побуждают процессор:

выполнять аутентификацию абонента с сетевым объектом;

выполнять аутентификацию устройства с сетевым объектом для упомянутого устройства;

генерировать защитный ключ, который связывает аутентификацию абонента и аутентификацию устройства; и

использовать защитный ключ, чтобы обезопасить связь между устройством и обслуживающей сетью.

29. Способ, действующий в сетевом объекте, содержащий:

выполнение аутентификации абонента с устройством;

RU 2013101768 A

RU 2013101768 A

выполнение аутентификации устройства для упомянутого устройства;

генерацию защитного ключа, который связывает аутентификацию абонента и аутентификацию устройства; и

использование защитного ключа, чтобы обезопасить связь между сетевым объектом и устройством.

30. Способ по п. 29, в котором аутентификация абонента основана на обмене данными соглашения о ключе аутентификации между сетевым объектом и устройством.

31. Способ по п. 29, в котором аутентификация устройства основана на обмене данными по схеме «запрос-ответ» между сетевым объектом и устройством.

32. Способ по п. 29, в котором аутентификация устройства включает в себя:

прием сертификата от устройства;

проверку сертификата, ассоциированного с устройством, на предмет того, что он не был аннулирован.

33. Способ по п. 29, дополнительно содержащий:

прием запроса о присоединении от устройства, при этом запрос о присоединении включает в себя индикацию возможностей аутентификации устройства у упомянутого устройства.

34. Способ по п. 29, в котором аутентификация устройства защищена по меньшей мере одним ключом, сгенерированным во время аутентификации абонента.

35. Способ по п. 29, в котором аутентификация абонента и аутентификация устройства выполняются одновременно в обменах комбинированными сообщениями.

36. Способ по п. 29, в котором аутентификация абонента выполняется при более раннем и отдельном от аутентификации устройства защищенном обмене данными.

37. Способ по п. 29, в котором защитный ключ генерируется как функция от по меньшей мере первого ключа, полученного при аутентификации абонента, и второго ключа, полученного при аутентификации устройства.

38. Способ по п. 29, в котором защитный ключ отдельно генерируется устройством и сетевым объектом.

39. Способ по п. 29, дополнительно содержащий:

получение специфического для абонента ключа как части соглашения на обслуживание, при этом специфический для абонента ключ используется для аутентификации абонента; и

получение специфического для устройства ключа для упомянутого устройства, при этом специфический для устройства ключ используется для аутентификации устройства.

40. Сетевой объект, содержащий:

интерфейс связи; и

схему обработки, соединенную с интерфейсом связи, при этом схема обработки сконфигурирована, чтобы:

выполнять аутентификацию абонента с устройством;

выполнять аутентификацию устройства для упомянутого устройства;

генерировать защитный ключ, связывающий аутентификацию абонента и аутентификацию устройства; и

использовать защитный ключ, чтобы обезопасить связь между сетевым объектом и устройством.

41. Сетевой объект по п. 40, в котором аутентификация абонента основана на обмене данными соглашения о ключе аутентификации между сетевым объектом и устройством.

42. Сетевой объект по п. 40, в котором аутентификация устройства основана на обмене данными по схеме «запрос-ответ» между сетевым объектом и устройством.

43. Сетевой объект по п. 40, в котором схема обработки дополнительно сконфигурирована, чтобы:

RU 2013101768 A

RU 2013101768 A

принимать запрос о присоединении от устройства, при этом запрос о присоединении включает в себя индикацию возможностей аутентификации устройства у упомянутого устройства.

44. Сетевой объект по п. 40, в котором аутентификация устройства защищена по меньшей мере одним ключом, сгенерированным во время аутентификации абонента.

45. Сетевой объект по п. 40, в котором аутентификация абонента и аутентификация устройства выполняются одновременно в обменах комбинированными сообщениями.

46. Сетевой объект по п. 40, в котором аутентификация абонента выполняется при более раннем и отдельном от аутентификации устройства защищенном обмене данными.

47. Сетевой объект по п. 40, в котором защитный ключ генерируется как функция от по меньшей мере первого ключа, полученного при аутентификации абонента, и второго ключа, полученного при аутентификации устройства.

48. Сетевой объект по п. 40, дополнительно содержащий:

получение специфического для абонента ключа как части соглашения на обслуживание, при этом специфический для абонента ключ используется для аутентификации абонента; и

получение специфического для устройства ключа для упомянутого устройства, при этом специфический для устройства ключ используется для аутентификации устройства.

49. Сетевой объект, содержащий:

средство для выполнения аутентификации абонента с устройством;

средство для выполнения аутентификации устройства для упомянутого устройства;

средство для генерации защитного ключа, связывающего аутентификацию абонента и аутентификацию устройства; и

средство для использования защитного ключа, чтобы обезопасить связь между сетевым объектом и устройством.

50. Считываемый процессором носитель, содержащий инструкции, действующие в сетевом объекте, которые при исполнении процессором побуждают процессор:

выполнять аутентификацию абонента с устройством;

выполнять аутентификацию устройства для упомянутого устройства;

генерировать защитный ключ, который связывает аутентификацию абонента и аутентификацию устройства; и

использовать защитный ключ, чтобы обезопасить связь между сетевым объектом и устройством.

RU 2013101768 A

RU 2013101768 A