РОССИЙСКАЯ ФЕДЕРАЦИЯ

(19) **RU** (11) **2012 116 881** (13) **A**

(51) МПК
*H04W 12/04* (2009.01)

ФЕДЕРАЛЬНАЯ СЛУЖБА
ПО ИНТЕЛЛЕКТУАЛЬНОЙ СОБСТВЕННОСТИ

# (12) ЗАЯВКА НА ИЗОБРЕТЕНИЕ

(21)(22) Заявка: **2012116881/08, 28.07.2010**

Приоритет(ы):
(30) Конвенционный приоритет:
**29.09.2009 US 61/246,723**

(43) Дата публикации заявки: **10.11.2013** Бюл. № **31**

(85) Дата начала рассмотрения заявки PCT на национальной фазе: **02.05.2012**

(86) Заявка PCT:
**IB 2010/053440 (28.07.2010)**

(87) Публикация заявки PCT:
**WO 2011/039655 (07.04.2011)**

Адрес для переписки:
**191036, Санкт-Петербург, а/я 24, "НЕВИНПАТ"**

(71) Заявитель(и):
**Нокиа Корпорейшн (FI)**

(72) Автор(ы):
**ФРАНКЛИН Стивен (GB),**
**ДЖЭРИ Стюарт (GB),**
**КУБОТА Кейичи (GB)**

## (54) СПОСОБ И УСТРОЙСТВО ДЛЯ УПРАВЛЕНИЯ КЛЮЧАМИ ПОСЛЕ СБОЯ ПРИ ХЭНДОВЕРЕ

### (57) Формула изобретения

1. Устройство для обеспечения управления ключами для хэндовера между различными доменами, содержащее по меньшей мере один процессор и по меньшей мере одну память, включающую компьютерный программный код, при этом указанная по меньшей мере одна память и указанный компьютерный программный код конфигурированы так, чтобы, совместно с процессором, обеспечивать выполнение устройством по меньшей мере следующих операций:

определение того, имеется ли индикация потенциального несоответствия ключей, в ответ на попытку выполнения хэндовера между первым доменом и вторым доменом и

установление действительности последнего набора ключей, используемого для осуществления шифрованной связи между мобильным терминалом и сетевым устройством, на основе результата указанного определения.

2. Устройство по п.1, отличающееся тем, что указанные память и компьютерный программный код также конфигурированы так, чтобы, совместно с процессором, обеспечивать инициирование устройством обмена новыми ключами в ответ на установление недействительности последнего набора ключей.

3. Устройство по п.1, отличающееся тем, что указанные память и компьютерный программный код также конфигурированы так, чтобы, совместно с процессором, обеспечивать определение устройством того, имеется ли индикация потенциального несоответствия ключей, путем определения, принято ли мобильным терминалом от

RU 2012116881 A

RU 2012116881 A

сетевого устройства подтверждение приема сообщения о завершении хэндовера, переданного указанным мобильным терминалом.

4. Устройство по п.1, отличающееся тем, что указанные память и компьютерный программный код также конфигурированы так, чтобы, совместно с процессором, обеспечивать определение устройством того, имеется ли индикация потенциального несоответствия ключей, путем определения, имеется ли синхронизация уровня 1.

5. Устройство по п.1, отличающееся тем, что указанные память и компьютерный программный код также конфигурированы так, чтобы, совместно с процессором, обеспечивать определение устройством того, имеется ли индикация потенциального несоответствия ключей, путем определения, предпринимает ли мобильный терминал попытку вернуться в исходное состояние после сбоя при хэндовере.

6. Устройство по п.1, отличающееся тем, что указанные память и компьютерный программный код также конфигурированы так, чтобы, совместно с процессором, обеспечивать определение устройством того, имеется ли индикация потенциального несоответствия ключей, путем определения, содержит ли принятая команда хэндовера действительные данные конфигурации.

7. Устройство по п.1, отличающееся тем, что указанные память и компьютерный программный код также конфигурированы так, чтобы, совместно с процессором, обеспечивать определение устройством того, имеется ли индикация потенциального несоответствия ключей, путем определения, принято ли сетевым устройством сообщение о завершении хэндовера от мобильного терминала.

8. Устройство по п.1, отличающееся тем, что указанные память и компьютерный программный код также конфигурированы так, чтобы, совместно с процессором, обеспечивать установление указанным устройством действительности последнего набора ключей путем установления недействительности последнего набора ключей в сетевом устройстве или в мобильном терминале в ответ на обнаружение наличия индикации потенциального несоответствия ключей.

9. Устройство по п.1, представляющее собой мобильный терминал и содержащее также схему пользовательского интерфейса, конфигурированную для упрощения для пользователя управления по меньшей мере некоторыми функциями мобильного терминала.

10. Способ обеспечения управления ключами для хэндовера между различными доменами, включающий:

определение того, имеется ли индикация потенциального несоответствия ключей, в ответ на попытку выполнения хэндовера между первым доменом и вторым доменом и

установление действительности последнего набора ключей, используемого для осуществления шифрованной связи между мобильным терминалом и сетевым устройством, на основе результата указанного определения.

11. Способ по п.10, также включающий инициирование обмена новыми ключами в ответ на установление недействительности последнего набора ключей.

12. Способ по п.10, отличающийся тем, что указанное определение того, имеется ли индикация потенциального несоответствия ключей, включает определение, принято ли мобильным терминалом от сетевого устройства подтверждение приема сообщения о завершении хэндовера, переданного указанным мобильным терминалом.

13. Способ по п.10, отличающийся тем, что указанное определение того, имеется ли индикация потенциального несоответствия ключей, включает определение, имеется ли синхронизация уровня 1.

14. Способ по п.10, отличающийся тем, что указанное определение того, имеется ли индикация потенциального несоответствия ключей, включает определение,

RU 2012116881 A

RU 2012116881 A

предпринимает ли мобильный терминал попытку вернуться в исходное состояние после сбоя при хэндовере.

15. Способ по п.10, отличающийся тем, что указанное определение того, имеется ли индикация потенциального несоответствия ключей, включает определение, содержит ли принятая команда хэндовера действительные данные конфигурации.

16. Способ по п.10, отличающийся тем, что указанное определение того, имеется ли индикация потенциального несоответствия ключей, включает определение, принято ли сетевым устройством сообщение о завершении хэндовера от мобильного терминала.

17. Способ по п.10, отличающийся тем, что установление действительности последнего набора ключей включает установление недействительности последнего набора ключей в сетевом устройстве или в мобильном терминале в ответ на обнаружение наличия индикации потенциального несоответствия ключей.

18. Машиночитаемый носитель, на котором хранятся части исполняемого компьютером программного кода, содержащие инструкции программного кода для выполнения способа по любому из пп.10-17.

RU 2012116881 A

RU 2012116881 A