РОССИЙСКАЯ ФЕДЕРАЦИЯ

(19) **RU** (11) **2015 114 703** (13) **A**

(51) МПК
H04W 4/00 (2009.01)

ФЕДЕРАЛЬНАЯ СЛУЖБА
ПО ИНТЕЛЛЕКТУАЛЬНОЙ СОБСТВЕННОСТИ

(12) ЗАЯВКА НА ИЗОБРЕТЕНИЕ

(21)(22) Заявка: **2015114703, 29.10.2013**

Приоритет(ы):
(30) Конвенционный приоритет:
02.11.2012 EP 12191036.8

(43) Дата публикации заявки: **20.12.2016** Бюл. № **35**

(85) Дата начала рассмотрения заявки PCT на национальной фазе: **02.06.2015**

(86) Заявка PCT:
EP 2013/072571 (29.10.2013)

(87) Публикация заявки PCT:
WO 2014/067925 (08.05.2014)

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

(71) Заявитель(и):
МОРФО КАРДЗ ГМБХ (DE)

(72) Автор(ы):
ШРИЯ Санджив (IN),
ФОГАТ Викас (IN)

(54) ТЕЛЕКОММУНИКАЦИОННАЯ ЧИП-КАРТА

(57) Формула изобретения

1. Телекоммуникационная чип-карта (100), позволяющая осуществить регистрацию мобильного телефонного устройства (104) в цифровой сотовой мобильной телекоммуникационной сети (107), содержащая:

- интерфейс (102) считывателя чип-карты, выполненный с возможностью обеспечения связи между телекоммуникационной чип-картой и мобильным телефонным устройством;
- процессорное средство (300) чип-карты;
- защищенное средство (302) памяти для хранения программ для исполнения процессорным средством чип-карты; и
- программу (304), сохраненную в защищенном средстве памяти, содержащую машиночитаемые инструкции, исполнимые процессорным средством чип-карты; при этом исполнение программы предписывает процессорному средству чип-карты выполнять этапы, на которых:
- выполняют (200) первую криптографическую взаимную аутентификацию между телекоммуникационной чип-картой и терминальным устройством (502) через интерфейс считывателя чип-карты, при этом у терминального устройства есть считыватель (507) чип-карты, функционирующий с возможностью соединения с интерфейсом считывателя чип-карты;
- принимают (214) конфигурационное сообщение (400, 402, 404, 406, 408, 410, 524) через интерфейс считывателя чип-карты;

RU 2015114703 A

RU 2015114703 A

- сохраняют (216) конфигурационное сообщение в защищенном средстве памяти;

- удаляют (218) программу из защищенного средства памяти, так что телекоммуникационная чип-карта (100) может быть модифицирована только один раз.

2. Телекоммуникационная чип-карта по п. 1, в которой исполнение инструкций дополнительно предписывает процессорному средству чип-карты выполнять любые из следующих этапов, на которых: выполняют аутентификацию MAC конфигурационного сообщения, проверяют цифровую подпись конфигурационного сообщения, дешифруют конфигурационное сообщение и их комбинации.

3. Телекоммуникационная чип-карта по п. 2 или 3, в которой конфигурационное сообщение является любым из следующего: набором телефонных номеров (402), информацией (400) об абоненте, операционной системой (404), данными (406) рекламы, приложением (408, 410) и их комбинацией.

4. Телекоммуникационная чип-карта по п. 1, в которой исполнение инструкций предписывает процессорному средству чип-карты стирать защищенное средство памяти, прежде чем сохранить конфигурационное сообщение в защищенном средстве памяти.

5. Система (500, 600, 700, 800) обновления для модификации телекоммуникационной чип-карты (100) по любому из предыдущих пунктов, при этом система обновления содержит терминальное устройство (502), при этом терминальное устройство содержит:

- считыватель (507) чип-карты, используемый для приема телекоммуникационной чип-карты и для обмена данными с интерфейсом (102) считывателя чип-карты;

- процессорное средство (506) терминального устройства;

- средство (510) памяти терминала для хранения программы средства терминала, при этом исполнение программы средства терминала предписывает процессорному средству терминала выполнять этапы, на которых:

- выполняют (200) первую криптографическую взаимную аутентификацию между терминальным устройством и телекоммуникационной чип-картой через интерфейс считывателя чип-карты;

- выполняют (202) вторую криптографическую взаимную аутентификацию между терминальным устройством и сервером (504);

- посылают (204) серверу криптографический маркер (518) безопасности;

- запрашивают (206) криптографическое сообщение (522) сервера от сервера;

- принимают (208) криптографическое сообщение сервера от сервера;

- дешифруют (210) криптографическое сообщение сервера с использованием криптографического ключа (530);

- создают (212) конфигурационное сообщение (524) с использованием дешифрованного криптографического сообщения сервера;

- посылают (214) конфигурационное сообщение телекоммуникационной чип-карте через интерфейс считывателя чип-карты.

6. Система обновления по п. 5, в которой терминальное устройство содержит считыватель (604) отпечатка пальца для сканирования отпечатка (606) пальца оператора.

7. Система обновления по п. 6, в которой терминальное устройство дополнительно содержит сохраненную запись (608) отпечатка пальца в средстве памяти терминального устройства, при этом исполнение программы терминального средства дополнительно предписывает терминальному процессору выполнять этап, на котором проверяют отпечаток пальца, сравнивая отпечаток пальца с записью отпечатка пальца, и при этом исполнение программы терминального средства предписывает процессорному средству терминала прерывать запрос криптографического сообщения сервера, если отпечаток пальца не проверен.

8. Система обновления по п. 6 или 7, в которой маркер безопасности содержит отпечаток пальца.

RU 2015114703 A

RU 2015114703 A

9. Система обновления по п. 5, причем система обновления дополнительно содержит считыватель (702) смарт-карты, функционирующий с возможностью взаимодействия через интерфейс со смарт-картой (704), при этом исполнение программы терминального средства дополнительно предписывает процессорному средству терминала выполнять этапы, на которых:

- выполняют криптографическую проверку допустимости смарт-карты, и
- прерывают запрос криптографического сообщения сервера, если отпечаток пальцев не проверен.

10. Система обновления по п. 9, в которой смарт-карта содержит память смарт-карты, содержащую идентификационный маркер (706); при этом идентификационный маркер содержит любое из следующего: сохраненные данные отпечатка пальца, биометрические данные, данные сканирования радужной оболочки глаза, криптографические данные аутентификации и их комбинации; при

этом исполнение программы терминального средства предписывает процессорному средству терминала извлекать идентификационный маркер из памяти смарт-карты через считыватель смарт-карты, при этом маркер безопасности содержит идентификационный маркер.

11. Система обновления по п. 5, в которой терминальное устройство дополнительно содержит пользовательский интерфейс (602), при этом исполнение инструкций дополнительно предписывает терминальному процессору выполнять этап, на котором принимают пользовательские данные (612) от пользовательского интерфейса, при этом маркер безопасности содержит пользовательские данные.

12. Система обновления по п. 5, в которой система обновления содержит сервер.

13. Способ конфигурирования телекоммуникационной чип-карты (100) с использованием системы обновления (500, 600, 700, 800), при этом телекоммуникационная чип-карта содержит интерфейс (102) считывателя чип-карты, выполненный с возможностью обеспечения связи между телекоммуникационной чип-картой и мобильным телефонным устройством, при этом телекоммуникационная чип-карта дополнительно содержит процессорное средство (300) чип-карты, при этом телекоммуникационная чип-карта дополнительно содержит защищенное средство (302) памяти для хранения программы для исполнения процессорным средством чип-карты, при этом телекоммуникационная чип-карта дополнительно содержит программу (304), сохраненную в безопасном средстве, содержащую машиночитаемые инструкции, исполняемые процессорным средством чип-карты, при этом система обновления содержит терминальное устройство (502), при этом терминальное устройство содержит считыватель (507) чип-карты, функционирующий с возможностью приема телекоммуникационной чип-карты и с возможностью обмена данными с интерфейсом считывателя чип-карты, при этом способ содержит этапы, на которых:

- выполняют (200) первую криптографическую взаимную аутентификацию между терминальным устройством и телекоммуникационной чип-картой с использованием интерфейса считывателя чип-карты;
- выполняют (202) вторую криптографическую взаимную

аутентификацию между терминальным устройством и сервером;

- посылают (204) криптографический маркер (518) безопасности из терминального устройства серверу;
- посылают (206) запрос (520) криптографического сообщения сервера от терминального устройства серверу;
- посылают (208) криптографическое сообщение (522) сервера от сервера терминальному устройству;
- дешифруют (210) криптографическое сообщение сервера с использованием

RU 2015114703 A

RU 2015114703 A

криптографического ключа (530);

- создают (212) конфигурационное сообщение (524) с использованием дешифрованного криптографического сообщения сервера;

- посылают (214) конфигурационное сообщение от терминального устройства телекоммуникационной чип-карте;

- сохраняют (216) конфигурационное сообщение в защищенном средстве памяти; и

- удаляют (218) программу из средства памяти, так что телекоммуникационная чип-карта (100) может быть модифицирована только один раз.

14. Способ по п. 13, в котором способ дополнительно содержит этап, на котором идентифицируют абонента с использованием криптографического маркера безопасности.

15. Способ по п. 14, в котором маркер безопасности содержит биометрический идентификатор, и в котором абонент идентифицируется путем сравнения биометрического идентификатора с биометрической базой данных.

RU 2015114703 A

RU 2015114703 A