РОССИЙСКАЯ ФЕДЕРАЦИЯ

(19) **RU** (11) **2008 104 523** (13) **A**

(51) МПК
H04W 4/00 (2009.01)

ФЕДЕРАЛЬНАЯ СЛУЖБА
ПО ИНТЕЛЛЕКТУАЛЬНОЙ СОБСТВЕННОСТИ,
ПАТЕНТАМ И ТОВАРНЫМ ЗНАКАМ

(12) ЗАЯВКА НА ИЗОБРЕТЕНИЕ

(21), (22) Заявка: **2008104523/09, 10.07.2006**

(30) Конвенционный приоритет:
11.07.2005 DE 102005032311.1

(43) Дата публикации заявки: **10.10.2009** Бюл. № **28**

(85) Дата перевода заявки PCT на национальную фазу: **11.02.2008**

(86) Заявка PCT:
EP 2006/006734 (10.07.2006)

(87) Публикация PCT:
WO 2007/006535 (18.01.2007)

Адрес для переписки:
101000, Москва, М.Златоустинский пер., 10, кв.15, "ЕВРОМАРКПАТ", пат.пов. И.А.Веселицкой, рег. № 11

(71) Заявитель(и):
ГИЗЕКЕ УНД ДЕВРИЕНТ ГМБХ (DE)

(72) Автор(ы):
ВАЙСС Дитер (DE),
РАНКЛЬ Вольфганг (DE)

(54) ПОСЛЕДУЮЩАЯ РЕАЛИЗАЦИЯ ФУНКЦИОНАЛЬНОСТИ МОДУЛЯ ИДЕНТИФИКАЦИИ АБОНЕНТА В ЗАЩИЩЕННОМ МОДУЛЕ

(57) Формула изобретения

1. Способ последующей реализации в защищенном модуле (3) функциональности модуля идентификации абонента, позволяющей с помощью мобильного радиотелефона (1) пользоваться сетью подвижной радиосвязи, при осуществлении которого:

функциональность модуля идентификации абонента реализуют в виде приложения, по меньшей мере первую часть которого загружают в защищенный модуль (3),

данные персонализации, необходимые для пользования сетью подвижной радиосвязи с помощью мобильного радиотелефона (1), передают в зашифрованном виде от провайдера (2) прямо или опосредованно в защищенный модуль (3),

зашифрованные данные персонализации расшифровывают посредством защищенного модуля (3) с помощью хранящегося в защищенном модуле (3) секретного ключа пользователя и

защищенный модуль (3) персонализируют с помощью расшифрованных данных персонализации.

2. Способ по п.1, отличающийся тем, что в первую часть приложения входят операции, важные для обеспечения безопасности.

3. Способ по п.1, отличающийся тем, что вторую часть приложения загружают в

RU 2008104523 A

RU 2008104523 A

мобильный радиотелефон (1).

4. Способ по п.1, отличающийся тем, что зашифрованные данные персонализации передаются по соответствующему запросу, направляемому пользователем провайдеру (2).

5. Способ по п.4, отличающийся тем, что запрос содержит открытый ключ пользователя и/или идентификатор пользователя, в частности зашифрованный открытым ключом провайдера (2).

6. Способ по п.4 или 5, отличающийся тем, что запрос содержит еще один идентификатор, на основании которого пользователю предоставляется пакет услуг.

7. Способ по п.1, отличающийся тем, что секретный ключ пользователя записан в защищенном модуле (3) уже при выдаче защищенного модуля (3) пользователю.

8. Способ по п.1, отличающийся тем, что секретный ключ пользователя генерируют после выдачи защищенного модуля (3) пользователю и записывают в защищенном модуле (3).

9. Способ по п.8, отличающийся тем, что секретный ключ пользователя генерируют посредством защищенного модуля (3).

10. Способ по п.8 или 9, отличающийся тем, что секретный ключ пользователя генерируют вместе с открытым ключом пользователя в виде пары ключей.

11. Способ по п.1, отличающийся тем, что передачу данных между защищенным модулем (3) и провайдером (2) осуществляют через радиоинтерфейс мобильного радиотелефона (1) или он-лайновое соединение, устанавливаемое с помощью другого устройства.

12. Способ по п.1, отличающийся тем, что в качестве защищенного модуля (3) используют носитель данных, отличающийся от чип-карты в формате ID-1 или ID-000 по стандарту ISO 7810.

13. Способ по п.1, отличающийся тем, что в качестве защищенного модуля (3) используют модуль доверительной платформы или защищенную мультимедийную карту.

RU 2008104523 A

RU 2008104523 A