РОССИЙСКАЯ ФЕДЕРАЦИЯ

(19) **RU** (11) **2006 120 406** (13) **A**

(51) МПК
H04L 29/06 (2006.01)

ФЕДЕРАЛЬНАЯ СЛУЖБА
ПО ИНТЕЛЛЕКТУАЛЬНОЙ СОБСТВЕННОСТИ,
ПАТЕНТАМ И ТОВАРНЫМ ЗНАКАМ

(12) ЗАЯВКА НА ИЗОБРЕТЕНИЕ

(21), (22) Заявка: **2006120406/09, 10.11.2004**

(30) Конвенционный приоритет:
11.11.2003 DE 10352538.6
16.12.2003 DE 10358987.2

(43) Дата публикации заявки: **27.12.2007 Бюл. № 36**

(85) Дата перевода заявки PCT на национальную фазу:
13.06.2006

(86) Заявка PCT:
EP 2004/052909 (10.11.2004)

(87) Публикация PCT:
WO 2005/046157 (19.05.2005)

Адрес для переписки:
129010, Москва, ул. Б.Спасская, 25, стр.3,
ООО "Юридическая фирма Городисский и
Партнеры", пат.пов. Г.Б. Егоровой, рег.№ 513

(71) Заявитель(и):
СИМЕНС АКЦИЕНГЕЗЕЛЛЬШАФТ (DE)

(72) Автор(ы):
ХОРН Гюнтер (DE)

(54) СПОСОБ ОБЕСПЕЧЕНИЯ ТРАФИКА ДАННЫХ МЕЖДУ ПЕРВЫМ ОКОНЕЧНЫМ УСТРОЙСТВОМ И ПЕРВОЙ СЕТЬЮ, А ТАКЖЕ ВТОРЫМ ОКОНЕЧНЫМ УСТРОЙСТВОМ И ВТОРОЙ СЕТЬЮ

(57) Формула изобретения

1. Способ обеспечения защиты трафика данных между первым оконечным устройством (1) и первой сетью (2), а также вторым оконечным устройством (4) и второй сетью (6), причем первое оконечное устройство (1) с помощью одного или нескольких первых ключей сеанса может осуществлять связь в первой сети (2), а второе оконечное устройство (4) с помощью одного или нескольких вторых ключей сеанса может осуществлять связь во второй сети (6),

отличающийся следующими этапами:

первое оконечное устройство (1) связывается со вторым оконечным устройством (4) через локальный интерфейс (3);

в первом оконечном устройстве (1) определяются один или несколько первых ключей сеанса, а один или несколько вторых ключей сеанса выводятся из первых ключей сеанса;

один или несколько вторых ключей сеанса передаются через локальный интерфейс (3) посредством протокола защиты на второе оконечное устройство (4);

второе оконечное устройство (4) с помощью одного или нескольких вторых ключей сеанса и/или с помощью ключей, выведенных из одного или нескольких вторых ключей сеанса, аутентифицируется во второй сети (6) по протоколу аутентификации.

2. Способ по п.1, в котором в качестве части протокола аутентификации вырабатываются ключи, выводимые из одного или нескольких вторых ключей сеанса, и используются для защиты сообщений протокола аутентификации и/или для защиты

RU 2006120406 A

RU 2006120406 A

коммуникаций во второй сети.

3. Способ по п.1 или 2, в котором первая сеть (1) представляет собой сеть протокола GSM, и один или несколько первых ключей сеанса вырабатываются при этом в SIM-модуле (SIM = Модуль идентификации абонента) на первом оконечном устройстве (1).

4. Способ по п.3, в котором протокол аутентификации является протоколом EAP-SIM (EAP = Расширяемый протокол аутентификации; SIM = Модуль идентификации абонента).

5. Способ по п.1 или 2, в котором первая сеть (1) является сетью стандарта UMTS, и один или несколько первых ключей сеанса вырабатываются в USIM-модуле (USIM = Универсальный модуль идентификации абонента) на первом оконечном устройстве (1).

6. Способ по п.5, в котором протокол аутентификации является протоколом EAP-AKA (EAP = Расширяемый протокол аутентификации; AKA = Соглашение о ключах аутентификации).

7. Способ по п.1, в котором локальный интерфейс (3) между первым и вторым оконечным устройством представляет собой беспроводный интерфейс, в частности, интерфейс Bluetooth и инфракрасный интерфейс.

8. Способ по п.1, в котором часть второй сети (6) является локальной сетью, в частности, сетью LAN и/или сетью WLAN.

9. Способ по п.1, в котором протокол защиты выполнен таким образом, что:

первое сообщение сигнализации от второго оконечного устройства (4) посылается к первому оконечному устройству (1), причем первым сообщением сигнализации запускается вывод одного или нескольких вторых ключей сеанса из первых ключей сеанса в первом оконечном устройстве (1);

в ответ на первое сообщение сигнализации второе сообщение сигнализации от первого оконечного устройства (1) посылается ко второму оконечному устройству (4), причем вторым сообщением сигнализации передается один или более вторых ключей сеанса.

10. Способ по п.1, в котором первым сообщением сигнализации передается параметр из протокола аутентификации.

11. Способ по п.9 или 10, в котором протокол защиты является расширенным Bluetooth-SIM-протоколом профиля доступа, который содержит первое и второе сообщения сигнализации.

12. Оконечное устройство, которое выполнено таким образом, что оно может использоваться в способе по любому из предшествующих пунктов в качестве первого оконечного устройства (1).

13. Оконечное устройство по п.12, при этом оконечное устройство содержит средство для определения одного или нескольких первых ключей сеанса и средство для вывода одного или нескольких вторых ключей сеанса из первых ключей сеанса.

14. Оконечное устройство, которое выполнено таким образом, что оно может использоваться в способе по любому из пп.1-11 в качестве второго оконечного устройства.

RU 2006120406 A

RU 2006120406 A