РОССИЙСКАЯ ФЕДЕРАЦИЯ

(19) **RU** (11) **2014 135 325** (13) **A**

(51) МПК
H04L 9/06 (2006.01)

ФЕДЕРАЛЬНАЯ СЛУЖБА
ПО ИНТЕЛЛЕКТУАЛЬНОЙ СОБСТВЕННОСТИ

(12) ЗАЯВКА НА ИЗОБРЕТЕНИЕ

(21)(22) Заявка: **2014135325, 28.01.2013**

Приоритет(ы):
(30) Конвенционный приоритет:
31.01.2012 AT A 131/2012

(43) Дата публикации заявки: **20.03.2016** Бюл. № **08**

(85) Дата начала рассмотрения заявки PCT на национальной фазе: **01.09.2014**

(86) Заявка PCT:
AT 2013/000013 (28.01.2013)

(87) Публикация заявки PCT:
WO 2013/113050 (08.08.2013)

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

(71) Заявитель(и):
ФАЙНЭЛОДЖИК БИЗНЕС ТЕКНОЛОДЖИС ГМБХ (AT)

(72) Автор(ы):
БАЙДЛЬ Хайнрих (AT),
ХРДИ Эрвин (AT),
ШАУЭРХУБЕР Юлиус (AT)

(54) КРИПТОГРАФИЧЕСКИЙ СПОСОБ АУТЕНТИФИКАЦИИ И ИДЕНТИФИКАЦИИ С ШИФРОВАНИЕМ В РЕАЛЬНОМ ВРЕМЕНИ

(57) Формула изобретения

1. Способ защиты данных и гарантии их происхождения, причем данные от клиентского устройства передают в центр в электронно зашифрованном виде, и причем способ содержит следующие этапы:

i) генерация и сохранение RSA-пары ключей, состоящей из первого ключа (Sa) и второго ключа (Pa) для подписывания клиентских сертификатов в центре,

ii) генерация и сохранение двух RSA-пар ключей для клиентского устройства, состоящих из третьего ключа клиентского устройства (Sc) и четвертого ключа клиентского устройства (Pc), а также первого ключа (St) шифрования ключа и второго ключа (Pt) шифрования ключа, причем первый ключ (St) шифрования ключа и второй ключ (Pt) шифрования ключа пригодны для защищенной передачи третьего ключа клиентского устройства (Sc),

iii) генерация зашифрованного ключа путем шифрования третьего ключа клиентского устройства (Sc) вторым ключом (Pt) шифрования ключа, а также генерация клиентского сертификата в центре путем шифрования специфического для клиента телефонного номера, а также IMEI клиентского устройства и/или клиентского номера четвертым ключом клиентского устройства (Pc) и последующего шифрования первым ключом (Sa) для подписывания клиентских сертификатов,

iv) передача зашифрованного ключа и клиентского сертификата на клиентское

RU 2014135325 A

RU 2014135325 A

устройство,

v) передача первого ключа (St) шифрования ключа на клиентское устройство по запросу посредством клиентского

устройства,

vi) дешифрование зашифрованного ключа первым ключом (St) шифрования ключа в клиентском устройстве, причем получают третий ключ клиентского устройства (Sc),

vii) шифрование переупорядоченной числовой последовательности в центре четвертым ключом клиентского устройства (Pc),

viii) передача зашифрованной переупорядоченной числовой последовательности на клиентское устройство,

ix) дешифрование зашифрованной переупорядоченной числовой последовательности в клиентском устройстве третьим ключом клиентского устройства (Sc),

x) шифрование первого ввода PIN-кода в клиентском устройстве третьим ключом клиентского устройства (Sc) в шифр,

xi) передача шифра и клиентского сертификата в центр,

xii) дешифрование шифра в центре четвертым ключом клиентского устройства (Pc), дешифрование первого ввода PIN-кода и проверка переданного клиентского сертификата сохраненным в центре клиентским сертификатом.

2. Способ по п. 1, отличающийся тем, что шифр в центре дешифруют и что переданный от клиентского устройства сертификат сравнивают с сохраненным в центре сертификатом, чтобы верифицировать аутентичность данных.

3. Способ по п. 1, отличающийся тем, что передачу данных от центра на клиентское устройство и от клиентского устройства в центр осуществляют по радиосоединению и/или по проводному соединению.

4. Способ по п. 2, отличающийся тем, что передачу данных от центра на клиентское устройство и от клиентского устройства в центр осуществляют по радиосоединению и/или по проводному соединению.

5. Способ по любому из пп. 1 или 2, отличающийся тем, что переупорядочение переупорядоченной числовой последовательности при инициализации способа однократно выбирается клиентом и передается в центр.

6. Способ по любому из пп. 3 или 4, отличающийся тем, что переупорядочение переупорядоченной числовой последовательности при инициализации способа однократно выбирается клиентом и передается в центр.

7. Способ по любому из пп. 1 или 2, отличающийся тем, что переупорядочение переупорядоченной числовой последовательности в центре для каждой передачи на клиентское устройство генерируют заново.

8. Способ по любому из пп. 3 или 4, отличающийся тем, что переупорядочение переупорядоченной числовой последовательности в центре для каждой передачи на клиентское устройство генерируют заново.

9. Способ по любому из пп. 1 или 2, отличающийся следующими дополнительными этапами:

iii.a) генерация временной метки в центре,

iv.a) передача зашифрованного ключа вместе с временной меткой на клиентское устройство,

x.a) шифрование первого ввода PIN-кода на клиентском устройстве вместе с ключом шифрования в шифр.

10. Способ по любому из пп. 3 или 4, отличающийся следующими дополнительными этапами:

iii.a) генерация временной метки в центре,

iv.a) передача зашифрованного ключа вместе с временной меткой на клиентское

RU 2014135325 A

RU 2014135325 A

устройство,

x.a) шифрование первого ввода PIN-кода на клиентском устройстве вместе с ключом шифрования в шифр.

11. Способ по любому из пп. 1 или 2, отличающийся следующими этапами:

x.b) шифрование второго ввода PIN-кода на клиентском устройстве третьим ключом клиентского устройства (Sc) в шифр, чтобы послать новый PIN-код в центр, и

x.c) шифрование третьего ввода PIN-кода на клиентском устройстве третьим ключом клиентского устройства (Sc) в шифр, чтобы подтвердить новый PIN-код.

12. Способ по любому из пп. 3 или 4, отличающийся следующими этапами:

x.b) шифрование второго ввода PIN-кода на клиентском устройстве третьим ключом клиентского устройства (Sc) в шифр, чтобы послать новый PIN-код в центр, и

x.c) шифрование третьего ввода PIN-кода на клиентском устройстве третьим ключом клиентского устройства (Sc) в шифр, чтобы подтвердить новый PIN-код.

13. Способ по любому из пп. 1 или 2, отличающийся тем, что дополнительно к первому вводу PIN-кода осуществляют числовой ввод номера кредитной карты и/или даты истечения срока кредитной карты, и/или контрольной цифры кредитной карты и вместе с первым

вводом PIN-кода в зашифрованном виде передают в центр.

14. Способ по любому из пп. 3 или 4, отличающийся тем, что дополнительно к первому вводу PIN-кода осуществляют числовой ввод номера кредитной карты и/или даты истечения срока кредитной карты, и/или контрольной цифры кредитной карты и вместе с первым вводом PIN-кода в зашифрованном виде передают в центр.

15. Способ по любому из пп. 1 или 2, отличающийся тем, что дополнительно к первому вводу PIN-кода, осуществляют числовой ввод специфического для товара числа, как, например, ISBN названия книги, и вместе с первым вводом PIN-кода в зашифрованном виде передают в центр.

16. Способ по любому из пп. 3 или 4, отличающийся тем, что дополнительно к первому вводу PIN-кода, осуществляют числовой ввод специфического для товара числа, как, например, ISBN названия книги, и вместе с первым вводом PIN-кода в зашифрованном виде передают в центр

RU 2014135325 A

RU 2014135325 A