РОССИЙСКАЯ ФЕДЕРАЦИЯ

(19) **RU** (11) **2 323 530** (13) **C2**

(51) МПК
*H04L 9/32* (2006.01)

ФЕДЕРАЛЬНАЯ СЛУЖБА
ПО ИНТЕЛЛЕКТУАЛЬНОЙ СОБСТВЕННОСТИ,
ПАТЕНТАМ И ТОВАРНЫМ ЗНАКАМ

# (12) ОПИСАНИЕ ИЗОБРЕТЕНИЯ К ПАТЕНТУ

(21), (22) Заявка: **2004118413/09, 26.11.2002**

(24) Дата начала отсчета срока действия патента:
**26.11.2002**

(30) Конвенционный приоритет:
**28.11.2001 NO 20015812**

(43) Дата публикации заявки: **10.01.2006**

(45) Опубликовано: **27.04.2008 Бюл. № 12**

(56) Список документов, цитированных в отчете о поиске: **RU 2158485 C1, 27.10.2000. US 6061791 A, 09.05.2000. WO 00/24218 A1, 27.04.2000. DE 19820422, T1, 11.11.1999. RU 2111615 C1, 20.05.1998.**

(85) Дата перевода заявки PCT на национальную фазу:
**28.06.2004**

(86) Заявка PCT:
**NO 02/00446 (26.11.2002)**

(87) Публикация PCT:
**WO 03/047161 (05.06.2003)**

Адрес для переписки:
**191186, Санкт-Петербург, а/я 230, "АРС-ПАТЕНТ", пат.пов. В.М.Рыбакову, рег. № 90**

(72) Автор(ы):
**САНДБЕРГ Лейф (SE)**

(73) Патентообладатель(и):
**ТЕЛЕНОР АСА (NO)**

## (54) СПОСОБ РЕГИСТРАЦИИ И АКТИВАЦИИ ФУНКЦИЙ PKI

(57) Реферат:

Изобретение относится к области инфраструктуры открытых ключей (PKI), а именно - регистрации и активации функций PKI в (инфраструктуры открытых ключей в SIM-картах. Сущность способа заключается в том, что ссылочный код и соответствующий код активации заносятся в таблицу на сервере защиты, интегрированном в PKI или подключенном к PKI. Пользователь внесит в бланк заявки ссылочный код или номер, а также свои личные данные, после чего заявка пересылается в PKI и на сервер защиты. После подтверждения регистрации со стороны PKI информация о подтверждении передается пользователю и дополняется просьбой ввести код активации на терминале пользователя. Одновременно код активации, ассоциированный со ссылочным кодом в таблице и идентификационные данные смарт-карты пользователя передаются в модуль активации в PKI, затем код активации вместе с идентификационными данными смарт-карты передаются с терминала в модуль активации и при их получении модуль активации определяет совпадают ли они с кодом активации и идентификационными данными, предварительно предоставленными сервером защиты и при их совпадении модуль выполняет команду активации PKI-компонента смарт-карты. Технический результат - уменьшение времени обработки. 12 з.п. ф-лы.

RU 2323530 C2

RU 2323530 C2

RUSSIAN FEDERATION

(19) **RU** (11) **2 323 530** (13) **C2**

(51) Int. Cl.
*H04L 9/32* (2006.01)

FEDERAL SERVICE
FOR INTELLECTUAL PROPERTY,
PATENTS AND TRADEMARKS

# (12) ABSTRACT OF INVENTION

(21), (22) Application: **2004118413/09, 26.11.2002**

(24) Effective date for property rights: **26.11.2002**

(30) Priority:
**28.11.2001 NO 20015812**

(43) Application published: **10.01.2006**

(45) Date of publication: **27.04.2008 Bull. 12**

(85) Commencement of national phase: **28.06.2004**

(86) PCT application:
**NO 02/00446 (26.11.2002)**

(87) PCT publication:
**WO 03/047161 (05.06.2003)**

Mail address:
**191186, Sankt-Peterburg, a/ja 230, "ARS-PATENT", pat.pov. V.M.Rybakovu, reg. № 90**

(72) Inventor(s):
**SANDBERG Lejf (SE)**

(73) Proprietor(s):
**TELENOR ASA (NO)**

## (54) METHOD FOR REGISTRATION AND ACTIVATION OF PKI FUNCTIONS

(57) Abstract:

FIELD: infrastructure of public keys (PKI), namely, registration and activation of PKI functions in infrastructures of public keys in SIM-cards.

SUBSTANCE: in accordance to the method, reference code and corresponding activation code are recorded in a table at protection server integrated in PKI or connected to PKI. The user inputs reference code or number in record form together with his personal data, after that the form is sent to PKI and to protection server. After registration is confirmed from the side of PKI, the confirmation information is transmitted to user and supplemented with a request to input activation code at user terminal. Simultaneously, the activation code associated with reference code in the table and identification data of smart-card of user are transmitted to activation module in PKI, then activation code together with identification data of smart-card is transmitted from terminal to activation module and on receipt thereof the activation module determines whether the data coincides with activation code and identification data, provided in advance by protection server, and in case they do, the module performs command of activation of PKI-component of smart-card.

EFFECT: reduced processing time.

13 cl

RU 2323530 C2

RU 2323530 C2

Область техники, к которой относится изобретение

Настоящее изобретение относится к области инфраструктуры открытых ключей (PKI), а именно - регистрации и активации функций PKI (инфраструктура открытых ключей) в SIM-картах (Subscriber Identity Module, модуль идентификации абонента).

Уровень техники

Для полной реализации потенциала сетей связи требуется наличие стандартизированной системы, которая позволяла бы пользователям совершать электронные сделки с той же степенью доверия, что и традиционные сделки с использованием бумажных документов.

Для этих целей была разработана инфраструктура PKI, представляющая собой базовую платформу для глобальной коммерции и связи. Использование PKI гарантирует конфиденциальность средств электронных коммуникаций, используемых для передачи важных данных, и их защищенность от вторжения. PKI используется для обработки цифровых подписей, для аутентификации и шифрования.

Инфраструктура PKI основана на использовании криптографии, что подразумевает скремблирование информации с применением математической формулы и виртуального ключа; таким образом, информация может быть декодирована только имеющей на это право стороной, обладающей соответствующим ключом. PKI использует пары криптографических ключей, предоставляемых доверенной третьей стороной, называемой Центром сертификации (ЦС). ЦС - это центральный компонент для операций с PKI; он осуществляет выдачу цифровых сертификатов, которые идентифицируют личность их владельца. ЦС ведет каталоги действительных сертификатов, а также список аннулированных сертификатов, и предоставляет доступ к этим данным.

Традиционно для использования функций PKI использовались терминалы данных, а сертификаты и ключи размещались в отдельной смарт-карте. Однако, по мере внедрения в сотовые телефоны функций терминалов данных, возникает потребность в реализации функций PKI также и в телефонах. При этом сертификаты и ключи будут, как правило, размещаться в абонентских картах, например, в случае телефонов GSM - в SIM-картах (Subscriber Identity Module, модуль идентификации абонента).

Для гарантии безопасности системы PKI, для регистрации новых пользователей путем выдачи цифровых сертификатов требуется применение безопасной процедуры. Необходима полная уверенность в том, что запрашивающее сертификат лицо является именно тем, кем оно представляется. Обычно для этого пользователю необходимо лично посетить какое-либо учреждение, например почтовое отделение, заполнить бланк и подтвердить свою личность каким-либо удостоверением, например паспортом. После того, как работник почтового отделения подтвердит правильность идентификационных данных, данные из заполненного бланка передаются электронным способом в ЦС. ЦС обрабатывает и удостоверяет данные и выпускает PKI-карту, либо в виде SIM-карты, либо смарт-карты, в комплекте с кодом активации. Далее PKI-карта и код активации пересылаются абоненту заказным письмом. Пользователь вновь посещает почтовое отделение, подтверждает свою личность, например, паспортом, и только после этого получает письмо.

Необходимость двукратного посещения учреждения становится препятствием для распространения PKI просто потому, что люди, как можно видеть, неохотно используют новые технологии, если последние имеют высокий входной порог, т.е. требуют большого объема начальных действий. Кроме того, описанный процесс занимает много времени - время, проходящее с момента заказа сертификата до получения абонентом доступа к функциям PKI, составляет, по меньшей мере, одну неделю.

С точки зрения стороны, выдающей цифровые сертификаты, затраты на процесс выдачи относительно высоки, в особенности из-за необходимости подготовки почтового отправления и его пересылки заказной почтой.

Таким образом, существует потребность в упрощении технологии выдачи, что будет выгодно как выдающей стороне, так и абоненту.

Сущность изобретения

Задача, на решение которой направлено настоящее изобретение, заключается в создании способа, не имеющего указанных выше недостатков. Этот способ отличается признаками, включенными в формулу изобретения.

Более конкретно, в настоящем изобретении предлагается способ применения инфраструктуры открытых ключей (Public, Key Infrastructure, PKI) для регистрации пользователя PKI и активации PKI-компонента смарт-карты пользователя с использованием предварительной печати серии запечатанных конвертов, каждый из которых содержит невидимый до вскрытия код активации, а также ссылочный номер или код, напечатанный на конверте снаружи на видном месте. Каждый ссылочный номер или код каждого конверта и ассоциированный с ним код активации хранится в таблице на сервере защиты, интегрированном в PKI или подключенном к PKI. Пользователь получает на руки один из запечатанных конвертов вместе с бланком заявки. Пользователю предлагается внести в форму заявки ссылочный код или номер, а также свои личные данные, после чего вся эта информация передается в PKI и на сервер защиты.

После того как регистрация будет подтверждена PKI, информация о подтверждении передается абоненту вместе с просьбой ввести код активации на своем терминале. Одновременно код активации, ассоциированный со ссылочным кодом или номером в таблице, и идентификационные данные смарт-карты, соответствующие смарт-карте пользователя, передаются в модуль активации в PKI. После ввода кода активации на терминале, код активации вместе с идентификационными данными смарт-карты передается с терминала в модуль активации. После получения кода активации и идентификационных данных смарт-карты модуль активации определяет, совпадают ли полученный код активации и идентификационные данные смарт-карты соответственно с кодом активации и идентификационными данными, предварительно предоставленными сервером защиты, и если совпадение подтверждается, модуль активации выполняет необходимую процедуру активации PKI-компонента смарт-карты.

Более конкретно, в настоящем изобретении предлагается способ надежной и безопасной активации компонента смарт-карты, являющегося частью инфраструктуры открытых ключей (PKI), в первом мобильном терминале, причем указанный мобильный терминал подключен к сети мобильной связи, предоставляющей доступ к серверу PKI, подключенному к той же сети, причем к той же сети подключен центр сертификации. Отличительными особенностями способа согласно изобретению является то, что он включает в себя следующие шаги:

a) предоставление пользователю второго кода активации;

b) прием электронным способом сервером PKI запроса на активацию PKI-компонента смарт-карты для пользователя, причем указанный запрос содержит по меньшей мере личные данные пользователя и ссылочный код, ассоциированный со вторым кодом активации;

c) обработка сервером PKI указанного запроса;

d) генерирование сервером PKI текстового сообщения, причем текстовое содержание указанного текстового сообщения является результатом обработки указанного запроса, и посылка текстового сообщения на первый мобильный терминал;

e) ответ первого мобильного терминала на полученное текстовое сообщение посылкой второго кода активации и идентификационных данных SIM-карты, ассоциированных с первым мобильным терминалом, в виде текстового сообщения на сервер PKI;

f) получение сервером PKI первого кода активации, ассоциированного с указанным ссылочным кодом;

g) сравнение сервером PKI второго кода активации с первым кодом активации;

если эти два кода активации совпадают, передача сервером PKI на первый мобильный терминал сообщения о совпадении, причем указанное сообщение является командой активации ключа PKI.

В предпочтительном варианте способ дополнительно включает в себя следующие шаги:

h) передача открытого ключа верификации на сервер PKI, предпочтительно в виде зашифрованного текстового сообщения;

i) введение на первом мобильном терминале PIN-кода, выбираемого самим пользователем;

j) соединение сервера PKI с центром сертификации, после чего центр сертификации выдает действительный сертификат с открытым ключом, ассоциированный с пользователем первого мобильного терминала;

k) получение первым мобильным терминалом подтверждения успешной сертификации, и, как следствие, активация PKI компонента в SIM-карте, ассоциированной с указанным первым терминалом.

В другом варианте предусмотрен сервер защиты, являющийся компонентом сервера PKI, либо непосредственно подключенный к серверу PKI, причем сервер защиты, в свою очередь, подключен к модулю активации.

Указанный шаг b) предпочтительно включает в себя следующие действия: пересылка электронным способом запроса на активацию PKI-компонента смарт-карты для пользователя на сервер защиты, причем сервер защиты в результате получения запроса модифицирует таблицу с данными статуса, ассоциированными с указанным запросом.

Указанные шаги c) и d) предпочтительно включают в себя следующие действия:

- обработка сервером защиты указанного запроса, передача запроса на сервер PKI и обработка запроса сервером PKI,

- передача результата обработки сервером PKI на сервер защиты и модификация сервером защиты указанной таблицы путем внесения в нее текущего статуса запроса,

- генерирование сервером PKI текстового сообщения, причем текстовое содержание текстового сообщения является результатом обработки указанного запроса; посылка текстового сообщения на первый мобильный терминал; причем одновременно или практически одновременно с этим сервер защиты передает первый код активации, который ассоциируется с запрошенным компонентом смарт-карты, в модуль активации.

Указанный шаг e) предпочтительно включает в себя следующие действия:

- активация на первом мобильном терминале меню, предназначенного для операций с PKI,

- ввод пользователем второго кода активации, посылка первым мобильным терминалом второго кода активации и идентификационных данных SIM-карты, ассоциированных с первым мобильным терминалом, в виде текстового сообщения на сервер PKI.

Указанный шаг g) предпочтительно включает в себя следующие действия:

- извлечение модулем активации, как компонентом сервера PKI, второго кода активации и ассоциированных с ним идентификационных данных SIM-карты из сервера PKI и сравнение указанного второго кода активации с полученным до этого первым кодом активации, и, если эти два кода совпадают, передача модулем активации на первый мобильный терминал сообщения, информирующего о совпадении, причем указанное сообщение является командой активации ключа PKI.

Указанные шаги h) и i) предпочтительно включают в себя следующие действия:

- передача в модуль активации сервера PKI открытого ключа верификации, предпочтительно посредством шифрованного текстового сообщения,

- введение на первом мобильном терминале кода, выбираемого самим пользователем,

- соединение модуля активации, как компонента сервера PKI, с центром сертификации, выдача в ответ центром сертификации действительного сертификата с открытым ключом, ассоциированным с пользователем первого мобильного терминала.

Сеть связи предпочтительно является сетью GSM или 3G, указанный терминал является мобильным телефоном GSM или 3G, а указанная смарт-карта является SIM-картой.

Идентификационными данными смарт-карты предпочтительно являются ISDN-номером (MSISDH) и идентификатором смарт-карты (ICCID).

Функции PKI предпочтительно содержатся в указанной смарт-карте, но являются скрытыми для пользователя до их активации.

Информация о подтверждении предпочтительно передается посредством SMS-сообщения, по электронной или обычной почте.

В наиболее предпочтительном варианте статус изначально установлен "не использована" и изменяется на "на рассмотрении" в процессе осуществления шага c), на "принята, но не активирована" в случае принятия в процессе осуществления шага g), и "активирована" в случае совпадения на шаге k).

Осуществление изобретения

Ниже приведено описание настоящего изобретения на примере типового варианта осуществления, когда пользователь желает заказать для своего GSM-телефона SIM-карту, имеющую функции PKI.

Как и ранее, пользователь должен лично посетить уполномоченное учреждение, например, почтовое отделение, банк или приемную оператора телефонной связи, абонентом которого является пользователь.

В уполномоченном учреждении пользователь получает заранее напечатанный запечатанный конверт и бланк заявки, которую ему предлагается заполнить. Ссылочный номер, напечатанный на видном месте, идентифицирует конверт. Бланк и запечатанный конверт, которые пользователь получает в офисе, однозначно связаны друг с другом, поскольку указанный ссылочный номер также либо печатается на бланке, либо должен быть внесен в заявку пользователем вместе с другими данными.

После заполнения бланка сотрудник учреждения проверяет соответствие предоставленных личных данных и данных в удостоверении личности, которое пользователь должен предъявить, и соответствие ссылочного номера номеру, напечатанному на конверте. Если личные данные и номер правильны, заявка отправляется на дальнейшую обработку, а пользователя просят не распечатывать конверт до тех пор, пока он не получит свою новую SIM-карту.

Закрытый конверт содержит код активации, который невидим до вскрытия конверта. Данные обо всех предварительно напечатанных конвертах хранятся, например, в таблице на сервере защиты, подключенном к PKI или интегрированном в PKI. Для каждого конверта хранятся по меньшей мере, соответствующий ссылочный номер, код активации и статус; таким образом, если серверу защиты известен ссылочный номер или код бланка заявки, то ему также известен код активации, который выдается пользователю в конверте вместе с бланком заявки, и текущий статус обработки заявки. Статус может быть одним из следующих: не использована; на рассмотрении; принята, но не активирована; активирована; не принята. Исходный статус - "не использована".

В приведенном примере данные из заявки считываются, предпочтительно электронным способом, и пересылаются на сервер защиты. Одновременно статус конверта в таблице изменяется с "не использована" на "на рассмотрении". Данные из заполненного бланка, который в этом примере следует рассматривать как заявку на SIM-карту с функциями PKI, обрабатываются сервером PKI под управлением ЦС посредством метода, соответствующего современному техническому уровню, который должен быть известен специалисту в данной области техники. Кроме того, статус конверта на сервере защиты изменяется в зависимости от результата обработки. Если заявка получает отказ, то соответствующий статус изменяется на "не принята". Напротив, если заявка принята, соответствующее состояние, как и следовало ожидать, изменяется на "принята".

Затем результат обработки заявки посылается пользователю посредством сообщения, передаваемого по сети связи, предпочтительно в виде SMS-сообщения или подобного сообщения, либо по электронной или обычной почте. Пользователю может быть выслана новая SIM-карта, но при этом не требуется использовать заказную почту, так как пользователь может подтвердить свою личность с помощью кода активации, скрытого в конверте. С другой стороны, если пользователь уже имеет SIM-карту с установленными функциями PKI, но на данный момент они недоступны, исчезает необходимость в выдаче новой SIM-карты. Одновременно сервер защиты передает в модуль активации код активации, ассоциированный со ссылочным номером или кодом, вместе с необходимыми

идентификационными данными соответствующей SIM-карты.

Сообщение о положительном результате будет выглядеть, например, следующим образом: "Ваша заявка принята, пожалуйста, вскройте запечатанный конверт и введите находящийся в нем код активации для Вашей SIM-карты".

Однако прежде чем пользователь сможет ввести код активации, должно быть активировано "Меню SIM PKI" ("SIM PKI menu"). После активации "Меню SIM PKI", для подписки на услугу пользователь вводит на своем телефоне код активации. Код активации посредством SMS-сообщения передается в PKI вместе с идентификационными данными SIM-карты. На ввод правильного кода пользователю дается 3 попытки.

Модуль активации извлекает код активации и идентификационные данные SIM-карты и проверяет их соответствие коду активации и идентификационным данным SIM-карты, предоставленным до этого сервером защиты. Затем модуль активации передает в SIM-карту "Команду запуска генерации ключей PKI" ("Generate PKI keys enabling command"), после чего программа генерации ключей в SIM-карте генерирует пару ключей, состоящую из секретного ключа и открытого ключа верификации.

Открытый ключ верификации (Verification Public Key, VPuK) посредством SMS-сообщения передается в модуль активации, причем SMS-сообщение желательно шифровать согласно спецификации GSM 03.48 по защите важной информации.

Затем Пользователю предлагается выбрать PIN_SIGNKEY, который является самостоятельно определяемым личным PIN-кодом подтверждения, используемым, например, для подписания сделок и идентификации.

В случае успешной верификации модуль активации соединяется с ЦС и выполняется выдача действительного сертификата с открытым ключом, ассоциированного с пользователем. Одновременно этот сертификат посылается в каталог сертификации.

Пользователю посылается подтверждение успешной сертификации, после чего меню PKI в SIM-карте деактивируется. Сразу вслед за этим в SIM-карте активируются функции PKI.

В настоящем изобретении представляется способ регистрации и активации функций PKI (Public Key Infrastructure, инфраструктура открытых ключей), не требующий от пользователя личного появления в уполномоченном учреждении более одного раза. Пересылка предметов и данных, связанных с функциями PKI, после первого подтверждения личности не требуется, поскольку пользователь становится обладателем кода активации до того, как его личность ассоциируется с кодом активации, в частности, в RA. Этим гарантируется то, что правильное лицо получает правильный код активации уже во время первого личного посещения.

С точки зрения пользователя, настоящее изобретение позволяет снизить количество действий, которые необходимо предпринять для получения доступа к функциям PKI. С точки зрения выдающей стороны, настоящее изобретение, вероятнее всего, повысит количество пользователей PKI. Кроме того, снижаются затраты на регистрацию, так как уменьшается время обработки, а необходимость применения заказной почты устраняется.

## Формула изобретения

1. Способ активации компонента смарт-карты, являющегося частью инфраструктуры открытых ключей (PKI), в мобильном терминале, причем указанный мобильный терминал подключен к сети мобильной связи, предоставляющей доступ к серверу PKI, подключенному к той же сети, причем к той же сети подключен центр сертификации, отличающийся тем, что включает в себя следующие шаги:

a) ассоциирование ссылочного кода с кодом активации;

b) прием электронным способом сервером PKI запроса, включающего личные данные пользователя и указанный ссылочный код, на регистрацию пользователя PKI и активацию PKI-компонента смарт-карты пользователя;

c) обработка сервером PKI указанного запроса;

d) генерирование сервером PKI текстового сообщения, причем текстовое содержание

указанного текстового сообщения является результатом обработки указанного запроса, и передача текстового сообщения на мобильный терминал;

e) передача мобильным терминалом в ответ на полученное текстовое сообщение кода активации и идентификационных данных SIM-карты, ассоциированных с мобильным терминалом, в виде текстового сообщения на сервер PKI;

f) сравнение сервером PKI переданного кода активации с предварительно полученным кодом активации, ассоциированным со ссылочным кодом, и передача при их совпадении сервером PKI на мобильный терминал сообщения о совпадении, причем указанное сообщение является командой активации ключа PKI.

2. Способ по п.1, отличающийся тем, что дополнительно включает в себя следующие шаги: g) передача открытого ключа верификации на сервер PKI, предпочтительно в виде зашифрованного текстового сообщения; h) введение на мобильном терминале PIN-кода, выбираемого самим пользователем;

i) соединение сервера PKI с центром сертификации, после чего центр сертификации выдает действительный сертификат с открытым ключом, ассоциированный с пользователем мобильного терминала; j) получение мобильным терминалом подтверждения успешной сертификации, и, как следствие, активация функции PKI в SIM-карте, ассоциированной с указанным терминалом.

3. Способ по п.1 или 2, отличающийся тем, что предусмотрен сервер защиты, являющийся компонентом сервера PKI, либо непосредственно подключенный к серверу PKI, причем сервер защиты, в свою очередь, подключен к модулю активации.

4. Способ по п.3, отличающийся тем, что шаг b) дополнительно включает в себя следующие действия: пересылка электронным способом запроса на активацию PKI-компонента смарт-карты для пользователя на сервер защиты, причем сервер защиты в результате получения запроса модифицирует таблицу с данными статуса, ассоциированными с указанным запросом.

5. Способ по п.4, отличающийся тем, что шаги c) и d) включают в себя следующие действия: обработка сервером защиты указанного запроса, передача запроса на сервер PKI и обработка запроса сервером PKI, передача результата обработки сервером PKI на сервер защиты и модификация сервером защиты указанной таблицы путем внесения в нее текущего статуса запроса, генерирование сервером PKI текстового сообщения, причем текстовое содержание текстового сообщения является результатом обработки указанного запроса; передача на мобильный терминал указанного текстового сообщения; причем сервер защиты передает код активации, который ассоциируется с запрошенным компонентом смарт-карты, в модуль активации.

6. Способ по п.5, отличающийся тем, что шаг e) включает в себя следующие действия:

активация на мобильном терминале меню, предназначенного для операций с PKI,

ввод пользователем кода активации, посылка мобильным терминалом кода активации и идентификационных данных SIM-карты, ассоциированных с мобильным терминалом, в виде текстового сообщения на сервер PKI.

7. Способ по п.6, отличающийся тем, что шаг f) включает в себя следующие действия:

извлечение модулем активации, как компонентом сервера PKI, кода активации и ассоциированных с ним идентификационных данных SIM-карты из сервера PKI и сравнение указанного кода активации с кодом активации, переданным мобильным терминалом, и передача при их совпадении модулем активации на мобильный терминал сообщения, информирующего о совпадении, причем указанное сообщение является командой активации ключа PKI.

8. Способ по п.6, отличающийся тем, что шаги g) и h) включают в себя следующие действия: передача в модуль активации сервера PKI открытого ключа верификации, предпочтительно посредством шифрованного текстового сообщения, введение на мобильном терминале кода, выбираемого самим пользователем, соединение модуля активации, как компонента сервера PKI, с центром сертификации, выдача в ответ центром сертификации действительного сертификата с открытым ключом, ассоциированным с

пользователем мобильного терминала.

9. Способ по п.1, отличающийся тем, что указанная сеть связи является сетью GSM или 3G, указанный терминал является мобильным телефоном GSM или 3G, указанная смарт-карта является SIM-картой.

10. Способ по п.9, отличающийся тем, что идентификационными данными смарт-карты являются ISDN-номером (MSISDH) и идентификатором смарт-карты (ICCID).

11. Способ по одному из пп.1, 2, 4-10, отличающийся тем, что указанные функции PKI содержатся в указанной смарт-карте, но являются скрытыми для пользователя до их активации.

12. Способ по одному из пп.2, 4-10, отличающийся тем, что информация о подтверждении передается посредством SMS-сообщения, по электронной или обычной почте.

13. Способ по одному из пп.1, 2 или 5, отличающийся тем, что статус изначально установлен "не использована" и изменяется на "на рассмотрении" в процессе осуществления шага c) в п.1, на "принята, но не активирована" в случае принятия в процессе осуществления шага f) в п.1, и "активирована" в случае совпадения в шаге j) в п.2.