РОССИЙСКАЯ ФЕДЕРАЦИЯ

(19) **RU** (11) **2 292 591** (13) **C2**

(51) МПК
G07B 17/00 (2006.01)
G07D 7/00 (2006.01)

ФЕДЕРАЛЬНАЯ СЛУЖБА
ПО ИНТЕЛЛЕКТУАЛЬНОЙ СОБСТВЕННОСТИ,
ПАТЕНТАМ И ТОВАРНЫМ ЗНАКАМ

(12) ОПИСАНИЕ ИЗОБРЕТЕНИЯ К ПАТЕНТУ

(21), (22) Заявка: **2003137601/09, 28.06.2002**

(24) Дата начала отсчета срока действия патента:
28.06.2002

(30) Конвенционный приоритет:
01.07.2001 DE 10131254.7

(43) Дата публикации заявки: **27.05.2005**

(45) Опубликовано: **27.01.2007 Бюл. № 3**

(56) Список документов, цитированных в отчете о поиске: **EP 732673 A2, 18.09.1996. RU 2158443 C1, 27.10.2000. SU 1304173 A1, 15.04.1987. US 4461028 A, 17.07.1984. US 5953427 A, 14.09.1999. EP 600646 A2, 08.06.1994. US 5091634 A, 25.02.1992.**

(85) Дата перевода заявки PCT на национальную фазу:
02.02.2004

(86) Заявка PCT:
DE 02/02348 (28.06.2002)

(87) Публикация PCT:
WO 03/005307 (16.01.2003)

Адрес для переписки:
191036, Санкт-Петербург, а/я 24, "НЕВИНПАТ", пат.пов. А.В.Поликарпову, рег.№ 009

(72) Автор(ы):
ДЕЛИЦ Александер (DE),
ФЕРИ Петер (DE),
ХЕЛЬМУС Юрген (DE),
ХЕЛЬ Алоизиус (DE),
МАЙЕР Гюнтер (DE),
РОБЕЛЬ Эльке (DE),
ШТУММ Дитер (DE)

(73) Патентообладатель(и):
Дойче Пост АГ (DE)

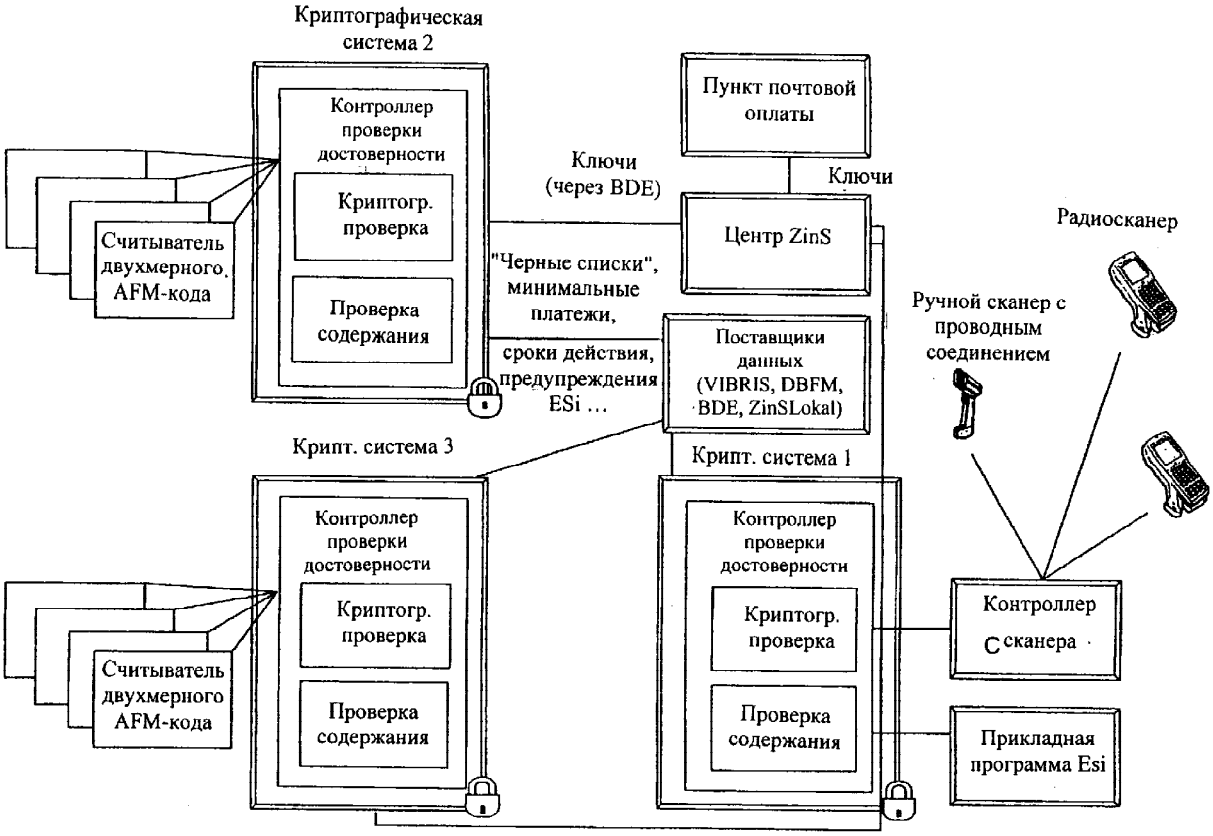
(54) СПОСОБ ПРОВЕРКИ ДЕЙСТВИТЕЛЬНОСТИ ЦИФРОВЫХ ОТМЕТОК О ФРАНКИРОВАНИИ

(57) Реферат:

Изобретение относится к средствам проверки отметок о франкировании почтовых отправлений. Техническим результатом является повышение надежности и быстроты проверки. В способе проверки подлинности отметки о франкировании, нанесенной на почтовое отправление, криптографическая информация, содержащаяся в этой отметке, дешифруется и используется для анализа ее подлинности, при этом считывающее устройство графически регистрирует отметку о франкировании и передает ее в проверочное устройство, которое управляет ходом частичных проверок, заключающихся, в частности, в выделении в содержимом штрих-кода отметки криптографической строки с симметричным ключом и ее дешифровании, а также в проверке времени между франкированием и датой ее частичной проверки. 13 з.п. ф-лы, 3 табл., 7 ил.

RU 2292591 C2

RU 2292591 C2



Фиг.2

RU 2292591 C2

RU 2292591 C2

RUSSIAN FEDERATION

(19) **RU** (11) **2 292 591** (13) **C2**

(51) Int. Cl.
G07B 17/00 (2006.01)
G07D 7/00 (2006.01)

FEDERAL SERVICE
FOR INTELLECTUAL PROPERTY,
PATENTS AND TRADEMARKS

(12) ABSTRACT OF INVENTION

(21), (22) Application: **2003137601/09, 28.06.2002**

(24) Effective date for property rights: **28.06.2002**

(30) Priority:
01.07.2001 DE 10131254.7

(43) Application published: **27.05.2005**

(45) Date of publication: **27.01.2007 Bull. 3**

(85) Commencement of national phase: **02.02.2004**

(86) PCT application:
DE 02/02348 (28.06.2002)

(87) PCT publication:
WO 03/005307 (16.01.2003)

Mail address:
191036, Sankt-Peterburg, a/ja 24, "NEVINPAT", pat.pov. A.V.Polikarpovu, reg.№ 009

(72) Inventor(s):
DELITs Aleksander (DE),
FERI Peter (DE),
KhEL'MUS Jurgen (DE),
KhEL' Aloizius (DE),
MAJER Gjunter (DE),
ROBEL' Ehl'ke (DE),
ShTUMM Diter (DE)

(73) Proprietor(s):
Dojche Post AG (DE)

(54) METHOD OF CHECKING VALIDITY OF DIGITAL MARKS ON FRANKING

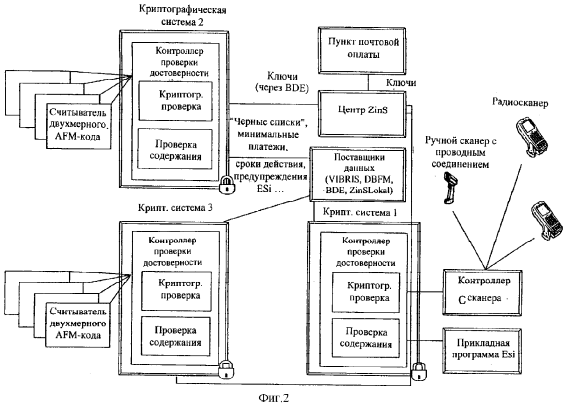
(57) Abstract:

FIELD: means for checking of validity of digital marks on franking.

SUBSTANCE: according to the method, validity of franking mark applied onto post note, the cryptographic data in the note is subject to decoding and is sued for analyzing its validity. Reading device registers mark on franking in digital form and then transmits it to checker, which control procedure of partial checking, including in separation of barcode of mark of cryptographic line with asymmetric key in content and it is subject to decoding. Time is also checked before franking and date of its partial checking as well.

EFFECT: improved reliability of checking; higher speed of operation.

13 cl, 7 dwg



Фиг.2

RU 2292591 C2

RU 2292591 C2

Известно, что почтовые отправления могут снабжаться цифровыми отметками о франкировании (знаками почтовой оплаты).

Чтобы облегчить отправителям почтовых отправлений создание отметок о франкировании, можно, например, в системе франкирования, применяемой в Deutsche Post AG, создавать эти отметки в клиентской системе и выдавать их на печатающее устройство через произвольный интерфейс.

Чтобы избежать неправомерного использования этого способа, в цифровые отметки о франкировании включают криптографическую информацию, например информацию, идентифицирующую клиентскую систему, управляющую созданием отметки о франкировании.

В основе изобретения лежит задача создания способа, с помощью которого подлинность отметок о франкировании может быть проверена быстро и надежно. В частности, способ должен быть пригоден для проверки в массовом масштабе, особенно в почтовых или грузовых центрах.

Согласно изобретению эта задача решается посредством того, что считывающее устройство графически регистрирует отметку о франкировании и передает ее в проверочное устройство, которое управляет ходом частичных проверок.

Особенно целесообразно, чтобы одна из частичных проверок включала в себя дешифрование криптографической информации, содержащейся в отметке о франкировании.

Благодаря интеграции дешифрования криптографической информации в процесс проверки можно непосредственно регистрировать подлинность отметок о франкировании, так что проверка может осуществляться в реальном времени, в частности, при обработке почтового отправления в обрабатывающей машине.

Далее, целесообразно, чтобы одна из частичных проверок включала сравнение даты создания отметки о франкировании и текущей даты. Интеграция даты создания почтового отправления, особенно в зашифрованной форме, повышает защищенность данных, так как путем сравнения даты создания отметки о франкировании и текущей даты можно избежать многократного использования одной и той же отметки о франкировании для доставки почтовых отправлений.

Для дальнейшего повышения скорости проверки целесообразно, чтобы считывающее устройство и проверочное устройство обменивались информацией при помощи синхронного протокола обмена данными.

В другом, также целесообразном, варианте выполнения изобретения считывающее устройство и проверочное устройство взаимодействуют друг с другом посредством асинхронного протокола обмена данными.

При этом особенно целесообразно, чтобы считывающее устройство посылало в проверочное устройство сообщение с данными.

Предпочтительно, это сообщение включает в себя содержание отметки о франкировании.

Дальнейшие преимущества, особенности и рациональные усовершенствования изобретения вытекают из зависимых пунктов формулы изобретения и последующего описания предпочтительных вариантов его осуществления со ссылками на чертежи.

На чертежах показано:

фиг.1 - базовая иллюстрация компонентов системы защиты платежей;

фиг.2 - показан особенно предпочтительный вариант выполнения системы защиты платежей, ручной сканер и персональный компьютер системы защиты платежей;

фиг.3 - иллюстрирует принцип создания и проверки отметок о франкировании;

фиг.4 - компоненты криптографической системы;

фиг.5 - предпочтительный вариант процесса проверки;

фиг.6 - другой, особенно предпочтительный, вариант процесса проверки с особенно предпочтительной последовательностью частичных проверок;

фиг.7 - предпочтительный ход процесса распределения ключей между центральным

пунктом загрузки (пунктом почтовой оплаты) и отдельными криптографическими проверочными устройствами (криптографическими серверами).

В дальнейшем изобретение представлено на примере системы франкирования с использованием персональных компьютеров. Шаги способа, служащие для защиты платежей, при этом независимы от системы, применяемой для создания отметок о франкировании.

Представленная децентрализованная проверка в отдельных инспекционных пунктах, в частности в почтовых центрах, является особенно предпочтительной, однако также возможна централизованная проверка.

В первом варианте выполнения изобретения проверка подлинности отметок о франкировании предпочтительно осуществляется путем случайной выборки при помощи индивидуальных сканеров.

Пригодная для этого проверочная система предпочтительно содержит компоненты, представленные на фиг.1.

На фиг.1 показано, с какими отдельными системами связана криптографическая система. Они кратко описываются ниже.

Сканер

Сканер служит для считывания отметки о компьютерном франкировании. В случае отметки о франкировании речь идет о двухмерном коде в формате матрицы данных с применением коррекции ошибок ECC200. В зависимости от типа сканера данные передаются по радио или по проводу, при этом радиосканеры имеют многострочный дисплей и тем самым возможность вывода информации и сенсорный монитор или клавиатуру для простейшего ввода. Интерфейс между сканерами и остальными устройствами предпочтительной системы защиты платежей компьютерного франкирования образован такими компонентами, как контроллер сканера и контроллер проверки достоверности. В то время как контроллер сканера управляет очередью матричных кодов, которые, поступая через ручной сканер, стоят в очереди на проверку, и по существу обеспечивает контакт со сканерами, он находится в контакте с остальной системой только через контроллер проверки достоверности.

Контроллер сканера/контроллер проверки достоверности

Контроллеры сканера или контроллеры проверки достоверности служат интерфейсом между сканерами и остальными системами для проверки двухмерного штрих-кода. Им передается содержание двухмерного штрих-кода, преобразованное с коррекцией ошибок из оптической записи, затем они инициируют проверку и в случае радиосканера обеспечивают вывод результатов считывания и проверки, а также служат интерфейсом между возможно необходимыми ручными дополнительными операциями и проверками, осуществляемыми контролером, а также другими системами.

Криптографическая система

Криптографическая система обеспечивает проверку содержания и криптографическую проверку двухмерного штрих-кода, а также защищенное хранение данных и алгоритмов, связанных с защитой. Отдельные ее компоненты будут подробнее рассмотрены ниже.

Пункт загрузки сумм платежей (пункт почтовой оплаты)

Пункт загрузки сумм платежей (пункт почтовой оплаты) является центральной системой средств компьютерного франкирования. Он используется в качестве интерфейса с клиентскими системами. Из него клиенты могут выгружать предварительно задаваемые суммы для последующего франкирования почтовых отправлений. В пункте загрузки сумм платежей (пункте почтовой оплаты) генерируются ключи для защиты этого процесса. Кроме того, он служит интерфейсом с биллинговыми системами. Для предпочтительной системы защиты платежей компьютерного франкирования обеспечиваются следующие интерфейсы:

- информация о почтовом отправлении посредством двухмерного штрих-кода,
- симметричные криптографические ключи,
- основные данные, например предварительно задаваемые суммы, остатки на счете.

Предпочтительная центральная система защиты платежей

В предпочтительной центральной системе защиты платежей относящаяся к почтовым отправлениям информация собирается и предоставляется в распоряжение другим системам. Здесь происходит создание отчетов о работе, которые в свою очередь приводят к созданию "черных списков". Кроме того, центральная система защиты платежей получает из пункта загрузки сумм платежей (пункта почтовой оплаты) текущие данные о ключах и передает их далее индивидуальным криптографическим серверам.

Поставщики данных

Для проверки содержания двухмерного штрих-кода необходим ряд основных данных, например "черные списки", минимальные платежи, сроки действительности в отношении продукции, а также коды предупреждений защиты платежей и последующей обработки. Эти данные предоставляются из различных систем (BDE, VIBRIS, локальной системы защиты платежей).

Прикладная программа защиты платежей

С помощью прикладной программы защиты платежей контролер AGB (контролёр, проверяющий соблюдение условий коммерческих сделок), который должен окончательно обрабатывать изъятые отправления с компьютерным франкированием, имеет возможность предпринять более детальную проверку франкирования, в которой представление результатов проверки не сводится к ограниченным возможностям выходных данных сканера. Дополнительно контролёр может распознать также и другие данные, например срок действительности суммы почтового сбора для текущего отправления, а также сумму и использованное франкирование.

Автоматическая регистрация двухмерного штрих-кода

Автоматическая регистрация двухмерного штрих-кода осуществляется внутри SSA. Для этого графическая информация передается на считыватель двухмерного AFM-кода. Он осуществляет преобразование изображения в содержание матричного кода. Вслед за этим содержание двухмерного штрих-кода передается для проверки в криптографическую систему, возвращаемый результат проверки анализируется и передается в оптическую систему регистрации (IMM) для кодирования почтового отправления. Предпочтительные части расширенного таким образом процесса проверки представлены на фиг.2.

Считыватель двухмерного AFM-кода

В считывающей машине (ALM/ILVM) имеется считыватель двухмерного AFM-кода, который через оптическую систему регистрации (IMM) получает графические данные почтового отправления и обрабатывает их далее с целью защиты платежей. В рамках предпочтительной системы защиты платежей компьютерного франкирования это означает, что в случае распознавания двухмерного кода из графических данных извлекается двухмерный матричный код, который с использованием способа коррекции ошибок ECC200 преобразуется в цепочку байтов, которая представляет содержание двухмерного штрих-кода.

Эта цепочка байтов передается для проверки в контроллер проверки достоверности. Результат проверки затем передается через интерфейс в оптическую систему регистрации и используется там для кодирования.

Криптографическая система для считывателя двухмерного AFM-кода

В зависимости от свойств криптографических карт можно производить, например, около 27 проверок в секунду. Так как скорость считывающих машин составляет примерно 10 считываемых почтовых отправлений в секунду, то нет смысла объединять каждый считыватель двухмерного AFM-кода с одной криптографической системой. Не следует также исходить из того, что отправления с компьютерным франкированием одновременно обрабатываются на всех ста процентах машин. Поэтому оказывается целесообразным отделить криптографические системы, чтобы несколько считывателей системы компьютерного франкирования работали с одной криптографической системой. При этом нужно выбрать такое "масштабируемое" решение, которое также дает возможность обеспечить наличие нескольких криптографических систем в одном почтовом центре. Это касается, например, почтовых центров с большим количеством отправлений и большим

количеством считывающих машин, где изначально может быть предусмотрена вторая криптографическая система. Кроме того, позднее при эксплуатации количество серверов при соответствующей потребности может быть увеличено.

С целью упрощения архитектура должна быть выбрана предпочтительно так, чтобы отдельные считывающие машины были постоянно связаны с одной криптографической системой и чтобы она также могла быть расширена дополнительной резервной конфигурацией, которая в случае ошибок попыталась бы переключиться на другую криптографическую систему.

Преимущество, которое достигается при разделении криптографической системы и считывателя двухмерного AFM-кода, состоит также и в том, что машинное считывание и проверка с помощью ручного сканера могут осуществляться с использованием одной и той же криптографической системы и поэтому одна и та же функция не должна реализовываться дважды, что дополнительно дает существенные преимущества при осуществлении изобретения.

Предпочтительные операции способа снабжения почтового отправления цифровой отметкой о франкировании после загрузки суммы платежа из центрального пункта загрузки (пункта почтовой оплаты) и создания отметки о франкировании при помощи локального персонального компьютера, а также последующая доставка почтового отправления и проверка нанесенной на него отметки о франкировании представлены на фиг.3.

Независимо от распределения ключей процесс осуществляется так, что клиент вначале загружает некоторую сумму, предназначенную для почтовой оплаты, в свой персональный компьютер. Для идентификации запроса при этом генерируется случайное число. В пункте загрузки сумм платежей (пункте почтовой оплаты) создается новая сумма почтовой оплаты для соответствующего клиента и из переданного случайного числа и дополнительной информации, обеспечивающей идентификацию клиентской системы (данные для идентификации клиентской системы, в дальнейшем называемые почтовым идентификатором) и суммы почтовой оплаты, создается так называемая криптографическая строка, которая кодируется одним секретным симметричным ключом, имеющимся в пункте загрузки сумм платежей (пункте почтовой оплаты).

Эта криптографическая строка и соответствующая сумма почтовой оплаты затем передаются в персональный компьютер клиента и вместе со случайным числом заносятся в его "сейф", защищенный от несанкционированного доступа.

Если почтовое отправление франкируется клиентом посредством принятой в ходе этого процесса суммы почтовой оплаты, то включаемые в двухмерный штрих-код данные о почтовом отправлении, в том числе криптографическая строка, дата франкирования и сумма франкирования, дополненные случайным числом, и почтовый идентификатор собираются в незашифрованной форме и вырабатывается хэш-значение, которое однозначно идентифицирует это содержимое.

Так как случайное число имеется в зашифрованной форме внутри криптографической строки, а также в незашифрованной форме внутри хэш-значения, то гарантируется, что данные о почтовом отправлении не могут быть изменены или созданы произвольно и можно определить его отправителя.

Затем относящиеся к почтовому отправлению данные преобразуются в двухмерный штрих-код, который при помощи печатающего устройства клиента печатается на почтовом отправлении как соответствующая отметка о франкировании. После этого готовое почтовое отправление может быть передано для отсылки по почте.

В особенно предпочтительном варианте обеспечения защиты платежей двухмерный штрих-код считывается в почтовом центре считывателем двухмерного AFM-кода или ручным сканером, а затем проверяется. Связанные с этим операции способа обозначены на схеме цифрами 5-8. Для проверки корректности двухмерного штрих-кода считыватель двухмерного AFM-кода передает все данные о почтовом отправлении в криптографическую систему, где содержащаяся в данных криптографическая информация, в частности криптографическая строка, дешифруется, чтобы определить случайное число,

использованное при создании хэш-значения.

Затем определяется хэш-значение (называемое также дайджестом сообщения) для данных о почтовом отправлении, включая дешифрованное случайное число, и проверяется, идентичен ли результат хэш-значению, содержащемуся в двухмерном штрих-коде.

Дополнительно к криптографической проверке достоверности осуществляют дальнейшие проверки содержания (шаг 7b), которые, например, предотвращают двойное использование одного двухмерного штрих-кода, или проверяют, не был ли клиент замечен в попытке обмана и вследствие этого занесен в "черный список".

После этого соответствующий результат проверки передается в считыватель системы компьютерного франкирования, который передает результат в оптическую систему регистрации (IMM) для кодирования штрих-кода. Затем этот штрих-код печатается на письме, а при отрицательном результате проверки почтовые отправления изымаются.

Архитектура криптографической системы

Обзор компонентов

На фиг.4 представлены отдельные компоненты криптографической системы, где снабженные надписями стрелки представляют входные и выходные потоки данных для внешних систем. Так как предпочтительная центральная система защиты платежей применяется для распределения ключей из пункта загрузки сумм платежей (пункта почтовой оплаты) между криптографическими системами локальных систем защиты платежей и эти данные на промежуточных этапах должны сохраняться, то в ней также должен быть предусмотрен компонент криптографической системы, в котором, однако, контроллер проверки достоверности, как правило, не используется.

Отдельные компоненты криптографической системы описываются в дальнейшем более детально.

Контроллер проверки достоверности

Контроллер проверки достоверности представляет собой интерфейс для проверки всего содержания двухмерного штрих-кода. Проверка двухмерного штрих-кода состоит из проверки его содержания и криптографической проверки. Для этой цели сканер должен передать считанное содержание двухмерного штрих-кода через контроллер сканера в контроллер проверки достоверности.

Так как ответственный за это контроллер проводного сканера и контроллер проверки достоверности находятся в различных компьютерных системах, то между ними должна быть предусмотрена связь на основе протокола TCP/IP; применение основанного на нем протокола вместо чистого программирования сокета является предпочтительным. В рамках криптографической системы здесь речь идет о менеджере сообщений, применяемом при регистрации рабочих параметров (BDE), или о протоколе, применяемом в рамках оптической системы регистрации, например Corba/IIOP.

Контроллер проверки достоверности инициирует отдельные проверочные подпрограммы, которые передают ему обратно свои результаты проверки.

Так как несколько контролёров AGB могут одновременно работать с различными сканерами, контроллер проверки достоверности должен быть выполнен "многосессионным". Это означает, что он должен осуществлять одновременные запросы на проверку и иметь возможность направлять соответствующие выходные данные в нужный сканер. К тому же он должен быть выполнен так, чтобы одновременно выполнять несколько запросов на проверку и выполнять параллельно с этим часть шагов проверки, например проверку хэш-значения и проверку минимального платежа.

К началу сессии контроллеру сообщается, с каким типом сканера он связан, и он получает возможность с помощью метода обратного вызова настраивать подпрограммы для вывода информации и для ручной дополнительной проверки. В зависимости от вида работы и от типа сканера результаты выдаются или на радиосканер, или в систему защиты платежей, а также регистрируются результаты ручной проверки.

Криптографическая карта

Особая проблема состоит в хранении ключа, с помощью которого криптографическая строка в двухмерном штрих-коде должна шифроваться и снова дешифроваться для проверки. Этот ключ обеспечивает защиту двухмерного штрих-кода от подделок, поэтому должна быть исключена возможность его похитить. Поэтому путем специальных мер защиты должно быть обеспечено, чтобы этот ключ никогда не появлялся в виде открытого текста на жестком диске, в памяти или при его передаче и чтобы он был защищен сильным криптографическим способом.

Базирующиеся только на программном обеспечении решения не дают надежной защиты, так как в каком-либо месте в системе ключ все же появляется в виде открытого текста или же ключ может быть считан в виде открытого текста из памяти при помощи отладчика. Эта опасность существует прежде всего потому, что системы могут администрироваться на расстоянии или могут выноситься из помещения с целью ремонта.

К тому же криптографические способы создают высокую нагрузку на процессор системы, который не оптимизирован для таких операций.

Поэтому рекомендуется применение криптографической процессорной карты со следующими особенностями:

- специальный криптографический процессор для ускорения криптографических способов обработки;

- закрытая система типа "черного ящика" для предотвращения доступа к критичным для защиты данным и способам.

Карты, которые обладают этими отличительными признаками, являются замкнутыми системами, которые в зависимости от выполнения соединены с компьютером через шину PCI или ISA и сообщаются с программными средствами компьютера через драйвер.

Наряду с поддерживаемой батареей главной памятью карты имеют также флэш-память, в которой может храниться индивидуальный код прикладной программы. Непосредственный доступ к главной памяти карт из внешних систем невозможен, вследствие чего обеспечивается очень высокая защищенность, так как ни данные о ключах, ни криптографические способы обеспечения защиты не доступны иначе, чем через защищенный драйвер.

Дополнительно карты при помощи собственных датчиков контролируют, не имеют ли место попытки манипуляций (например, в зависимости от выполнения карты скачки температуры, излучение, открытие защитной крышки, скачки напряжения).

Если такая попытка манипуляции имеет место, то поддерживаемое батареями содержимое главной памяти тотчас же стирается и производится отключение карты.

Для криптографического сервера функция дешифрования почтового идентификатора, функция проверки хэш-значения, а также функция импортирования данных о ключах должны быть загружены непосредственно на карту, так как эти подпрограммы очень важны для защиты.

Далее, все криптографические ключи, а также конфигурации сертификатов, которые необходимы для проверки подлинности, также сохраняются в поддерживаемой батареями памяти карты. Если карта не имеет достаточно памяти, то, как правило, на карте имеется мастер-ключ, с помощью которого вышеуказанные данные шифруются и затем могут быть записаны на жесткий диск системы. При этом, однако, перед использованием этой информации данные должны быть снова дешифрованы.

Следующая таблица дает обзор моделей подходящих карт различных производителей и их сертификатов.

Криптографические карты для применения в предпочтительной системе защиты платежей для компьютерного франкирования

Изготовитель	Тип	Сертификация
IBM	4758-023	FIPS PUB 140-1, уровень 3, и ZKA-eCash
IBM	4858-002	FIPS PUB 140-1, уровень 4 и ZKA-eCash (до 07/2000) CCEAL 5 (в настоящее время в фазе сертификации)
Ultimaco	KryptoServer	ITSEC-E2 и ZKA-eCash
Ultimaco	KryptoServer 2000 (приблизительно с 1 квартала 2001)	FIPS PUB 140-1, уровень 3, ITSEC-E2 и ZKA-eCash (осуществляется)

Racal/Zaxus	WebSentry PCI	FIPS PUB 140-1, уровень 4

Наряду с выполнением предъявляемых к карте требований вследствие желаемой сертификации BSI также очень важно, какие сертификаты имеют отдельные модели в настоящее время и какие из них находятся сейчас на стадии проведения сертификации.

Сертификаты изделий при этом разделяются на три категории в соответствии с различными сертификационными учреждениями.

ITSEC является опубликованным Европейской Комиссией нормативным документом для сертификации продукции и систем информационных технологий с учетом их свойств в отношении защиты информации. Оценка степени доверия производится по ступеням от E0 до E6, где E0 обозначает недостаточную, а E6 - наивысшую защиту. Усовершенствованием и гармонизацией с аналогичными международными стандартами являются CC (общие критерии), которые находятся сейчас в процессе стандартизации по ISO (стандарт ISO 15408). Этот регулирующий документ используется для оценки защищенности системы.

В настоящее время изделия из приведенной выше таблицы еще не имеют сертификата по CC. Однако модель IBM 4758-002 находится на стадии такой сертификации.

Стандарт FIPS PUB 140-1 является изданным правительством США нормативным документом для оценки степени защиты коммерческих криптографических устройств. Этот нормативный документ в основном касается свойств аппаратного обеспечения. Оценка осуществляется в соответствии с 4 уровнями, из которых уровень 1 обозначает наименьшую, а уровень 4 - наивысшую защиту.

Дополнительно к упомянутому выше стандарту оценки имеется нормативный документ, который издан Центральной кредитной комиссией (ZKA) и регулирует допуск к эксплуатации систем и продуктов информационных технологий в области электронных платежей.

Наряду с уже упомянутыми свойствами карт и их сертификатами имеется еще ряд предпочтительных возможностей, которые кратко перечислены ниже:

- Возможность изготовления собственного (снабженного цифровой подписью) программного обеспечения и загрузка его на карту.
- Интегрированный генератор случайных чисел (сертифицированный по FIPS PUB 140-1).
- Аппаратная реализация стандартов шифрования данных DES, тройного DES и SHA-1.
- Создание ключа RSA и обработка с использованием секретного/открытого ключей длиной до 2048 бит.
- Функции управления ключами.
- Функции управления сертификатами.
- В определенной степени возможна параллельная эксплуатация нескольких криптографических карт в одной системе.

Криптографический интерфейс

Функции, существенные для защиты в рамках применения криптографической карты, хранятся непосредственно на карте и поэтому доступны извне только через драйвер карты. В качестве интерфейса между драйвером и контроллером проверки достоверности используется компонент криптографического интерфейса, который направляет запросы подпрограмм проверки через драйвер в карту.

Так как внутри одного компьютера может применяться несколько карт, то задача криптографического интерфейса состоит также и в том, чтобы производить распределение загрузки от отдельных запросов на проведение проверки. Эта функция целесообразна в особенности тогда, когда проверочные подпрограммы криптографической системы используются дополнительно еще одним или в зависимости от почтового центра несколькими считывателями двухмерного AFM-кода.

Другая задача состоит в управлении передачей информации с целью распределения ключей. На уровне 2 может использоваться только простейший механизм передачи ключа, зашифрованного с целью защиты, внутри подписанного файла. Требование к криптографическому интерфейсу в этом случае состоит в том, чтобы предоставить

утилиту, которая дает возможность импорта такого файла.

Функции криптографической системы

Ход проверки в контроллере проверки достоверности

Для проверки двухмерного штрих-кода контроллер проверки достоверности обеспечивает главную проверочную функцию в качестве интерфейса к сканеру или считывающей системе. Эта проверочная функция координирует ход частичных проверок (отдельных компонентов проверки).

Передаваемые из подпрограмм частичных проверок коды событий, касающихся защиты платежей, преобразуются в соответствующий код защиты платежей на основании предварительно заданной таблицы, которая предпочтительно хранится централизованно и передается в криптографическую систему. Внутри этой таблицы дополнительно устанавливаются приоритеты, которые определяют, какой код назначается, если зарегистрировано несколько событий защиты платежей.

Этот код защиты платежей затем отправляется обратно в качестве результата проверки, вместе с поясняющим текстом. В зависимости от системы, осуществляющей дальнейшую обработку вне криптографической системы, этот результат затем выводится на радиосканер или выдается внутри прикладной программы защиты платежей, или при автоматической проверке преобразуется в код TIT2 и печатается на почтовом отправлении.

Так как ход процесса в системах с ручным сканером и автоматических считывающих системах различен, то для этих случаев реализованы различные функции.

В зависимости от того, какой механизм связи между считывающей системой и контроллером проверки достоверности применяется, вызов функции и возврат результатов различаются. В случае применения синхронного протокола, основанного на RPC (удаленном вызове процедуры), такого как Corba/IIOP, проверочные функции вызываются непосредственно, а результаты проверки передаются после их завершения. Клиент, т.е. контроллер сканера или считывающая система, в этом случае ожидают выполнения проверки и возврата ее результатов. Поэтому в последнем случае у клиента должен быть предусмотрен пул потоков, который может проводить параллельную проверку для нескольких запросов.

При асинхронном механизме с использованием TGM проверочный метод не вызывается непосредственно контроллером сканера или считывающей системой, а в криптографическую систему посылается сообщение, которое содержит запрос на проведение проверки, содержимое двухмерного штрих-кода и дополнительную информацию, например, о текущей программе сортировки. При поступлении этого сообщения в криптографическую систему вызывается и выполняется проверочная функция, а результаты считывания и проверки возвращаются обратно в виде нового сообщения. Преимущество этого способа состоит в том, что в системе, делающей запрос, процесс не останавливается вплоть до получения результата.

Проверка для системы с ручным сканером

Проверочная подпрограмма для системы с ручным сканером ожидает в качестве входных параметров идентификатор сессии, а также содержание двухмерного штрих-кода.

В качестве дополнительного параметра ожидается также идентификатор сортировочной программы. Последний упомянутый параметр служит для определения минимального платежа.

На фиг.5 представлен ход проверки в контроллере проверки достоверности для случая, когда проверка инициирована системой с ручным сканером. При этом имеется в виду проверка с помощью радиосканера с последующим сравнением адреса с содержимым двухмерного штрих-кода "вручную". В случае использования сканера с проводным подключением в системе защиты платежей или в прикладной программе защиты платежей картина была бы аналогичной.

Предпочтительный ход проверки с использованием радиосканера, контроллера сканера и проверочного устройства (контроллера проверки достоверности) представлен на фиг.5.

Проверочное устройство в представленном особенно предпочтительном варианте

выполнения изобретения управляет последовательностью частичных проверок, где первая частичная проверка включает считывание матричного кода, содержащегося в цифровой отметке о франкировании. Считанный матричный код прежде всего передается из радиосканера в контроллер сканера. Затем в зоне контроллера сканера осуществляется проверка матричного кода, а также его передача в проверочное устройство. Проверочное устройство управляет разделением содержания кода. Результат считывания передается затем в регистрирующее устройство, в представленном случае - в радиосканер. Благодаря этому пользователь считывающего устройства узнает, например, что отметку о франкировании можно прочитать и при этом можно распознать информацию, содержащуюся в матрице. Затем проверочное устройство дешифрует криптографическую строку, содержащуюся в матричном коде. При этом, предпочтительно, вначале проверяется версия ключа, предположительно примененного для создания отметки о франкировании. Затем проверяется хэш-значение, содержащееся в криптографической строке.

Далее осуществляется проверка предусмотренного минимального платежа.

Кроме того, проверяется идентификационный номер (почтовый идентификатор) клиентской системы, управлявшей созданием отметки о франкировании.

Затем осуществляется сравнение идентификационного номера с "черным списком".

Путем выполнения этих шагов проверки в такой особенно простой и рациональной форме можно простым способом обнаружить неправомочно созданные отметки о франкировании.

Результат проверки передается в виде цифрового сообщения, которое может, например, передаваться в исходный радиосканер. Благодаря этому пользователь радиосканера может, например, изъять отправление из потока почтовых отправлений. Разумеется, равным образом можно изъять отправление из нормального процесса обработки почтовых отправлений при автоматизированном осуществлении этого варианта способа.

Предпочтительно, результат проверки протоколируется в зоне проверочного устройства.

В качестве возвращаемого значения должны возвращаться код события защиты платежей и соответствующее ему текстовое сообщение, а также объект двухмерного штрих-кода.

Ход проверки для считывателя двухмерного AFM-кода

В качестве входного параметра проверочная подпрограмма для считывателя двухмерного AFM-кода также ожидает идентификатор сессии, а также содержание двухмерного штрих-кода и уникальный идентификатор активной в данный момент сортирующей программы.

На фиг.6 показан ход проверки в контроллере проверки достоверности для случая, когда проверка инициирована считывающей системой.

Для пояснения процесса также показаны оптическая регистрирующая система (IMM-система) и считыватель двухмерного AFM-кода, чтобы представить общую картину проверки. Однако участие криптографической системы ограничивается проверкой хода процесса от получения двухмерного штрих-кода до возврата результата, а также протоколированием результата.

В случае интерфейса с менеджером сообщений в контроллере проверки достоверности могут быть запущены несколько сервисных задач, которые ожидают сообщения с запросами на проведение проверки, а содержание сообщений может быть использовано для вызова проверочных подпрограмм. Происходит ожидание результата работы проверочной подпрограммы, упаковка его в сообщение и отправка обратно клиенту, который дал запрос.

На фиг.6 представлен еще один предпочтительный вариант управления ходом частичных проверок при помощи проверочного устройства (контроллера проверки достоверности). В этом варианте выполнения изобретения регистрация отметок о франкировании осуществляется при помощи автоматической оптической системы распознавания (Prima/IMM). Данные из оптического проверочного устройства поступают в

считывающее и регистрирующее устройство (считыватель двухмерного AFM-кода).

В представленном на фиг.6 варианте осуществления способа проверки действительности цифровых отметок о франкировании считывание цифровых отметок о франкировании осуществляется предпочтительно еще более автоматизированным путем, например путем оптической записи изображения того участка на почтовом отправлении, где преимущественно бывает расположена отметка о франкировании. Дальнейшие шаги проверки осуществляются по существу в соответствии с ходом проверки, представленном на фиг.5.

Возвращаемое проверочной подпрограммой значение содержит, прежде всего, код защиты платежей и соответствующее сообщение, а также преобразованное содержание, дополненное почтовым идентификатором. Из этих возвращаемых значений создается сообщение, которое передается в считывающую систему, выдавшую запрос.

Проверки содержания

Разделение и преобразование содержания двухмерного штрих-кода

Входные данные: сканированный двухмерный штрих-код

Описание

С помощью этой функции содержание двухмерного штрих-кода, состоящее из 80 байтов, должно быть разделено и преобразовано в структурированный объект, называемый в дальнейшем объектом двухмерного штрих-кода, чтобы обеспечить возможность лучшего его отображения, а также более эффективной дополнительной обработки. Отдельные поля и преобразования описаны в нижеследующей таблице.

При преобразовании двоичных чисел в десятичные следует обратить внимание на то, что левый байт последовательности байтов является старшим байтом. Если преобразование не может быть осуществлено, возможно вследствие конфликта типов или из-за потери данных, то должно быть создано сообщение о событии защиты платежей "Штрих-код компьютерного франкирования не читается", которое передается обратно в контроллер проверки достоверности. Дальнейшая проверка содержания или криптографическая проверка в этом случае не имеют смысла.

Поле	Тип	Преобразуется в	Описание
Почтовое предприятие	Код ASCII (3 байта)		Преобразование не требуется
Тип франкирования	Двоичное (1 байт)	Короткое целое	
Обозначение версии	Двоичное (1 байт)	Короткое целое	Номер версии способа
Номер ключа	Двоичное (1 байт)	Короткое целое	Тип ключа
Криптографическая строка	Двоичное (32 байта)		Последовательность байтов должна быть принята неизменной, после дешифрования из нее выделяется почтовый идентификатор
Почтовый идентификатор		Текст (16 символов)	Поле заполняется после дешифрования криптографической строки
Текущий номер отправления	Двоичное (3 байта)	Целое	Только положительные числа
Ключ продукции	Двоичное (2 байта)	Целое	Положительные числа, ссылка на соответствующую таблицу ссылок
Оплата	Двоичное (2 байта)	С плавающей точкой	Преобразование в положительное десятичное число, которое можно разделить на сто, указывается в евро
Дата франкирования	Двоичное (3 байта)	Дата	После преобразования в положительное десятичное число дата может быть преобразована в формат ГГГГММДД (год, месяц, день)
Почтовый индекс получателя	Двоичное (3 байта)	2 значения, одно для страны, одно для почтового индекса	После преобразования в положительное десятичное число первые две цифры дают код страны, пять остальных цифр - почтовый индекс
Улица/почтовый ящик	Код ASCII (6 байтов)	Сокращенное название улицы или почтовый ящик	Если первые символы - числа, то закодирован почтовый ящик, иначе - три первые и последние буквы названия улицы с номером дома
Оставшаяся сумма почтового сбора	Двоичное (3 байта)	С плавающей точкой + поле валюты (текст 32 символа)	После преобразования в положительное десятичное число первая цифра дает валюту (1 = евро), следующие четыре цифры - цифры перед запятой и последние две цифры - цифры после запятой
Хэш-значение	Двоичное (20 байтов)		Последовательность байтов должна быть передана неизменной, служит для криптографической проверки достоверности франкирования

Возвращаемое значение: объект двухмерного штрих-кода; код предупреждения 00, если

преобразование успешно, иначе - предупреждение о событии защиты платежей "Штрих-код компьютерного франкирования не читается".

Проверка номера версии

Входные данные: текущий объект двухмерного штрих-кода

Описание:

По первым трем полям может быть определена версия двухмерного штрих-кода. Из нее также становится ясно, является ли он вообще двухмерным штрих-кодом Deutsche Post, а не двухмерным штрих-кодом другого поставщика услуг. Содержание полей следует сравнить со списком действительных значений, предварительно заданных в прикладной программе. Если соответствие не обнаружено, то возвращается предупреждение защиты платежей "Версия компьютерного франкирования". Дальнейшая проверка содержания, а также криптографическая проверка в этом случае не имеют смысла и не должны осуществляться.

Возвращаемое значение: код предупреждения 00, если проверка версии успешна, иначе - код предупреждения о событии защиты платежей "Версия компьютерного франкирования".

Проверка почтового идентификатора

Входные данные: объект двухмерного штрих-кода с зашифрованным почтовым идентификатором

Описание:

Содержащийся в двухмерном штрих-коде почтовый идентификатор защищен при помощи контрольных цифр (контроль циклическим избыточным кодом CRC 16), которые в этой точке должны быть проверены. Если эта проверка не проходит, то в качестве результата должно быть выдано предупреждение защиты платежей "Предполагаемая подделка компьютерного франкирования (почтовый идентификатор)". Для проверки почтового идентификатора требуется предварительное дешифрование криптографической строки.

Возвращаемое значение: код "00" в случае, если проверка успешна, иначе - код предупреждения о событии защиты платежей "Предполагаемая подделка компьютерного франкирования (почтовый идентификатор)".

Проверка превышения времени

Входные данные: объект двухмерного штрих-кода

Описание:

Эта функция служит для автоматической проверки периода времени между франкированием почтового отправления в системе компьютерного франкирования и его обработкой в почтовом центре. Между обеими датами может пройти только определенное количество дней. Количество дней при этом определяется в зависимости от вида продукции и времени ее прохождения плюс один день ожидания.

Конфигурация периода времени хранится предпочтительно в виде срока действия для соответствующей продукции и централизованно устанавливается в рамках одного шаблона обработки. Для каждого ключа продукции (поля двухмерного штрих-кода), возможного в компьютерном франкировании, фиксируется соответствующее количество дней, которые могут пройти между франкированием и обработкой в почтовом центре. В упрощенном способе предварительно конфигурируется только одно значение периода времени, которое относится к стандартным почтовым отправлениям и хранится в системе в качестве константы.

При проверке определяется количество дней между текущей датой проверки при обработке и датой, содержащейся в двухмерном штрих-коде, например от 02.08 до 01.08=1 день. Если вычисленное количество дней больше, чем заданное для продукции значение, то в контроллер проверки достоверности возвращается код защиты платежей, соответствующий предупреждению "Дата компьютерного франкирования (франкирование)", в противном случае - код, который указывает на успешную проверку. Если согласно упрощенному способу всегда производится сравнение со значением

времени для стандартных отправлений, то после выдачи результата проверки должна иметься возможность корректировать этот результат проверки, например, вручную с помощью клавиш на сканере, если текущая продукция допускает более длительный срок передачи.

Следующая проверка превышения времени относится к содержанию почтового идентификатора. Оплаченный в виде заранее заданной суммы почтовый сбор и тем самым также и почтовый идентификатор имеют заранее заданный срок действия, в течение которого отправления должны быть франкированы. В почтовом идентификаторе содержится дата, вплоть до которой сумма почтовой оплаты является действительной. Если дата франкирования на определенное количество дней больше, чем эта дата действительности почтового сбора, то возвращается код предупреждения защиты платежей, относящийся к предупреждению защиты платежей "Дата компьютерного франкирования (почтовый сбор)".

Возвращаемое значение: код "00" в случае, если проверка успешна, иначе - код предупреждения о событии защиты платежей "Дата компьютерного франкирования (франкирование)" или "Дата компьютерного франкирования (почтовый сбор)".

Проверка платежа

Входные данные: объект двухмерного штрих-кода; идентификатор текущей сортирующей программы

Описание:

Эта функция осуществляет проверку платежа, содержащегося в двухмерном штрих-коде, по сравнению с минимальным платежом, который определен для отправлений соответствующей сортирующей программы. В случае сумм речь идет о суммах в евро.

Приведение в соответствие сортирующих программ и минимальных платежей осуществляется через автоматический интерфейс.

Может быть применен упрощенный способ, как и при проверке превышения времени. В этом случае в файле конфигурации прикладной программы определяется постоянный минимальный платеж, который действует для всех отправлений. Поэтому передача идентификатора сортирующей программы не требуется.

При последующей проверке производится сравнение, чтобы определить, не находится ли содержащийся в двухмерном штрих-коде минимальный платеж ниже этой отметки. Если это имеет место, то возвращается код, соответствующий событию защиты платежей "Недоплата компьютерного франкирования", в противном случае - код успешного завершения.

Возвращаемое значение: код "00" в случае, если проверка успешна, иначе - код предупреждения о событии защиты платежей "Недоплата компьютерного франкирования".

Сопоставление с "черным списком"

Входные данные: объект двухмерного штрих-кода с дешифрованным почтовым идентификатором

Описание:

Эта функция проверяет, не содержится ли принадлежащий двухмерному штрих-коду почтовый идентификатор в "черном списке". "Черные списки" служат для того, чтобы изымать из процесса доставки почтовые отправления от клиентов, которые были замечены в попытках неправомерного использования системы или персональные компьютеры которых были похищены.

"Черные списки" при этом формируются централизованно в рамках проекта Банка данных франкирования. В рамках интерфейса для этого проекта должен быть определен способ обмена данными для децентрализованных систем почтовых центров.

Если прикладной программы формирования "черного списка" или обмена данными еще не существует, то необходимо создать переходный механизм. Формирование этих данных может осуществляться как переходная часть в виде листа Excel, из которого генерируется csv-файл. Этот файл должен пересылаться по электронной почте контролерам AGB и вводиться ими в системы посредством механизма импорта, который

должен быть предусмотрен. Позднее осуществляется передача данных по пути, определенному в предпочтительной концепции информационной технологии защиты платежей.

Почтовый идентификатор характеризует индивидуальную предварительно задаваемую сумму, которую клиент извлекает из системы (из пункта почтовой оплаты). Эти суммы сохраняются в так называемом "сейфе" в клиентской системе. Речь идет о компоненте аппаратного обеспечения в форме смарт-карты вместе со считывающим устройством или в форме защитной заглушки. В "сейфе" предварительно заданные суммы надежно сохраняются и клиент может извлечь из него отдельные суммы для франкирования, не нуждаясь в онлайновом соединении с пунктом загрузки сумм платежей (пунктом почтовой оплаты).

Каждый сейф обозначается уникальным идентификатором. Этот идентификатор сейфа вносится в "черный список", если соответствующие почтовые отправления должны быть изъяты вследствие подозрения в неправомерном использовании компьютерного франкирования. Идентификатор сейфа состоит из нескольких полей. Наряду с уникальным ключом в идентификаторе сейфа содержатся также другие поля, такие как дата действительности и контрольные цифры. Для однозначной идентификации сейфа являются решающими первые три поля идентификатора сейфа. Они также находятся в первых трех полях почтового идентификатора, вследствие чего может устанавливаться соответствие между сейфом и предварительно заданной суммой. Поля описаны в следующей таблице:

Номер байта	Длина	Значение	Содержание данных	Комментарий
b1	1	Обозначение поставщика	00	Не используется
			01	Тестовый поставщик: почтовая фирма
			FF	Ящик пункта почтовой оплаты почтовой фирмы
b2	1	Допустимый номер модели	XX	Заполняется для каждого изготовителя, начиная с 01 (первая заявленная модель), с возрастанием для каждой новой допустимой модели
b3, b4, b5	3	Серийный номер модели	XX XX XX	Заполняется для каждой допустимой модели каждого изготовителя с возрастанием от 00 00 01 до FF FF FF.

Если первые три поля почтового идентификатора текущего проверяемого франкирования идентичны первым трем полям идентификатора "сейфа", содержащегося в "черном списке", то возвращается назначенное клиенту внутри "черного списка" событие защиты платежей, в противном случае - код успешного завершения.

Возвращаемое значение: код "00" в случае, если проверка успешна, иначе - код предупреждения, назначенный клиенту или сейфу в "черном списке".

Сравнение содержания двухмерного штрих-кода с открытым текстом почтового отправления

Входные данные: объект двухмерного штрих-кода

Описание:

Чтобы предотвратить возможность использования копий двухмерного штрих-кода, производится сравнение кодированных в двухмерном штрих-коде данных об отправлении и данных, приведенных на письме в виде открытого текста. Это сравнение можно выполнять непосредственно на радиосканерах, так как на них имеются достаточные возможности для показа изображения и ввода данных. В случае ручных сканеров с проводным подключением проверка должна производиться на персональном компьютере (системы защиты платежей).

Процесс заключается в том, что контроллер проверки достоверности после прохождения автоматизированных проверок инициирует выдачу данных двухмерного штрих-кода в радиосканер или в персональный компьютер системы защиты платежей. Для этого у него в распоряжении имеется метод обратного вызова, назначаемый в начале сессии.

Контроллер осуществляет его вызов для текущего объекта двухмерного штрих-кода. После этого контроллер сканера или персональный компьютер системы защиты платежей обеспечивают отображение содержания двухмерного штрих-кода и выдают в качестве

возвращаемого значения (после обработки контролером) "00" или соответствующий код ошибки.

При успешном анализе возвращается код успешного завершения, в противном случае - предупреждение защиты платежей "Компьютерное франкирование - открытый текст".

При автоматической проверке эта проверка не требуется. В этом случае проверка может осуществляться преимущественно в рамках централизованного анализа в автономном режиме, либо при помощи сравнений оборота, либо путем сравнения целевого почтового индекса с почтовым индексом, содержащимся в двухмерном штрих-коде.

Возвращаемое значение: код "00" в случае, если проверка успешна, иначе - код предупреждения о событии защиты платежей "Компьютерное франкирование - открытый текст"

Криптографические проверки

Криптографическая проверка состоит из двух частей:

а) дешифрование криптографической строки и

б) сравнение хэш-значений.

Обе части проверки должны проводиться в защищенной области криптографической карты, так как клиент путем похищения информации, создаваемой в процессе обработки, смог бы создавать действительные хэш-значения для франкирования.

Дешифрование криптографической строки

Входные данные: объект двухмерного штрих-кода

Описание:

В качестве входного параметра эта функция получает разделенный объект двухмерного штрих-кода, полученного в результате сканирования. При помощи даты франкирования и номера ключа отыскивается действительный для этого момента времени симметричный ключ и криптографическая строка переданного объекта дешифруется с помощью этого ключа по методу тройного DES в режиме CBC. Каким должен быть вектор инициализации, внутренний или внешний режим CBC и какую длину блока использовать, решается в рамках интерфейса с системой защиты платежей.

Если ключ, содержащийся в двухмерном штрих-коде, в криптографической системе отсутствует, то возвращается предупреждение защиты платежей "Предполагаемая подделка компьютерного франкирования (ключ)" с сообщением об ошибке, указывающим, что ключ с данным номером не найден.

Результат операции состоит из дешифрованного почтового идентификатора, а также дешифрованного случайного числа. Дешифрованный почтовый идентификатор вносится в соответствующее поле объекта двухмерного штрих-кода. Случайное число из соображений защиты не должно стать известным, так как клиент при обладании этой информацией смог бы создавать действительные хэш-значения и тем самым подделывать двухмерные штрих-коды.

После дешифрования метод вызывает функцию вычисления хэш-значения и возвращает значение, возвращаемое этой функцией.

Вычисление хэш-значения

Входные данные: объект двухмерного штрих-кода; дешифрованное случайное число из криптографической строки (дешифрованное случайное число не должно быть известно вне карты)

Описание:

Функция вычисления хэш-значения определяет первые 60 байтов из исходного результата сканирования, содержащегося в объекте двухмерного штрих-кода. К ним добавляются дешифрованный почтовый идентификатор, а также переданное дешифрованное случайное число. Из этого согласно способу SHA-1 вычисляется хэш-значение, которое сравнивается с хэш-значением, содержащимся в объекте двухмерного штрих-кода. Если все 20 байтов совпадают, то криптографическая проверка является успешной и возвращается соответствующее возвращаемое значение.

При несоответствии в контроллер проверки достоверности возвращается

предупреждение защиты платежей "Предполагаемая подделка компьютерного франкирования (хэш-значение)".

В качестве возвращаемого значения дополнительно передается также вычисленное хэш-значение, чтобы оно могло быть выведено вместе с результатом проверки.

Возвращаемое значение: вычисленное хэш-значение; код "00" в случае, если проверка успешна, в противном случае - код предупреждения о событии защиты платежей "Предполагаемая подделка компьютерного франкирования (хэш-значение)" или "Предполагаемая подделка компьютерного франкирования (ключ)".

Вывод результата

Представление результата проверки и считывания

Описание:

Контроллер проверки достоверности имеет возможность с помощью метода обратного вызова управлять выдачей результата в устройство вывода, связанное с текущей проверкой. Для этого он передает этому методу обратного вызова объект двухмерного штрих-кода и определенный код предупреждения защиты платежей. В качестве возвращаемого значения может передаваться код метода дополнительной обработки, выбранного контролером AGB.

Метод обратного вызова для вывода результатов предоставляется при регистрации в контроллере проверки достоверности также в начале сессии.

Протоколирование результатов

Входные данные: объект двухмерного штрих-кода, код результата проверки

Описание:

Протоколирование результата согласно упрощенному способу осуществляется в файле в той системе, в которой работает контроллер проверки достоверности. Как правило, результаты или наборы указаний передаются непосредственно в BDE и через предпочтительный интерфейс защиты платежей BDE записываются в банк данных предпочтительной локальной системы защиты платежей.

Предпочтительно сохраняются почтовый идентификатор, порядковый номер, дата франкирования, почтовый платеж, ключ продукции, почтовый индекс, результирующий код защиты платежей, текст сообщения, длительность проверки, время проверки, идентификатор сканера, вид работы сканера, способ регистрации, а также вид последующей обработки. Все значения выдаются отделенными друг от друга точкой с запятой, в виде одного набора данных для каждого почтового отправления, и могут быть таким образом проанализированы далее, например, в программе Excel.

Если система находится в режиме "начальной регистрации", то в колонку "режим регистрации" должна быть введена буква "e" вместо "n" для последующих регистраций.

Подготовка основных данных

Описание:

Для проверки содержания двухмерного штрих-кода необходим ряд основных данных. Здесь речь идет о:

- "черном списке" для компьютерного франкирования,
- сортирующей программе и минимальных платежах,
- общем минимальном платеже,
- ключе продукции для компьютерного франкирования,
- максимальном времени доставки в зависимости от ключа продукции компьютерного франкирования,
- общем максимальном времени доставки,
- событиях защиты платежей, приоритетах и соответствиях инструкциям по последующей обработке,
- инструкциях по последующей обработке.

Основные данные могут быть заранее сконфигурированы в переходный период за исключением "черного списка" компьютерного франкирования, а также криптографических ключей пункта загрузки сумм платежей (пункта почтовой оплаты).

В случае необходимости для некоторых данных могут быть реализованы простые программы обработки и распределения. В этом случае формирование данных должно осуществляться в виде листа Excel, из которого генерируется scv-файл. Этот файл должен отсылаться по электронной почте контролёру AGB и вводиться им в системы при помощи механизма, который должен быть для этого предусмотрен.

Как правило, данные распределяются в соответствии со способом, описанным в Предпочтительной концепции информационных технологий защиты платежей, или обеспечивается возможность доступа к этим данным.

Соответствующие структуры данных описаны в модели данных Предпочтительной концепции защиты платежей.

Распределение ключей

Симметричные ключи, которые в пункте загрузки сумм платежей (пункте почтовой оплаты) используются для защиты содержания двухмерных штрих-кодов и которые требуются криптографической системе для проверки достоверности, из соображений защиты меняются через регулярные интервалы. При использовании во всех почтовых центрах ключи должны автоматически и надежно передаваться из пунктов почтовой оплаты в криптографические системы.

При этом передача должна осуществляться через предпочтительный сервер защиты платежей, так как пункт загрузки сумм платежей (пункт почтовой оплаты) не должен иметь никакой конфигурации, относящейся к тому, какие существуют предпочтительные локальные системы защиты платежей и криптографические системы для них.

Особенно предпочтительные шаги способа замены ключей представлены на фиг.7. Предпочтительный процесс замены ключей осуществляется между центральным пунктом загрузки (пунктом почтовой оплаты), центральным криптографическим сервером и несколькими локальными криптографическими серверами.

Так как симметричные ключи имеют большое значение для защиты двухмерного штрих-кода от подделок, их замена должна быть защищена при помощи сильной криптографической защиты и полного удостоверения идентичности взаимодействующих сторон.

Конфигурация

Базовая конфигурация/управление ключами криптографического аппаратного обеспечения

Для базового конфигурирования криптографической карты необходимы различные действия. Они должны предприниматься администратором защиты. При этом речь идет примерно о следующих мерах:

- инсталляция интерфейса прикладных программ на карту,
- генерация или инсталляция секретных ключей для защиты программ администрирования и загружаемого программного обеспечения.

В зависимости от выбранного типа карты и ее изготовителя необходимы различные действия.

Предусмотренное для предпочтительной системы защиты платежей и согласованное с прикладными программами базовое конфигурирование криптографической карты включает следующие шаги:

- надежное шифрование и передачу симметричных ключей, например пары RSA-ключей, в карту при одновременном создании сертификата для открытого ключа и выдаче ключа,
- жесткое предварительное конфигурирование сертификата для пункта загрузки сумм платежей (пункта почтовой оплаты) для гарантии того, что подлежащий импортированию ключ выдан пунктом загрузки сумм платежей (пунктом почтовой оплаты).

Базовая конфигурация прикладной программы криптографической системы

Каждый сканер, каждый пользователь и каждая криптографическая карта внутри криптографической системы должны обозначаться уникальным идентификатором. В конечном итоге каждый считыватель двухмерного APM-кода также должен быть обозначен уникальным идентификатором.

Вход в систему/выход из системы

Перед началом сессии с использованием контроллера проверки достоверности должен быть осуществлен вход в систему. Этот вход в систему включает в качестве параметров идентификатор сканера, идентификатор пользователя, а также методы обратного вызова для ручной проверки или выдачи результатов считывания и проверки.

В качестве возвращаемого значения передается идентификатор сессии, который также должен передаваться при последующих вызовах проверок внутри сессии. Для идентификатора сессии в контроллере проверки достоверности запоминается контекст сессии, в котором сохраняются параметры передачи.

Если пользователь во время своей сессии делает изменения в режиме работы, в предварительно заданной продукции или в других параметрах сессии, которые могут конфигурироваться во время работы, то эти изменения фиксируются в предназначенных для этого переменных внутри контекста сессии.

При выходе из системы контекст сессии, как положено, удаляется. Последующие вызовы проверок с этим идентификатором сессии отклоняются.

Администрирование пользователей и паролей должно быть определено в общей концепции администрирования для предпочтительной защиты платежей, которая является составной частью предпочтительной концепции информационной технологии защиты платежей.

Считывающие системы должны быть зарегистрированы в контроллере проверки достоверности перед выполнением запросов на проверку. В качестве параметров должны передаваться идентификатор системы считывания, а также пароль. Возвращаемым значением при успешном запросе также является идентификатор сессии, который должен передаваться при последующих запросах на проверку.

При выключении считывающей системы должен осуществляться соответствующий выход из системы с этим идентификатором сессии.

Прочее

Специальные пользовательские обязанности

В рамках концепции защиты предусмотрены две специальные пользовательские обязанности, которые должны выполняться двумя различными лицами.

Администратор защиты

Обязанности администратора защиты включают в себя:

- создание командных файлов для администрирования криптографической карты,
- подписывание этих командных файлов,
- инициализацию и управление криптографическими картами,
- контроль загружаемого программного обеспечения и соответствующей конфигурации.

Администратор защиты идентифицирует себя секретным ключом для осуществления администрирования карты. Этот ключ хранится на дискете или смарт-карте и должен держаться администратором в строгом секрете.

Только подписанные с помощью этого ключа команды администрирования могут выполняться на криптографической карте. Так как при помощи этого механизма защищены последовательность команд и соответствующие параметры, то выполнение этих команд может быть также делегировано системным администраторам на местах. Администратор защиты для этого должен сделать команды доступными и написать соответствующее руководство.

Другая задача состоит в управлении криптографическими картами, где для каждой карты фиксируются серийный номер, конфигурация и системный номер той системы, в которой она инсталлирована, а также местоположение этой системы. Для резервных криптографических карт также фиксируется, в чьем владении карты находятся.

Вместе с менеджером обеспечения качества он контролирует источники программного обеспечения и соответствующие конфигурации программного обеспечения и дает разрешение на его инсталляцию.

Кроме того, он осуществляет проверку программного обеспечения, инсталлируемого или

инсталлированного на карту или в криптографический сервер, а также запуск и подписывание программного обеспечения карты.

Программное обеспечение карты следует специально проверить, чтобы установить, не может ли в каком-либо месте через интерфейс драйвера быть выдан наружу один из секретных ключей или не были ли предприняты попытки таких манипуляций, как, например, сохранение постоянных заранее заданных ключей или применение ненадежных способов кодирования. Дополнительно к программному обеспечению карты также должно быть проверено программное обеспечение криптографического сервера, связанного с картой.

Идентификация осуществляется точно так же, как у администратора защиты, с помощью секретного ключа. При этом речь идет, однако, о секретном ключе для подписывания программного обеспечения.

Дополнительная защита состоит здесь в том, что для инсталляции программного обеспечения должно быть подписано не только программное обеспечение, но и соответствующая инсталляционная команда. Так как полномочия для этого имеют два различных лица (менеджер обеспечения качества и администратор защиты) и благодаря тому, что соответствующие ключи хранятся в двух различных местах, здесь также обеспечивается высокая степень защиты.

Распределение программного обеспечения осуществляется менеджером обеспечения качества в координации с администратором защиты.

Таким образом, этот особенно предпочтительный вариант выполнения изобретения предусматривает два различных ключа идентификации, благодаря чему защита данных существенно улучшается.

Формула изобретения

1. Способ проверки подлинности цифровой отметки о франкировании, нанесенной на почтовое отправление, включающий дешифрование содержащейся в указанной отметке криптографической информации и ее использование для проверки подлинности этой отметки, отличающийся тем, что проверочное устройство осуществляет считывание двухмерного штрих-кода, содержащегося в отметке о франкировании, разделяет содержимое данных указанного штрих-кода для частичных проверок, осуществляет частичные проверки почтовых отправлений, для чего выделяет в указанном содержимом двухмерного штрих-кода криптографическую строку и дешифрует ее, осуществляют частичную проверку периода времени между временем франкирования почтового отправления в указанном содержимом штрих-кода и датой его частичной проверки, с помощью проверочного устройства осуществляют одновременно частичные проверки разных почтовых отправлений, результаты которых передают в виде цифровых сообщений, при неуспешных результатах частичных проверок почтовые отправления изымают из процесса обработки почтовых отправлений.

2. Способ по п.1, отличающийся тем, что считывающее устройство и проверочное устройство обмениваются информацией с использованием синхронного протокола.

3. Способ по п.2, отличающийся тем, что указанный протокол основан на удаленном вызове процедуры (RPC).

4. Способ по одному из пп.1-3, отличающийся тем, что считывающее устройство и проверочное устройство взаимодействуют друг с другом с использованием асинхронного протокола.

5. Способ по п.4, отличающийся тем, что считывающее устройство посылает в проверочное устройство сообщение с данными.

6. Способ по п.5, отличающийся тем, что указанное сообщение включает в себя содержание отметки о франкировании.

7. Способ по п.5, отличающийся тем, что сообщение с данными содержит запрос на запуск криптографической проверочной подпрограммы.

8. Способ по одному из пп.1-3, отличающийся тем, что при помощи криптографического интерфейса осуществляют распределение загрузки между несколькими проверочными

средствами.

9. Способ по одному из пп.1-3, отличающийся тем, что содержание отметки о франкировании разделяют на отдельные поля.

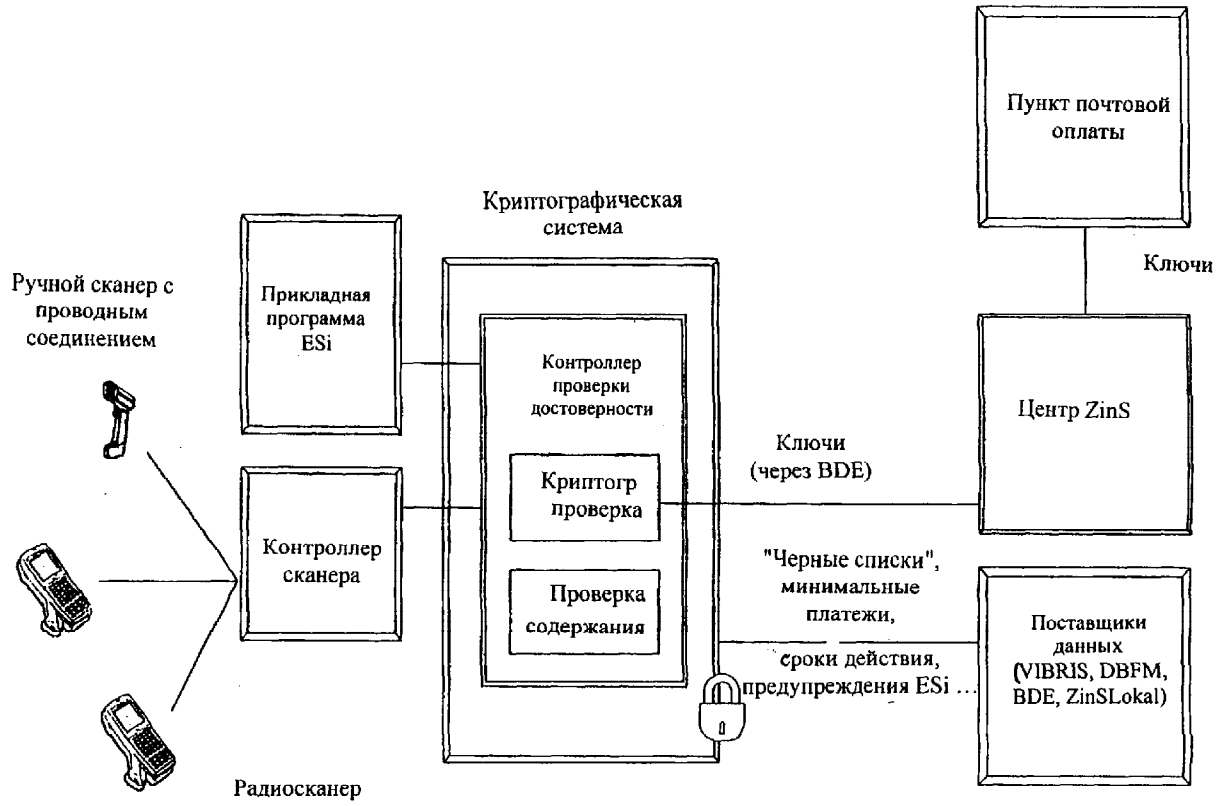
10. Способ по одному из пп.1-3, отличающийся тем, что из отметки о франкировании определяют идентификационный номер (почтовый идентификатор) клиентской системы, управлявшей созданием отметки о франкировании.

11. Способ по одному из пп.1-3, отличающийся тем, что идентификационные данные (почтовые идентификаторы) отдельных клиентских систем регистрируют в "черном списке" и отправления с такими почтовыми идентификаторами изымают из нормального процесса обработки почтовых отправлений.

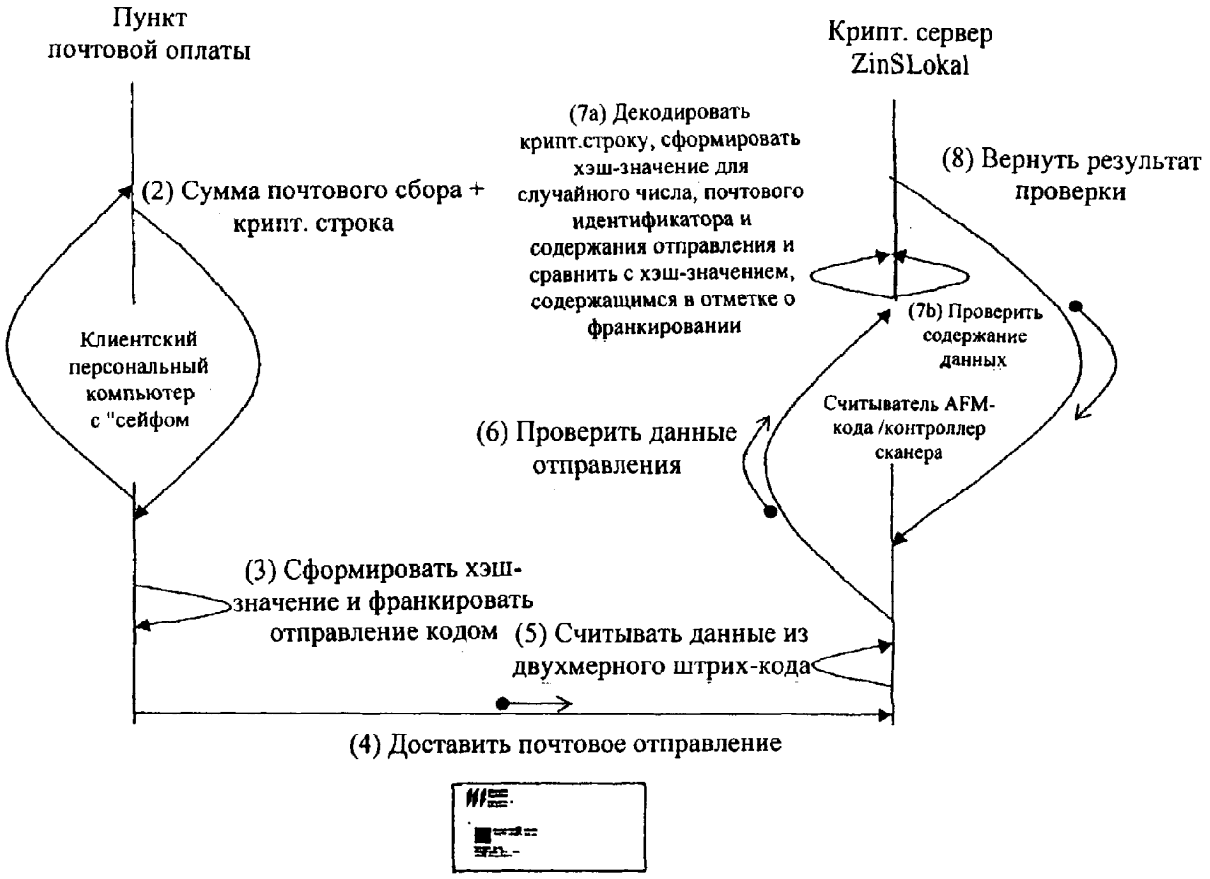
12. Способ по одному из пп.1-3, отличающийся тем, что содержащиеся в отметке о франкировании зашифрованные данные об адресе получателя сравнивают с адресом получателя, указанным для доставки почтового отправления.

13. Способ по одному из пп.1-3, отличающийся тем, что параметры проверки для этого способа можно изменять.

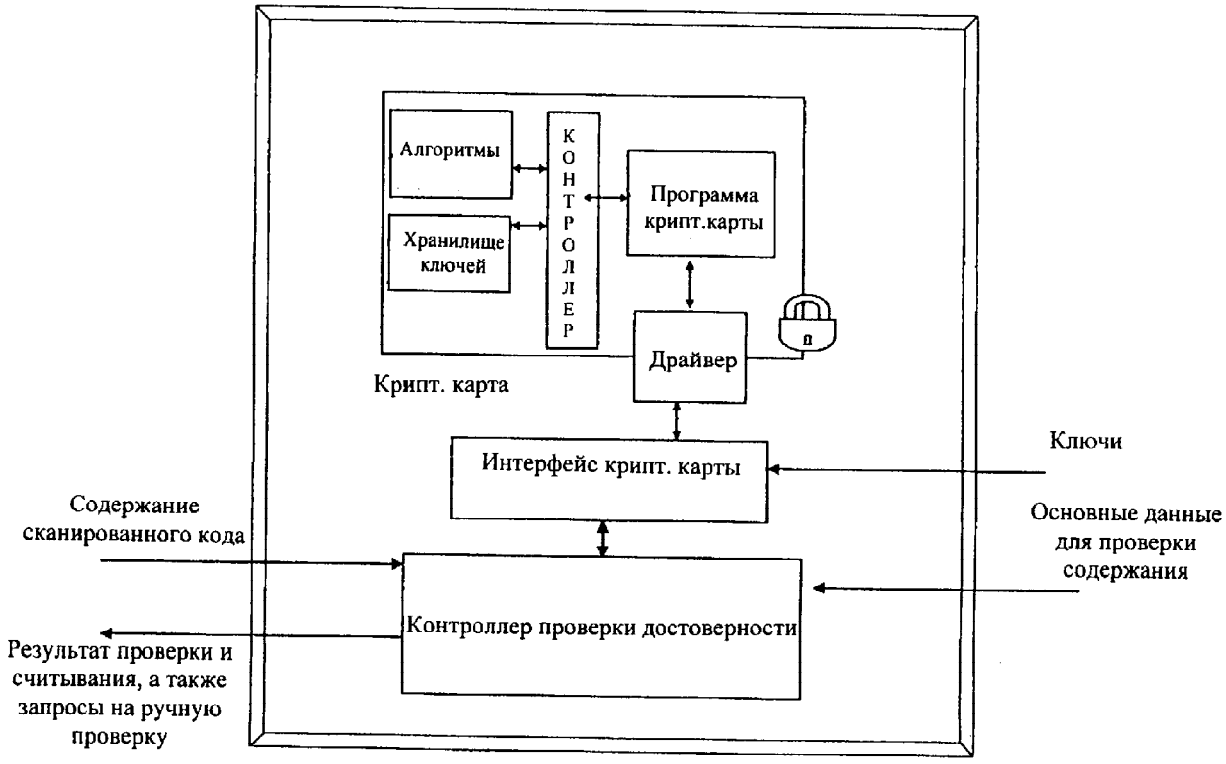
14. Способ по п.13, отличающийся тем, что изменение параметров способа осуществляют только после ввода персонального цифрового ключа (секретного ключа) системного администратора.


Пункт почтовой оплаты
Ключи
Криптографическая система
Ручной сканер с проводным соединением
Прикладная программа ESi
Контроллер проверки достоверности
Криптогр проверка
Проверка содержания
Ключи (через BDE)
Центр ZinS
Контроллер сканера
"Черные списки", минимальные платежи,
сроки действия, предупреждения ESi ...
Поставщики данных (VIBRIS, DBFM, BDE, ZinSLokal)
Радиосканер

Фиг.1


Пункт почтовой оплаты
Крипт. сервер ZinSLokal
(7a) Декодировать крипт.строку, сформировать хэш-значение для случайного числа, почтового идентификатора и содержания отправления и сравнить с хэш-значением, содержащимся в отметке о франкировании
(8) Вернуть результат проверки
(2) Сумма почтового сбора + крипт. строка
(7b) Проверить содержание данных
Клиентский персональный компьютер с "сейфом
Считыватель AFM-кода /контроллер сканера
(6) Проверить данные отправления
(3) Сформировать хэш-значение и франкировать отправление кодом
(5) Считывать данные из двухмерного штрих-кода
(4) Доставить почтовое отправление

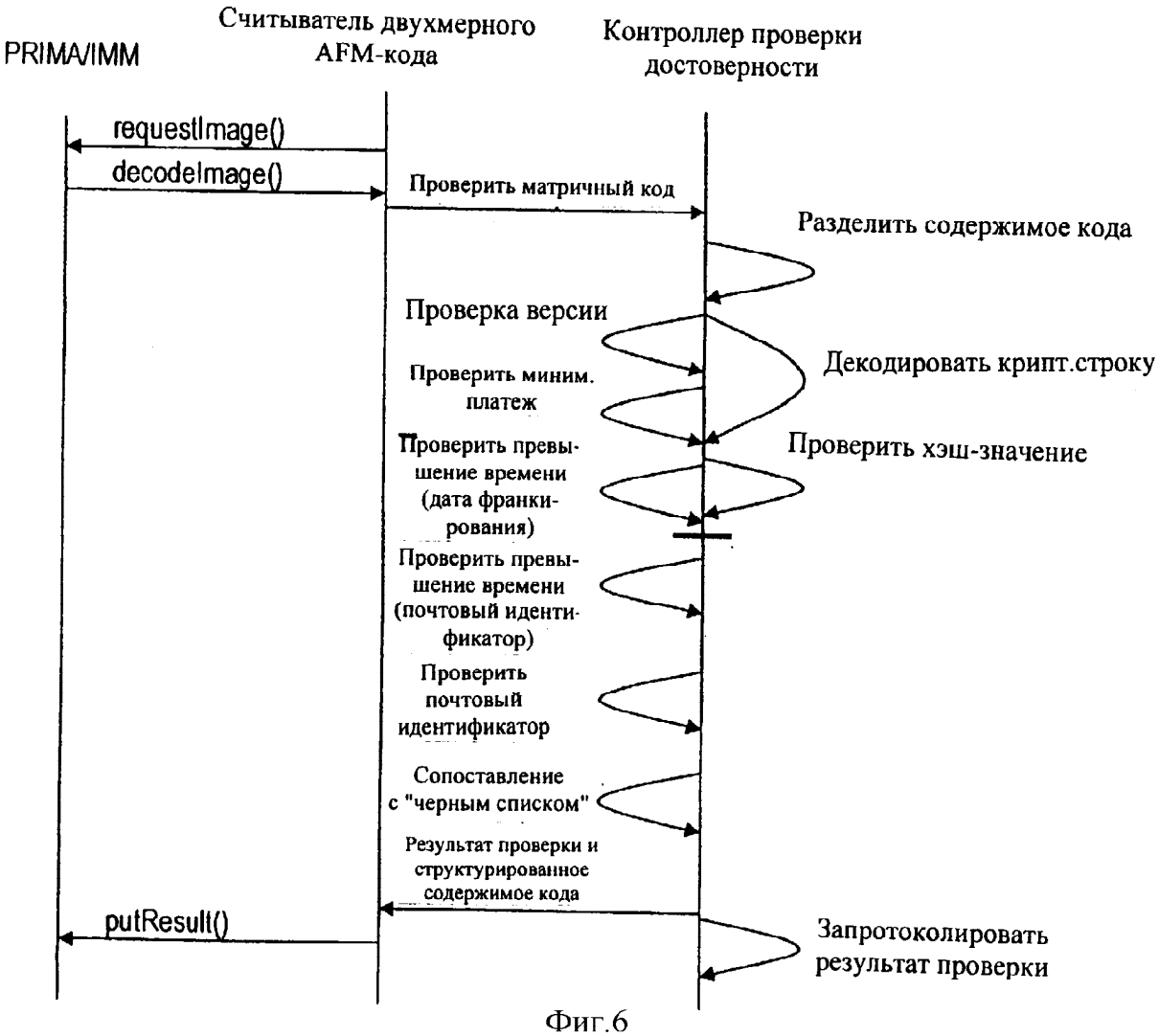
Фиг.3


Алгоритмы
Хранилище ключей
КОНТРОЛЛЕР
Программа крипт.карты
Драйвер
Крипт. карта
Интерфейс крипт. карты
Ключи
Содержание сканированного кода
Основные данные для проверки содержания
Контроллер проверки достоверности
Результат проверки и считывания, а также запросы на ручную проверку

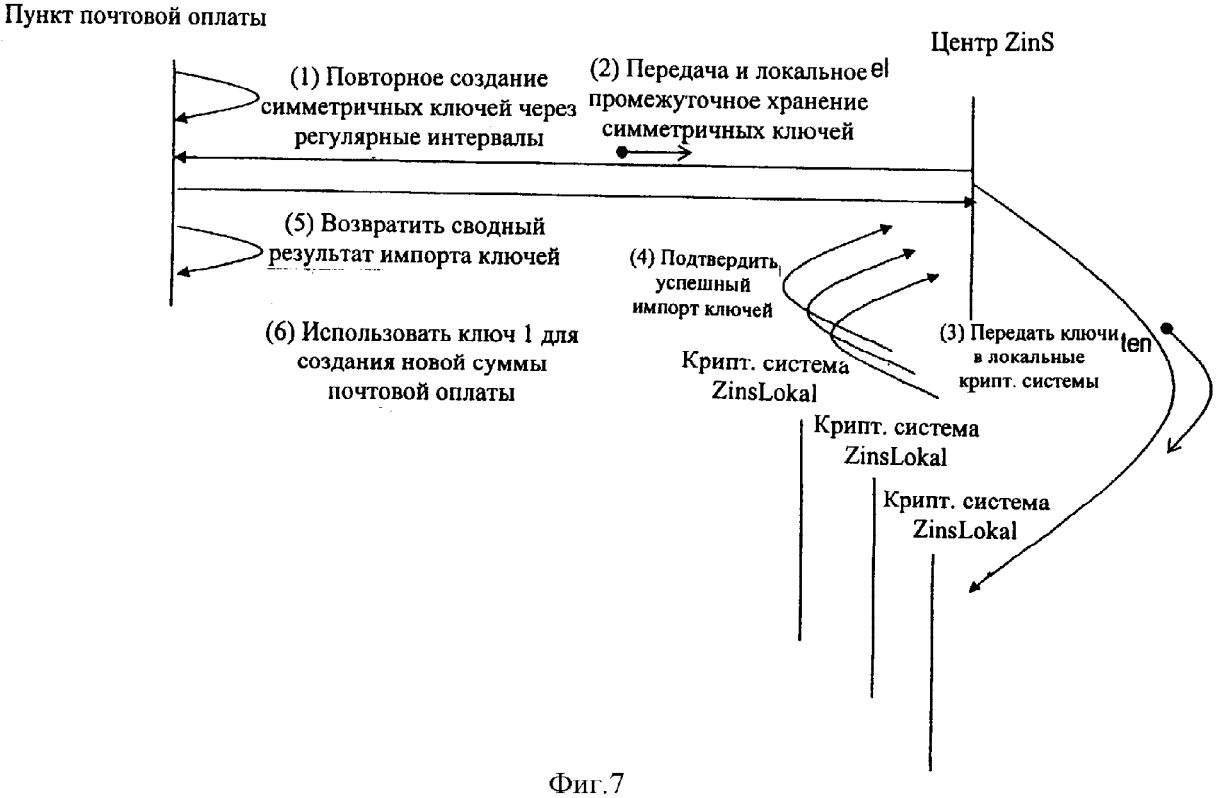
Фиг.4


Радиосканер
Контроллер сканера
Считывать матричный код
Проверить матричный код
Разделить содержимое кода
Показать результат считывания
Показать результат
Проверка версии
Дешифровать крипт.строку
(Проверить минимальный платеж)
Проверить хэш-значение
Проверить почтовый идентификатор
Сопоставление с "черным списком"
Считывать матричный код
Проверить превышение времени
Представить результат проверки
Показать результат
Сравнить матричный код с открытым текстом
Показать релевантное содержимое
(Режим работы 1)
Запротоколировать результат проверки
Вернуть результат сравнения с открытым текстом

Фиг.5


PRIMA/IMM
Считыватель двухмерного AFM-кода
Контроллер проверки достоверности
requestImage()
decodeImage()
Проверить матричный код
Разделить содержимое кода
Проверка версии
Декодировать крипт.строку
Проверить миним. платеж
Проверить превышение времени (дата франкирования)
Проверить хэш-значение
Проверить превышение времени (почтовый идентификатор)
Проверить почтовый идентификатор
Сопоставление с "черным списком"
Результат проверки и структурированное содержимое кода
putResult()
Запротоколировать результат проверки

Фиг.6


Пункт почтовой оплаты
Центр ZinS
(1) Повторное создание симметричных ключей через регулярные интервалы
(2) Передача и локальное el промежуточное хранение симметричных ключей
(5) Возвратить сводный результат импорта ключей
(4) Подтвердить, успешный импорт ключей
(3) Передать ключи ten в локальные крипт. системы
(6) Использовать ключ 1 для создания новой суммы почтовой оплаты
Крипт. система ZinsLokal
Крипт. система ZinsLokal
Крипт. система ZinsLokal

Фиг.7