



**ФЕДЕРАЛЬНАЯ СЛУЖБА
ПО ИНТЕЛЛЕКТУАЛЬНОЙ СОБСТВЕННОСТИ**

(12) ОПИСАНИЕ ИЗОБРЕТЕНИЯ К ПАТЕНТУ

(21)(22) Заявка: 2014132162, 07.01.2013

(24) Дата начала отсчета срока действия патента:
07.01.2013

Дата регистрации:
29.09.2017

Приоритет(ы):

(30) Конвенционный приоритет:
05.01.2012 US 61/583,550;
06.03.2012 US 61/607,546;
21.09.2012 US 61/704,428

(43) Дата публикации заявки: 27.02.2016 Бюл. № 6

(45) Опубликовано: 29.09.2017 Бюл. № 28

(85) Дата начала рассмотрения заявки РСТ на
национальной фазе: 05.08.2014

(86) Заявка РСТ:
US 2013/020580 (07.01.2013)

(87) Публикация заявки РСТ:
WO 2013/103991 (11.07.2013)

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

(72) Автор(ы):

ПАУЭЛЛ Гленн (US),
ШИТС Джон Ф. (US),
ТЭЙТ Пол (US),
ВАГНЕР Ким Р. (US),
КОГАНТИ Кришна Прасад (US),
ПЕРЛ Марк (US),
РОДРИГЕС Эктор (US),
ЗЛОТ Сью (US)

(73) Патентообладатель(и):

ВИЗА ИНТЕРНЭШНЛ СЕРВИС
АССОСИЭЙШН (US)

(56) Список документов, цитированных в отчете
о поиске: US 2004/0182921 A1, 23.09.2004. US
6366682 B1, 02.04.2002. US 2006/0049256 A1,
09.03.2006. US 2010/0318468 A1, 16.12.2010. US
2011/0246315 A1, 06.10.2011. WO 2010/0141501
A2, 09.12.2010.

(54) ЗАЩИТА ДАННЫХ С ПЕРЕВОДОМ

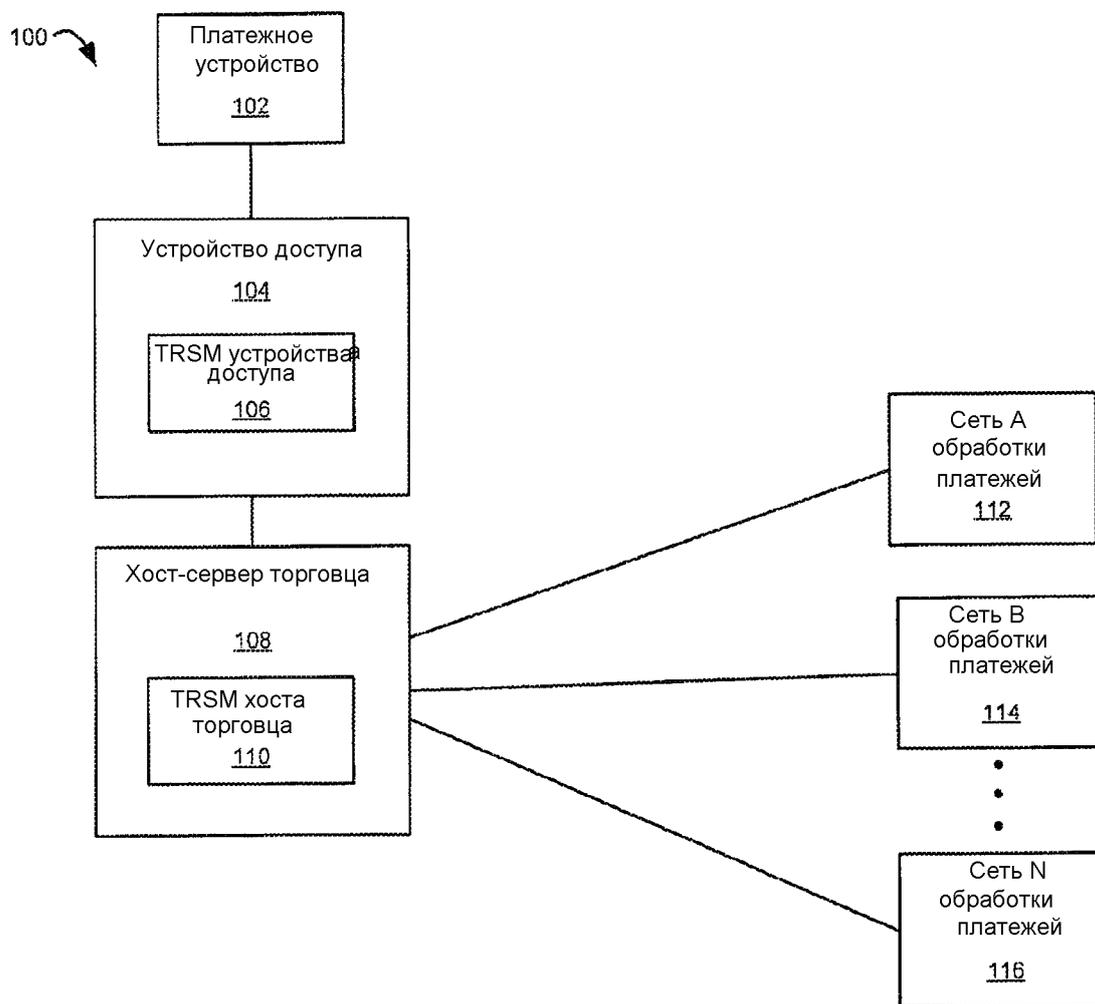
(57) Реферат:

Изобретение относится к области шифрования данных. Технический результат - обеспечивают механизм для передачи и маршрутизации зашифрованного идентификатора/номера счета через сеть обработки без необходимости обновления существующей инфраструктуры маршрутизации для обработки зашифрованных значений, что улучшает безопасность идентификатора/номера счета, так как идентификатор/номер счета может оставаться зашифрованным, пока сообщение запроса авторизации проходит через узлы сети при обработке. Способ защиты данных,

ассоциированных с транзакцией, содержащий этапы, на которых: принимают посредством устройства доступа личный идентификационный номер (PIN) и уязвимые данные, включающие в себя идентификатор счета; шифруют посредством устройства доступа PIN, при этом шифрование PIN использует первый вариант ключа шифрования, основанный на исходном ключе; шифруют посредством устройства доступа уязвимые данные, включающие в себя идентификатор счета, при этом зашифрованный идентификатор счета имеет тот же формат, что и идентификатор счета, и поднабор цифр

зашифрованного идентификатора счета представляет собой зашифрованные цифры идентификатора счета; записывают зашифрованный идентификатор счета в поле сообщения запроса авторизации, причем поле предназначено для приема идентификатора счета; используют элемент данных сообщения запроса

авторизации в качестве сигнала для идентификации наличия зашифрованного идентификатора счета в сообщении запроса авторизации; и передают хост-серверу сообщение запроса авторизации, включающее в себя зашифрованный PIN и зашифрованные уязвимые данные. 5 н. и 27 з.п. ф-лы, 9 ил.



ФИГ.1

RU 2631983 C2

RU 2631983 C2



FEDERAL SERVICE
FOR INTELLECTUAL PROPERTY

(51) Int. Cl.
G06Q 20/38 (2012.01)
G06F 21/60 (2013.01)

(12) ABSTRACT OF INVENTION

(21)(22) Application: **2014132162, 07.01.2013**

(24) Effective date for property rights:
07.01.2013

Registration date:
29.09.2017

Priority:

(30) Convention priority:
05.01.2012 US 61/583,550;
06.03.2012 US 61/607,546;
21.09.2012 US 61/704,428

(43) Application published: **27.02.2016** Bull. № 6

(45) Date of publication: **29.09.2017** Bull. № 28

(85) Commencement of national phase: **05.08.2014**

(86) PCT application:
US 2013/020580 (07.01.2013)

(87) PCT publication:
WO 2013/103991 (11.07.2013)

Mail address:
129090, Moskva, ul. B. Spasskaya, 25, stroenie 3,
OOO "Yuridicheskaya firma Gorodisskij i Partnery"

(72) Inventor(s):

PAUELL Glenn (US),
SHITS Dzhon F. (US),
TEJT Pol (US),
VAGNER Kim R. (US),
KOGANTI Krishna Prasad (US),
PERL Mark (US),
RODRIGES Ektor (US),
ZLOT Syu (US)

(73) Proprietor(s):

VIZA INTERNESHNL SERVIS
ASSOSIEJSHN (US)

(54) DATA PROTECTION WITH TRANSLATION

(57) Abstract:

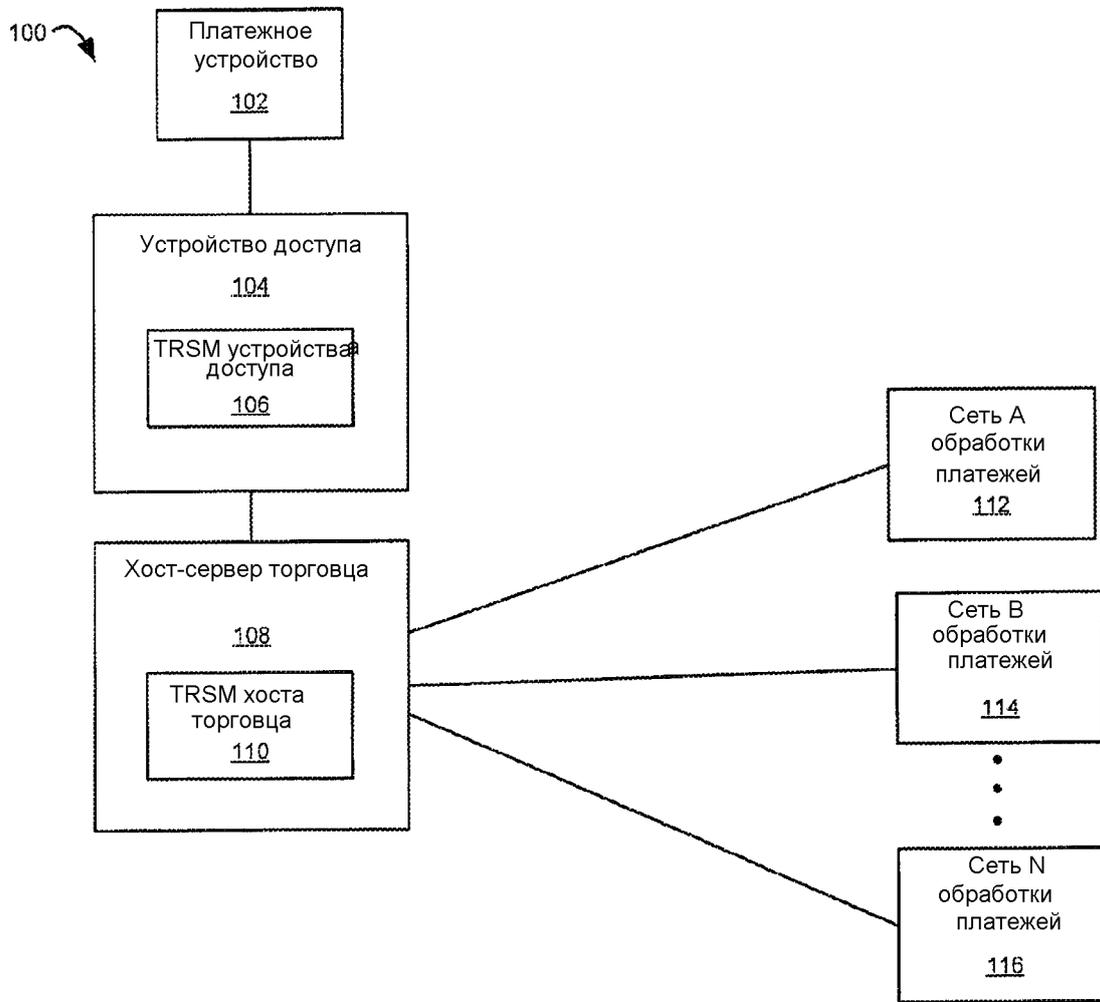
FIELD: information technology.

SUBSTANCE: method of protecting data, associated with the transaction, containing the stages at which: personal identification number (PIN) and sensitive data, including account identifier, are received through access devices; PIN is encrypted by access device. PIN encryption uses the first version of encryption key, based on seed key; sensitive data, including account identifier, is encrypted through access device. Encrypted account identifier has the same format as account identifier, and subset of numbers of encrypted account identifier represents the encrypted numbers of account identifier; the encrypted account identifier is written in the field of authorization request message. Field is used to receive account identifier; element of authorization

request message data is used as a signal to identify the existence of encrypted account identifier in authorization request message; and authorization request message, including encrypted PIN and encrypted sensitive data, is transmitted to host server.

EFFECT: providing a mechanism for transfer and routing encrypted identifier, account number through network of processing without the need to update existing routing infrastructure to handle encrypted values, that improves identifier security, account number, as identifier, account number can remain encrypted until the authorization request message passes through the nodes of network.

32 cl, 9 dwg



ФИГ.1

ПЕРЕКРЕСТНЫЕ ССЫЛКИ НА РОДСТВЕННЫЕ ЗАЯВКИ

[0001] Настоящая заявка является родственной по отношению к Предварительной Заявке США № 61/583,550, поданной 05 января 2012 г. (Регистрационный Номер №: 79900-819288), которая для всех целей во всей своей полноте включена в настоящий документ посредством ссылки. Настоящая заявка также является родственной по отношению к Предварительной Заявке США № 61/607,546, поданной 06 марта 2012 г. (Регистрационный Номер №: 7900-829470), которая для всех целей во всей своей полноте включена в настоящий документ посредством ссылки. Настоящая заявка дополнительно является родственной по отношению к Предварительной Заявке США № 61/704,428, поданной 21 сентября 2012 г. (Регистрационный Номер №: 79900-851259), которая для всех целей во всей своей полноте включена в настоящий документ посредством ссылки.

УРОВЕНЬ ТЕХНИКИ

[0002] Данные финансового счета могут быть защищены от неавторизованного доступа посредством таких мер, как шифрование данных в устройствах с методами обеспечения безопасности, основанными на аппаратном обеспечении. Тем не менее, существующие меры безопасности, такие как шифрование личного идентификационного номера (PIN), могут оставлять незащищенными уязвимые данные, такие как первичный номер счета (PAN). Существующие решения для защиты уязвимых данных могут требовать применения схем управления ключей, которые отличаются от тех, что используются для шифрования данных PIN, увеличивая нагрузку на торговцев по обеспечению безопасности финансовых данных.

[0003] Торговцы могут защищать данные финансового счета посредством организации маршрутизации всех транзакций в единый пункт назначения для обработки платежей. Тем не менее, при маршрутизации запроса авторизации в отношении транзакции, торговец может иметь возможность выбора сети обработки платежей из числа нескольких доступных сетей обработки платежей. Для торговца может потребоваться обеспечить дешифрование информации в сообщении запроса авторизации и повторное шифрование информации на основании пункта назначения маршрутизации сообщения запроса авторизации. В некоторых сетях обработки платежей может отсутствовать решение шифрования для уязвимых данных. Торговец может пожелать использовать меры шифрования, предоставляемые первой сетью обработки платежей, при этом продолжая иметь возможность маршрутизации запросов авторизации в альтернативные сети обработки платежей.

[0004] Описываемые в настоящем документе варианты осуществления решают эти и другие проблемы.

СУЩНОСТЬ ИЗОБРЕТЕНИЯ

[0005] Предоставляются методики для защиты уязвимых данных при маршрутизации запроса авторизации для транзакции в среду, которая содержит множество параметров сети обработки платежей.

[0006] В одном варианте осуществления описывается способ. Способ включает в себя этап, на котором шифруют личный идентификационный номер (PIN) устройством доступа. Шифрование PIN использует первый вариант ключа шифрования, основанный на исходном ключе. Устройство доступа шифрует уязвимые данные, используя второй вариант ключа шифрования, основанный на исходном ключе. Сообщение запроса авторизации, включающее в себя зашифрованный PIN и зашифрованные уязвимые данные, передается хост-серверу.

[0007] В другом варианте осуществления способ включает в себя этап, на котором принимают сообщение запроса авторизации на хост-сервере. Модуль безопасности,

соединенный с возможностью осуществления связи с хост-сервером, дешифрует зашифрованные уязвимые данные. Модуль безопасности повторно шифрует дешифрованные уязвимые данные с помощью первого ключа шифрования зоны уязвимых данных, ассоциированного с первой сетью обработки платежей. Первое переведенное сообщение запроса авторизации, включающее в себя повторно зашифрованные уязвимые данные, передается хост-сервером первой сети обработки платежей. В дополнительном варианте осуществления сообщение запроса авторизации, принятое хост-сервером, включает в себя PIN. Модуль безопасности дешифрует зашифрованный PIN и повторно шифрует дешифрованный PIN с помощью первого ключа шифрования зоны PIN, ассоциированного с первой сетью обработки платежей. Первое переведенное сообщение запроса авторизации включает в себя повторно зашифрованный PIN. В дополнительном варианте осуществления модуль безопасности выполнен с возможностью передачи второго переведенного сообщения запроса авторизации второй сети обработки платежей. Второй ключ шифрования зоны PIN используется для повторного шифрования PIN для второго переведенного сообщения запроса авторизации, а второй ключ шифрования зоны уязвимых данных используется для повторного шифрования уязвимых данных для второго сообщения запроса авторизации.

[0008] Другой вариант осуществления технологии направлен на систему. Система включает в себя процессор и машиночитаемый носитель информации, связанный с процессором. Машиночитаемый носитель информации содержит код, исполняемый процессором для реализации способа, содержащего этап, на котором шифруют личный идентификационный номер (PIN) устройством доступа. Шифрование PIN использует первый вариант ключа шифрования, основанный на исходном ключе. Устройство доступа шифрует уязвимые данные, используя второй вариант ключа шифрования, основанный на исходном ключе. Сообщение запроса авторизации, включающее в себя зашифрованный PIN и зашифрованные уязвимые данные, передается хост-серверу.

[0009] Дополнительный вариант осуществления технологии направлен на систему. Система включает в себя процессор и машиночитаемый носитель информации, связанный с процессором. Машиночитаемый носитель информации содержит код, исполняемый процессором для реализации способа, содержащего этап, на котором принимают сообщение запроса авторизации на хост-сервере. Сообщение запроса авторизации включает в себя зашифрованные уязвимые данные. Модуль безопасности, соединенный с возможностью осуществления связи с хост-сервером, дешифрует зашифрованные уязвимые данные. Модуль безопасности повторно шифрует дешифрованные уязвимые данные с помощью первого ключа шифрования зоны уязвимых данных, ассоциированного с первой сетью обработки платежей. Первое переведенное сообщение запроса авторизации, включающее в себя повторно зашифрованные уязвимые данные, передается хост-сервером первой сети обработки платежей.

[0010] В дополнительном варианте осуществления способ включает в себя этап, на котором принимают данные, ассоциированные с идентификатором личного счета (PAI). Устройство доступа может шифровать PAI. Зашифрованный PAI может иметь тот же формат, что и у PAI. Зашифрованный PAI записывается в поле сообщения запроса авторизации. Поле сообщения запроса авторизации является полем, которое предназначено для приема PAI. Элемент данных сообщения запроса авторизации используется в качестве сигнала для идентификации наличия зашифрованного PAI в сообщении запроса авторизации. Устройство доступа передает сообщение запроса авторизации.

[0011] Эти и прочие варианты осуществления более подробно описываются ниже.
КРАТКОЕ ОПИСАНИЕ ЧЕРТЕЖЕЙ

[0012] Фиг. 1 показывает примерную систему, в которой могут быть реализованы варианты осуществления технологии.

5 [0013] Фиг. 2 является иллюстративной блок-схемой для шифрования PIN и уязвимых данных на устройстве доступа и хосте торговца.

[0014] Фиг. 3 является иллюстративной блок-схемой для перевода уязвимых данных на хосте.

10 [0015] Фиг. 4 является иллюстративной блок-схемой для перевода PIN и уязвимых данных на хосте.

[0016] Фиг. 5 является таблицей, показывающей иллюстративную спецификацию для структуры и содержимого дорожки один платежного устройства.

[0017] Фиг. 6 является таблицей, показывающей иллюстративную спецификацию для структуры и содержимого дорожки два платежного устройства.

15 [0018] Фиг. 7 является блок-схемой, иллюстрирующей реализацию шифрования с сохранением формата в соответствии с вариантом осуществления.

[0019] Фиг. 8 является блок-схемой, иллюстрирующей интерпретацию данных для определения того, было ли применено шифрование с сохранением формата.

20 [0020] Фиг. 9 изображает иллюстративную высокоуровневую структурную схему компьютерной системы.

ПОДРОБНОЕ ОПИСАНИЕ ИЗОБРЕТЕНИЯ

[0021] Раскрываемые в данном документе варианты осуществления направлены на методики для защиты финансовых данных в сообщении запроса авторизации. Понятия, используемые в данном документе для описания вариантов осуществления, могут быть
25 поняты при обращении к предоставленным ниже описаниям.

[0022] «Сообщение запроса авторизации» может быть запросом для авторизации транзакции. Сообщение запроса авторизации может быть отправлено эмитенту платежного счета для запроса авторизации транзакции, выполняемой с помощью
30 платежного счета. Сообщение запроса авторизации может генерировать торговец. Сообщение запроса авторизации может быть передано эмитенту через эквайера.

[0023] Сообщение запроса авторизации может иметь определенный формат, чтобы способствовать осуществлению запросов и ответов между точками в финансовой сети. Например, сообщение запроса авторизации может быть стандартизованным сообщением обмена, таким как сообщение, которое соответствует стандарту Международной
35 Организации по Стандартизации (ISO) 8583, который является стандартом для систем, которые осуществляют обмен электронными транзакциями. Сообщение стандарта ISO 8583 может включать в себя индикатор типа сообщения, одну или более битовых карт, указывающих на то, какие элементы данных присутствуют в сообщении, и элементы данных сообщения. Данные, включенные в сообщение запроса авторизации, могут
40 включать в себя данные, полученные от платежного устройства, как, впрочем, и прочие данные, относящиеся к транзакции, владельцу платежного счета и торговцу. Например, сообщение запроса авторизации может включать в себя личный идентификационный номер (PIN), и уязвимые данные, такие как первичный номер счета (PAN), имя держателя карты, и дискреционные данные. Дополнительно, сообщение запроса авторизации
45 может включать в себя дату истечения срока действия платежного устройства, код валюты, сумму транзакции, отметку транзакции торговца, город акцептанта, штат/ страну акцептанта, транзитный номер маршрутизации, идентификационные данные терминала, идентификационные данные сети, и т.д. Сообщение запроса авторизации

может быть защищено при помощи шифрования для того, чтобы предотвратить раскрытие данных.

[0024] Сообщение запроса авторизации может включать в себя идентификатор платежного счета. Идентификатор платежного счета может быть ассоциирован с портативным устройством покупателя, таким как кредитная карта или дебетовая карта. Например, идентификатор платежного счета может быть первичным номером счета (PAN). PAN может быть уникальным номером платежной карты, таким как номер счета кредитной карты, ассоциированный с кредитной картой, или номер дебетового счета, ассоциированный с дебетовой картой. PAN может идентифицировать эмитента, как, впрочем, и счет держателя карты. Там где в данном документе используется понятие PAN, следует понимать, что может быть использован любой идентификатор платежного счета.

[0025] Личный идентификационный номер (PIN) может быть цифровым паролем, обмен которым осуществляется между пользователем и системой и который используется для аутентификации пользователя системой. Блок PIN может быть зашифрованным блоком данных, используемым для инкапсуляции PIN. Блок PIN может быть составлен из PIN, длины PIN и поднабора PAN.

[0026] Дискреционные данные эмитента (IDD), также именуемые как «дискреционные данные», могут быть данными, которые размещаются на Дорожке 1 и/или Дорожке 2 магнитной ленты или чипе платежного устройства или иным образом ассоциированы с платежным счетом. IDD могут быть переменными по длине и могут содержать данные проверки покупателя и/или карты, такие как значение смещения PIN, значение проверки PIN (PVV), значение проверки карты (CVV), и т.д. IDD также могут включать в себя прочие данные, которые определены торговыми марками и/или эмитентами карты, такие как информация, используемая в программе лояльности, данные корпоративного обслуживания, и т.д.

[0027] «Эквайер», как правило, является коммерческой организацией (например, коммерческим банком), который имеет коммерческие отношения с конкретным торговцем. Например, эквайер может размещать фонды на счету банка торговца и возмещать эти фонды от эмитентов.

[0028] «Эмитент», как правило, является коммерческой организацией (например, банком или кредитным обществом), которая выпускает платежное устройство для владельца счета и обеспечивает функции администрирования и управления для платежного счета. Некоторые организации могут выполнять функции как эмитента, так и эквайера. Платежный счет может быть любым счетом, который используется в транзакции, таким как кредитный, дебетовый или предоплаченный счет.

[0029] «Платежное устройство» может относиться к устройству, используемому для инициирования транзакции, такому как портативное устройство покупателя или портативное устройство связи. Платежное устройство может взаимодействовать с устройством доступа, таким как устройство точки продажи, для инициирования транзакции. Как правило, портативное устройство покупателя является переносным и компактным, таким, что оно может помещаться в кошельке или кармане покупателя (например, карманного размера). Конкретные примеры портативных устройства покупателя включают в себя платежные карты, такие как интеллектуальные карты, дебетовые устройства (например, дебетовые карта), кредитные устройства (например, кредитная карта), или устройства с хранимой суммой (например, карта с хранимой суммой или «предоплаченная» карта). Портативное устройство связи, также именуемое как «мобильное устройство», может быть, например, сотовым или беспроводным

телефоном (например, смартфоном), персональным цифровым помощником (PDA), портативным компьютером (например, планшетным компьютером или компьютером класса лэптоп), пейджером или иным портативным устройством, которое переносится держателем платежного счета.

5 [0030] «Устройство доступа» может относиться к устройству, которое принимает информацию от платежного устройства для инициирования транзакции. Например, устройством доступа может быть устройство точки продажи, выполненное с
возможностью считывания данных счета, закодированных на магнитной ленте или чипе портативного устройства покупателя формата карты. Другие примеры устройств
10 доступа включают в себя сотовые телефоны, PDA, персональные компьютеры, серверные компьютеры, планшеты, переносные специализированные считывающие устройства, абонентские приемники, электронные кассовые аппараты, банкоматы (АТМ), виртуальные кассовые аппараты, киоски, системы безопасности, системы доступа и подобное. Устройства доступа могут использовать средства, такие как радиочастотные
15 (RF) считывающие устройства или считывающие устройства с магнитной ленты для взаимодействия с платежным устройством. Устройство доступа может быть устройством, расположенным в физическом местоположении торговца, или может быть виртуальной точкой продажи, такой как web-сайт, который является частью транзакции формы электронной коммерции (электронной коммерции). При транзакции формы
20 электронной коммерции владелец счета может вводить данные платежного счета в портативное устройство связи, персональный компьютер или иное устройство, выполненное с возможностью осуществления связи с компьютером торговца. При других транзакциях без участия карты, таких как транзакции заказа через почту или заказа по телефону, информация может быть введена в компьютер торговца,
25 выступающего в роли устройства доступа. В дополнительном примере связь может происходить между бесконтактным элементом портативного устройства связи и устройством доступа, таким как считывающее устройство торговца или терминал точки продажи, посредством использования механизма беспроводной связи, такого как связь ближнего поля (NFC), RF, инфракрасная, оптическая связь и т.д.

30 [0031] «Сеть обработки платежей» может включать в себя систему, которая принимает сообщение запроса авторизации. Сеть обработки платежей может получать информацию из сообщения запроса авторизации для использования при определении того, одобрить ли транзакцию, ассоциированную с сообщением запроса авторизации. Сеть обработки платежей может отправлять сообщение ответа авторизации торговцу, указывающее
35 на то, одобрена ли транзакция. В некоторых вариантах осуществления сеть обработки платежей может выполнять процесс выплат, который может вызывать занесение транзакций на счета, ассоциированные с платежными устройствами, использованными для транзакций, и вычисление чистой дебетовой или кредитовой позиции каждого пользователя платежных устройств. Сеть обработки платежей может управляться
40 эквайером и/или эмитентом.

[0032] «Хост» может быть одной или более системами, такими как сервер, отвечающими за выполнение обработки транзакции торговца, решение маршрутизации и/или захват. Хост может размещаться у торговца, в шлюзе, процессоре или другом объекте. В некоторых вариантах осуществления хост может быть ассоциирован с
45 моделями непосредственного обмена торговца (MDEX), активного посредника (VAR), или иными моделями связности. Там, где в данном документе используется понятие «хост-сервер торговца», следует понимать, что может быть использован любой сервер, такой как сервер обработки платежей.

[0033] «Модуль безопасности с защитой от вмешательства» (TRSM) является устройством, которое включает в себя физические средства защиты для предотвращения раскрытия криптографических параметров безопасности, которые содержатся в устройстве. TRSM доступны с различными уровнями защиты. TRSM, который является защищенным от вмешательства, может использовать физические меры, такие как упрочненный корпус, делающий проникновение в устройство сложным. TRSM с индикацией вмешательства может обладать характеристиками аппаратного обеспечения, которые делают очевидными попытки проникновения для последующих наблюдателей, как, например, уплотнение, которое будет разрушено во время проникновения в устройство. TRSM с реакцией на вмешательство может быть выполнен с возможностью обнаружения попытки проникновения и разрушения уязвимой информации, такой как криптографические параметры безопасности, при возникновении попытки проникновения.

[0034] «Модуль безопасности аппаратного обеспечения» (HSM) является TRSM с криптопроцессором безопасности, который может управлять цифровыми ключами, ускорять криптопроцессы и/или обеспечивать жесткую аутентификацию для доступа к важным ключам для серверных приложений. HSM может обеспечивать как логическую, так и физическую защиту уязвимой информации от неавторизованного доступа. HSM может быть физическим устройством в виде подключаемой карты или внешним устройством безопасности. HSM может быть соединен с возможностью осуществления связи с хостом.

[0035] Промышленные стандарты безопасности данных для платежных карт (PCI DSS) являются набором требований, применяемых к объектам, задействованным в обработке транзакции. Цель требований состоит в обеспечении безопасности финансовых данных.

[0036] Схема с Извлекаемым Уникальным Ключом для Каждой Транзакции (DUKPT) является схемой управления ключами, которая может получать уникальный ключ транзакции для каждой транзакции. DUKPT использует базовый ключ извлечения (BDK), который, как правило, известен только стороне, которая инициализирует TRSM, и получателю сообщения, зашифрованного посредством TRSM. В TRSM, как правило, внедряется исходный ключ, который извлечен из BDK. Ключ транзакции может быть извлечен из исходного ключа. Если извлеченный ключ раскрыт, то будущие и прошлые данные транзакции остаются защищенными, поскольку следующие или предыдущие ключи не могут быть легко определены из извлеченного ключа. DUKPT может быть использована для шифрования данных, ассоциированных с транзакцией электронной коммерции, таких как PIN и/или уязвимых данных.

[0037] Например, клавиатура ввода PIN может включать в себя TRSM с внедренным уникальным исходным ключом и серийным номером ключа. Клавиатура ввода PIN может генерировать уникальный ключ для каждой транзакции. Сообщение запроса авторизации, генерируемое клавиатурой ввода PIN, может включать в себя зашифрованный блок PIN и серийный номер ключа. Сообщение запроса авторизации может быть передано от клавиатуры ввода PIN хост-серверу торговца со своим собственным TRSM. TRSM хост-сервера торговца может использовать серийный номер ключа (KSN) для восстановления базового ключа извлечения (BDK), используемого при генерировании уникального исходного ключа клавиатуры ввода PIN. TRSM может использовать BDK и KSN для дешифрования зашифрованных данных.

[0038] Алгоритм Трехкратного Шифрования Данных (TDEA), также именуемый как «Стандарт Трехкратного Шифрования Данных», «3DES», «Трехкратный DES» и «TDES»,

является блочным шифром, который применяет алгоритм шифра Стандарта Шифрования Данных (DES) три раза к каждому шифруемому блоку данных.

5 [0039] «Ключ Шифрования Зоны» (ZEK) может указывать один или более ключей, используемых для шифрования данных между двумя конкретными точками (например, между хостом и сетью обработки платежей). Отдельные ZEK могут быть использованы для PIN или для уязвимых данных. В предпочтительном варианте осуществления ZEK используется только для шифрования уязвимых данных между сторонами и предпочтительно не является таким же, как PIN, MAC или другие конкретные ключи шифрования.

10 [0040] «Сервер» может включать в себя один или более компьютеров. Несколько компьютеров сервера могут быть соединены с возможностью осуществления связи через сетевые соединения, такие как проводные, беспроводные и/или интернет сетевые соединения. Один или более компьютеров сервера могут хранить базы данных.

ШИФРОВАНИЕ И ПЕРЕВОД ЗОНЫ PIN И УЯЗВИМЫХ ДАННЫХ

15 [0041] Когда платежное устройство используется для транзакции, то для транзакции может быть сгенерировано сообщение запроса авторизации. Сообщение запроса авторизации может включать в себя личный идентификационный номер (PIN) и уязвимые данные, такие как первичный номер счета (PAN), имя держателя карты, адрес держателя карты, дискреционные данные эмитента, или иные уязвимые данные. Уязвимые данные
20 могут быть данными, которые хранятся с помощью платежного устройства, как, например, на магнитной ленте или чипе платежного устройства. В качестве альтернативы данными хранения могут быть данные, предоставленные пользователем устройству доступа, такие как информация об адресе держателя карты, предоставленная пользователем в ходе электронной коммерции или иной транзакции без участия карты.
25 PIN и уязвимые данные могут быть зашифрованы устройством доступа, которое принимает информацию от платежного устройства. PIN и уязвимые данные могут быть зашифрованы при помощи вариантов ключа шифрования основанных на исходном ключе, который внедрен в устройство доступа.

[0042] Фиг. 1 показывает примерную систему 100, в которой могут быть реализованы
30 варианты осуществления технологии. Система 100 включает в себя один или более серверных компьютеров, подсистемы обработки данных и сети, которые могут быть использованы для инициирования сообщения запроса авторизации для транзакции и маршрутизации сообщения запроса авторизации к объекту, выполненному с
35 возможностью одобрения транзакции. Там, где показан лишь один из каждого компонента, следует понимать, что варианты осуществления технологии могут включать в себя более одного из каждого компонента. В дополнение, некоторые варианты осуществления технологии могут включать меньшее число компонентов, чем все из
40 показанных на Фиг. 1. Также, компоненты на Фиг. 1 могут осуществлять связь через любое пригодное средство связи (включая Интернет), используя любой пригодный протокол связи.

[0043] При типичной транзакции платежное устройство 102 взаимодействует с
устройством 104 доступа для инициирования транзакции. Устройство 104 доступа может
включать в себя модуль 106 безопасности с защитой от вмешательства (TRSM)
устройства доступа. TRSM 106 устройства доступа может быть физически и/или с
45 возможностью связи соединен с (или может быть неотъемлемым компонентом)
устройством 104 доступа. Устройство доступа может принимать информацию,
ассоциированную с платежным устройством 102, включая уязвимые данные, когда
платежное устройство 102 взаимодействует с устройством 104 доступа. В некоторых

вариантах осуществления устройство 104 доступа принимает уязвимые данные и/или PIN от устройства, хранящего информацию счета, такого как портативное устройство связи.

5 [0044] В иллюстративном примере платежное устройство 102 может быть кредитной картой, а устройство 104 доступа может быть клавиатурой ввода PIN, смонтированной в корпусе TRSM. Клавиатура ввода PIN может иметь интерфейс пользователя для приема цифрового ввода, указывающего пароли PIN, и считывающее устройство для магнитной ленты для получения данных дорожки с магнитной ленты платежного устройства.

10 [0045] В других вариантах осуществления информацией платежного устройства может быть ввод пользователя, который принимается устройством 104 доступа. Данные PIN могут быть приняты от платежного устройства 102 или через ввод пользователя, принятый посредством устройства 106 доступа.

15 [0046] Когда устройство 104 доступа принимает данные, такие как PIN и информацию платежного устройства, TRSM 106 может зашифровать данные. В некоторых случаях может потребоваться получить PAN перед шифрованием PIN. Уязвимые данные, такие как PAN, имя держателя карты, адрес держателя карты, и дискреционные данные могут быть определены из информации, принятой от платежного устройства 102. Уязвимые данные могут быть получены путем анализа данных дорожки, полученных устройством
20 104 доступа от платежного устройства 102. В некоторых вариантах осуществления устройство 106 доступа шифрует PIN посредством генерирования блока PIN, основанного на PIN, длины PIN и поднабора PAN. Устройство 104 доступа может шифровать уязвимые данные, включающие в себя одно или более из следующего: PAN, имя держателя карты, адрес держателя карты, дискреционные данные и любую иную
25 информацию, которая рассматривается в качестве уязвимых данных.

[0047] TRSM 106 устройства доступа может хранить исходный ключ, используемый для шифрования данных. Для каждой транзакции из исходного ключа может быть извлечен один или более ключей транзакции. Для соответствия требованиям, таким как PCI DSS, может потребоваться, чтобы разные ключи транзакции применялись к
30 PIN и уязвимым данным. PIN может быть зашифрован, используя первый ключ транзакции, извлеченный из исходного ключа, а уязвимые данные могут быть зашифрованы, используя второй ключ транзакции, извлеченный из исходного ключа. Таким образом, как PIN, так и уязвимые данные могут быть зашифрованы, используя одну и ту же схему управления ключами (такую как DUKPT) и один и тот же алгоритм
35 шифрования (такой как TDEA).

[0048] Сообщение запроса авторизации, включающее в себя данные PIN и зашифрованные уязвимые данные, может быть сгенерировано устройством 104 доступа и передано хост-серверу 108 торговца. Сообщение запроса авторизации может включать в себя назначенные поля для различных типов данных. Когда шифрование применяется
40 к данным в сообщении запроса авторизации, шифрование может менять параметры (такие как тип данных, длина данных, и т.д.) поля, ассоциированного с зашифрованными данными. Благодаря измененным параметрам зашифрованные данные могут быть помещены в новое поле. Например, сообщение запроса авторизации может включать в себя поле с таким размером, чтобы вмещать PAN. Когда применяется шифрование,
45 PAN и прочие уязвимые данные могут быть помещены в одно или более альтернативных полей сообщения запроса авторизации. В сообщении запроса авторизации может быть добавлено поле для сигнализации того, что зашифрованный PAN находится в поле зашифрованного PAN. Уязвимые данные, такие как PAN, имя держателя карты, и

дискреционные данные могут быть зашифрованы в устройстве 104 доступа и помещены в отдельные элементы внутри поля сообщения запроса авторизации, такого как поле 53 сообщения запроса авторизации в формате ISO.

5 [0049] В некоторых вариантах осуществления шифрование с сохранением формата применяется к уязвимым данным в сообщении запроса авторизации. Например, когда используется шифрование с сохранением формата, то поднабор цифр PAN может быть заменен зашифрованными значениями, тогда как отдельные цифры PAN остаются неизменными. В предпочтительном варианте осуществления первые шесть цифр и последние четыре цифры PAN остаются неизменными, а цифры в середине заменяются зашифрованными значениями. Таким образом, сообщение запроса авторизации может обрабатываться сетями обработки платежей, которые не выполнены с возможностью обработки сообщения запроса авторизации с альтернативными полями для хранения зашифрованных данных. Для сигнализации наличия зашифрованных данных внутри поля PAN сообщения запроса авторизации измененная дата истечения срока действия 10 может быть включена в поле даты истечения срока действия сообщения запроса авторизации. Например, сообщение запроса авторизации может содержать дату истечения срока действия, которая находится через 40 лет по отношению к дате истечения срока действия, ассоциированной с платежным устройством, использованным для транзакции.

20 [0050] Хост-сервер 108 торговца может включать в себя TRSM 110 хоста торговца. TRSM 110 хоста торговца может быть с возможностью связи и/или физически соединен с или может быть неотъемлемым компонентом хост-сервера 108 торговца. В некоторых вариантах осуществления TRSM 110 хоста торговца может быть расположен удаленно от здания сервера 108 торговца. Для того чтобы обеспечивать маршрутизацию транзакций к нескольким сетям обработки платежей, торговцу может потребоваться, чтобы TRSM 110 хоста торговца переводил зашифрованные данные в сообщении запроса авторизации. Например, может потребоваться перевести ключи в TRSM 110 хоста торговца для совместимости со стандартами PCI DSS, ограничивающими незащищенность ключей, ассоциированных с TRSM 106 устройства доступа. Когда 25 хост-сервер 108 торговца выполнен с возможностью маршрутизации сообщений запроса авторизации нескольким сетям 112-116 обработки платежей, хост-сервер 108 торговца может переводить зашифрованные данные в Ключ Шифрования Зоны (ZEK), ассоциированный с конкретной сетью обработки платежей. Хост-сервер 108 торговца может определять, каким образом осуществлять маршрутизацию сообщения запроса авторизации на основании информации, которая содержится в сообщении запроса авторизации. Например, первые шесть цифр поля PAN, содержащие PAN, зашифрованный в соответствии со способом шифрования с сохранение формата, могут быть использованы хост-сервером 108 торговца для определения того, каким образом осуществлять маршрутизацию сообщения запроса авторизации.

40 [0051] Перевод посредством TRSM 110 хоста торговца может включать в себя дешифрование PIN и уязвимых данных в сообщении запроса авторизации, принятом от устройства 104 доступа, и повторное шифрование PIN и уязвимых данных, используя один или более Ключей Шифрования Зоны (ZEK). ZEK может быть ассоциирован с конкретной сетью обработки платежей. ZEK, как правило, является ключом, который совместно используется сетью обработки платежей и хост-сервером 108 торговца. 45 Может потребоваться применение разных ZEK к PIN и уязвимым данным, например, для совместимости с PCI DSS. Перевод может выполняться TRSM 110 Хоста Торговца таким образом, что дешифрованный PIN и уязвимые данные никогда не раскрываются

хост-серверу 108 торговца. Хост-сервер 108 торговца может передавать сообщение запроса авторизации, включающее в себя переведенный PIN и уязвимые данные, одной из сетей 112-116 обработки платежей, в которую должна быть выполнена маршрутизация сообщения запроса авторизации.

5 [0052] В некоторых вариантах осуществления хост-сервер 108 торговца может осуществлять маршрутизацию сообщения запроса авторизации в сеть обработки платежей, которая не выполнена с возможностью обработки зашифрованных данных. В таких вариантах осуществления зашифрованные уязвимые данные могут быть дешифрованы и сообщение запроса авторизации, включающее в себя дешифрованные
10 уязвимые данные, может быть передано от хост-сервера 108 торговца сети обработки платежей.

[0053] Сеть обработки платежей, которая принимает сообщение запроса авторизации, может дешифровать PAN и прочие уязвимые данные и также может проверять PIN. Сеть обработки платежей может определять, является ли транзакция авторизованной.
15 В некоторых случаях сообщение запроса авторизации может быть передано серверу эмитента, который может определять, является ли транзакция авторизованной. Сообщение ответа авторизации, указывающее на то, была ли транзакция авторизована, может маршрутизироваться обратно хост-серверу 108 торговца от эмитента и/или сети обработки платежей, которая приняла сообщение запроса авторизации. Ответ
20 авторизации может быть отображен устройством 104 доступа, распечатан по приему, или иным образом переправлен держателю платежного счета.

[0054] Следует понимать, что сервер, ассоциированный с сетью обработки платежей или иным объектом и ассоциированным TRSM, может быть использован вместо хост-сервера 108 торговца и TRSM 110 хоста торговца.

25 [0055] Процесс безналичного расчета и выплат, как правило, проводится каждой из сетей обработки платежей в фиксированное время. Фиксированное время может меняться от одной сети к другой. Процесс безналичных расчетов является процессом обмена финансовыми подробностями между эквайером и эмитентом, чтобы способствовать выполнению проводки на платежный счет счета держателя и выверки
30 позиции выплат покупателя.

[0056] Внутри TRSM данные могут быть зашифрованы и/или дешифрованы, используя DUKPT и TDES. Следует иметь в виду, что другие системы распределения ключей (такие как мастер/сеансовый и фиксированный ключ) и/или другие алгоритмы шифрования (такие как RSA, DEA, ECIES, EAS, или другие алгоритмы шифрования) могут быть
35 применены.

[0057] Фиг. 2 является иллюстративной блок-схемой для шифрования PIN и уязвимых данных в устройстве доступа и хосте торговца. На этапе 202 держатель карты может представить платежное устройство 102 устройству 104 доступа. На этапе 204 устройство 104 доступа может считать данные с платежного устройства 102, такие как данные
40 дорожки, хранящиеся на магнитной ленте платежного устройства. Данные, считанные с платежного устройства 102, могут включать в себя уязвимые данные, такие как PAN, имя держателя карты, и дискреционные данные. На этапе 206 устройство 104 доступа может принять PIN, такой как PIN, введенный через интерфейс пользователя устройства 104 доступа.

45 [0058] На этапе 208 устройство 104 доступа может зашифровать PIN, используя первый ключ. Первый ключ может быть первым ключом конкретной транзакции, извлеченным из ключа, внедренного в устройство 104 доступа. На этапе 210 устройство 104 доступа может зашифровать уязвимые данные, используя второй ключ. Уязвимые

данные могут включать в себя одно или более из следующего: PAN, имя держателя карты, дискреционные данные, адрес держателя карты, и любые другие уязвимые данные, принятые устройством 104 доступа. Второй ключ может быть вторым ключом конкретной транзакции, извлеченным из ключа, внедренного в устройство 104 доступа.

5 На этапе 212 устройство 104 доступа может генерировать сообщение запроса авторизации, включающее в себя зашифрованный PIN и зашифрованные уязвимые данные, и передавать сообщение запроса авторизации хост-серверу, такому как хост-сервер 108 торговца.

[0059] В некоторых вариантах осуществления хост-устройство может принимать сообщение запроса авторизации, включающее в себя зашифрованные уязвимые данные от устройства доступа. Запрос авторизации может включать в себя или может не включать в себя зашифрованный PIN. Например, устройство доступа может принимать уязвимые данные от кредитной карты или другого платежного устройства в отношении транзакции, которая не требует номера PIN. В таких вариантах осуществления хост-устройство может переводить уязвимые данные.

[0060] Фиг. 3 является иллюстративной блок-схемой для перевода уязвимых данных на хосте. На этапе 302 хост, такой как хост-сервер 108 торговца, принимает сообщение запроса авторизации, включающее в себя зашифрованные уязвимые данные, от устройства 104 доступа. Хост может получить уязвимые данные посредством анализа сообщения запроса авторизации. На этапе 304 хост может дешифровать уязвимые данные, используя информацию, извлеченную из базового ключа извлечения. Для перевода уязвимых данных хост может дешифровать уязвимые данные, используя информацию, извлеченную из базового ключа извлечения, ассоциированного с устройством 104 доступа, как указывается на этапе 304, и повторно зашифровать уязвимые данные, используя ключ шифрования зоны, как указывается на этапе 306. На этапе 308 хост может передать сообщение запроса авторизации сети обработки платежей.

[0061] В некоторых вариантах осуществления хост может принимать сообщение запроса авторизации, включающее в себя зашифрованный PIN и зашифрованные уязвимые данные. Хост может переводить PIN и уязвимые данные.

[0062] Фиг. 4 является иллюстративной блок-схемой для перевода PIN и уязвимых данных в хосте. На этапе 402 хост, такой как хост-сервер 108 торговца, принимает сообщение запроса авторизации, включающее в себя зашифрованный PIN и зашифрованные уязвимые данные от устройства 104 доступа. Дешифрованные уязвимые данные, такие как дешифрованный PAN, могут потребоваться для дешифрования PIN. Хост может получать уязвимые данные посредством анализа сообщения запроса авторизации. На этапе 404 хост может дешифровать уязвимые данные, используя информацию, извлеченную из базового ключа извлечения. Хост может получать PIN посредством анализа сообщения запроса авторизации. На этапе 406 хост может дешифровать PIN, используя информацию, извлеченную из базового ключа извлечения, и в некоторых случаях также используя дешифрованный PAN. Для перевода PIN хост может повторно шифровать PIN, используя ключ шифрования зоны, как указывается на этапе 408. В некоторых вариантах осуществления PIN повторно шифруется, используя ключ шифрования зоны и дешифрованный PAN. Для перевода уязвимых данных хост может повторно шифровать уязвимые данные, используя ключ шифрования зоны, как указывается на этапе 410.

[0063] В некоторых вариантах осуществления отдельные ключи шифрования зоны могут быть использованы для шифрования PIN и уязвимых данных. Например, ключ

шифрования зоны, конкретный для PIN, может быть использован или сгенерирован для использования при шифровании номеров PIN, и ключ шифрования зоны, конкретный для уязвимых данных, может быть использован или сгенерирован для использования при шифровании уязвимых данных. Кроме того, каждая сеть 112-116 обработки платежей может использовать один или более ключей шифрования зоны, которые являются конкретными для индивидуальной сети обработки платежей. Таким образом, первый ключ шифрования зоны, конкретный для PIN, и первый ключ шифрования зоны, конкретный для уязвимых данных, могут быть использованы для перевода, когда сообщение запроса авторизации должно быть маршрутизировано в первую сеть 112 обработки платежей, и второй ключ шифрования зоны, конкретный для PIN, и второй ключ шифрования зоны, конкретный для уязвимых данных, могут быть использованы для перевода, когда сообщение запроса авторизации должно быть маршрутизировано во вторую сеть 114 обработки платежей.

[0064] Хост-сервер 108 торговца может определять, какая сеть обработки платежей из сетей 112-116 обработки платежей должна принимать сообщение запроса авторизации. На этапе 412 хост-сервер 108 торговца может передавать сообщение запроса авторизации, включающее в себя переведенный (повторно зашифрованный) PIN и переведенные (повторно зашифрованные) уязвимые данные, определенной сети обработки платежей.

[0065] В некоторых вариантах осуществления хост-сервер 108 торговца включает в себя поддержку «белого списка», который позволяет исключить из защиты конкретные диапазоны карт, определенные торговцем или сетью обработки платежей. Когда уязвимые данные кодируются в устройстве 104 доступа, часть уязвимых данных может быть сохранена в незашифрованном виде для использования в устройстве 104 доступа. Например, некоторые или все из данных в поле дискреционных данных или другом поле данных дорожки на магнитной ленте платежного устройства 102 могут оставаться незашифрованными в сообщении запроса авторизации. Торговцам, которые используют данные в поле дискреционных данных для программ лояльности, программ корпоративного обслуживания или подобного, может потребоваться, чтобы эти данные оставались незашифрованными для сбора данных или иных целей.

[0066] В некоторых вариантах осуществления имя держателя карты и/или данные в поле дискреционных данных могут быть сделаны доступными устройству доступа до шифрования. Например, если приложение, исполняемое устройством доступа или другим устройством торговца, использует эти уязвимые данные (например, отображая имя держателя карты на кассовом аппарате, который соединен с возможностью связи с устройством клавиатуры для ввода PIN), то уязвимые данные могут быть раскрыты устройству продавца перед шифрованием.

[0067] Как рассмотрено выше, чип или магнитная лента в платежном устройстве могут иметь одну или более дорожек (как правило, три дорожки, именуемые как «дорожка один», «дорожка два» и «дорожка три»), которые содержат данные. Данные могут быть отформатированы в соответствии со стандартизированной структурой. Фиг. 5 и 6 являются таблицами, показывающими иллюстративные спецификации для данных дорожки платежного устройства. Следует иметь в виду, что данные дорожки со структурой, описанной на Фиг. 5 и 6, могут быть сохранены с привязкой к платежному счету на портативном мультимедийном устройстве или другом устройстве, используемом для электронной коммерции или иных транзакций без участия карты.

[0068] Фиг. 5 является таблицей, показывающей иллюстративную спецификацию для структуры и содержимого дорожки один платежного устройства. Дорожка 1

закодирована с помощью 7-битной схемы, которая основана на ASCII. Поля дорожки 1 могут включать в себя начальную граничную метку (такую как «%»), указывающую позицию, с которой начинаются отформатированные данные дорожки.

5 [0069] Код формата (такой как «В», указывающий финансовое учреждение), как правило, является следующим знаком в дорожке 1.

[0070] Первичный Номер Счета (PAN) может быть составлен из шести цифр Номера Идентификации Эмитента (PIN), переменной длины (максимум 12 цифр) личного номера счета и контрольной цифры. Конец данных, ассоциированных с PAN, может быть указан с помощью знака-разделителя, такого как каре (^).

10 [0071] Поле имени может включать в себя один алфавитный знак (в качестве фамилии) и разделитель фамилии. Знак пробела может потребоваться для разделения логических элементов поля имени, отличных от фамилии. Разделитель, завершающий поле имени, может быть закодирован вслед за последним логическим элементом поля имени. Если кодируется только фамилия, то Разделитель Полей (FS), такой как «^», может следовать за фамилией. В некоторых вариантах осуществления поле имени включает в себя 15 фамилию, с последующим разделителем фамилии (например, знак «/»), с последующим именем или инициалом, с последующим пробелом, с последующим вторым именем или инициалом. Имя может дополнительно включать в себя точку за вторым именем или инициалом, с последующим названием. Имя, как правило, оканчивается разделителем 20 (знаком «^»). Например, имя John C. Smith может быть закодировано как «SMITH/JOHN C».

[0072] Поле истечения срока действия дорожки один может иметь формат ГГММ, где ‘ГГ’ представляет собой последние две цифры года, а ‘ММ’ является цифровым представлением месяца.

25 [0073] Служебный код может быть цифровым полем с тремя подполями, представленными отдельными цифрами. Как правило, служебный код используется для указания критерия приемки эмитента для транзакций магнитной ленты и указания того, присутствует ли на карте связанная интегральная микросхема, обеспечивающая эквивалентное применение, как то, что определено магнитной лентой или теснением. 30 Каждое подполе служебного кода может быть идентифицировано своей позицией (позиция 1, 2 и 3) и может функционировать независимо, позволяя судить о его отдельных функциях.

[0074] Дискреционные данные эмитента могут следовать за служебным кодом. Конец дорожки указывается конечной граничной меткой, такой как знак вопроса («?»). Вслед 35 за конечной граничной меткой может быть включен знак продольного контроля избыточным кодом (LRC).

[0075] Фиг. 6 является таблицей, показывающей иллюстративную спецификацию для структуры и контента дорожки два платежного устройства. Коды знаков на дорожке два основаны на 5-битной схеме, которая основана на ASCII. Дорожка два может 40 содержать поля, аналогичные тем, что содержатся в дорожке один, как описано выше, но может отсутствовать поле имени держателя карты.

[0076] В некоторых вариантах осуществления данные PIN могут храниться и считываться с дорожки три платежного устройства.

ШИФРОВАНИЕ СО СПУТЫВАНИЕМ

45 [0077] После того как шифрование выполнено над полями данных, ассоциированными с платежным устройством 102, зашифрованная информация может быть сохранена в одном или более альтернативных полях сообщения запроса авторизации и спутанные данные могут быть сохранены в первоначальных полях сообщения запроса авторизации.

Например, данные могут быть считаны из полей PAN, имени держателя карты и дискреционных данных, ассоциированных с платежным устройством 102. Спутанные данные могут быть записаны в поля сообщения запроса авторизации, предназначенные для PAN, имени держателя карты и дискреционных данных, а зашифрованные версии PAN, имени держателя карты и дискреционных данных могут быть записаны в одно или более альтернативных полей сообщения запроса авторизации.

[0078] В иллюстративном примере, применительно к сообщению запроса авторизации, которое совместимо со стандартами ISO, альтернативное поле, такое как поле 53 ISO, может быть определено для приема зашифрованных данных и ассоциированных атрибутов шифрования. Новое определение поля 53 ISO может соответствовать типу «составного» поля, как определено в стандарте ISO. Новое поле 53 может принимать зашифрованные данные блока PIN и зашифрованные уязвимые данные. Когда применяется шифрование зон к сообщению запроса авторизации, то шифрование зон может быть применено к полю 53.

[0079] Когда спутанные данные записываются в поле PAN сообщения запроса авторизации, некоторые цифры PAN в сохраненном поле PAN могут быть сохранены, а другие цифры PAN могут быть спутаны. Например, поднабор цифр PAN, например, цифры 7-12 («средние шесть» цифр) PAN, могут быть спутаны, тогда как другие цифры, такие как первые шесть и последние четыре цифры PAN, остаются в качестве открытого текста. Спутывание может быть выполнено, например, посредством замены цифр 7-11 PAN на число 9, и замены цифры 12 PAN на число, вычисленное таким образом, чтобы гарантировать то, что последняя цифра PAN является действительной контрольной цифрой. Так как оставшиеся цифры PAN, такие как первые шесть цифр и заключительные четыре цифры, не спутаны, то оставшиеся цифры могут быть использованы для функций, таких как маршрутизация и определение приема. Таким образом, системы, которые предназначены для обработки данных, содержащихся в поле PAN, могут функционировать нормальным образом, несмотря на то, что PAN защищено посредством спутывания средних шести цифр. Зашифрованный PAN, хранящийся в поле зашифрованного PAN, может быть дешифрован, обеспечивая возможность записи дешифрованного (первоначального) PAN в поле PAN.

ШИФРОВАНИЕ С СОХРАНЕНИЕМ ФОРМАТА

[0080] Может быть желательным зашифровать данные, которые содержатся в сообщении запроса авторизации, без изменения формата сообщения запроса авторизации. Например, некоторые системы могут быть не предназначены для обработки сообщения запроса авторизации с добавленным полем закодированного PAN. Шифрование с сохранением формата может быть применено к уязвимым данным, таким как PAN, имя держателя карты и дискреционные данные из дорожки 1 и дорожки 2 данных дорожки, ассоциированных с платежным устройством 102.

[0081] PAN может быть закодирован таким образом, что результирующий закодированный PAN имеет тот же размер, что и первоначальный PAN. Таким образом, закодированный PAN может быть записан в поле первоначального PAN сообщения запроса авторизации, и не требуется альтернативного поля сообщения запроса авторизации для приема зашифрованного PAN. Некоторые цифры PAN могут быть оставлены незашифрованными, когда шифрование с сохранением формата применяется к PAN. Например, первые шесть и последние четыре цифры PAN могут оставаться незашифрованными, для обеспечения возможности маршрутизации и других функций, зависящих от данных, которые содержатся в этих цифрах.

[0082] Шифрование с сохранением формата может функционировать иначе

применительно к PAN, которые содержат действительные контрольные цифры.

Алгоритм для определения действительных контрольных цифр может быть таким, который определен в стандартах ISO. Контрольная цифра, которая, как правило,

является заключительной цифрой PAN, может быть цифрой, вычисленной из других цифр в сообщении, которое может быть использовано для определения того, были ли корректно приняты все цифры PAN. Контрольная цифра может быть использована для обнаружения ошибок передачи. В некоторых вариантах осуществления последняя цифра из цифр 7-12 («средние шесть» цифр) PAN вычисляется таким образом, что первоначальная последняя цифра незашифрованного PAN также является действительной контрольной цифрой для PAN, зашифрованного с помощью шифрования с сохранением формата. Когда PAN не содержит действительной контрольной цифры, все средние цифры могут быть зашифрованы с помощью алгоритма шифрования с сохранением формата.

[0083] Уязвимые данные могут быть преобразованы в десятичный алфавит перед шифрованием. После того как был применен алгоритм шифрования с сохранением формата, результирующие зашифрованные знаки в форме десятичного алфавита могут быть преобразованы в первоначальный кодовый набор и формат первоначальных уязвимых данных. Преобразованный результат шифрования может быть использован для замены первоначальных полей для уязвимых данных, таких как PAN, имя держателя карты, дискреционные данные, и т.д., в сообщении запроса авторизации.

[0084] Как правило, не будет очевидно из данных в полях, к которым было применено шифрование с сохранением формата, что данные были зашифрованы. Может быть использован сигнал в существующем поле данных сообщения запроса авторизации для указания того, что поле сообщения запроса авторизации содержит зашифрованные данные. Для реализации сигнала поле сообщения запроса авторизации, которое не содержит зашифрованные данные, может быть переписано с помощью нового содержимого, которое является модифицированной версией первоначального содержимого поля. Например, дата истечения срока действия в поле даты истечения срока действия сообщения запроса авторизации может быть заменено на измененную дату истечения срока действия. В одном варианте осуществления измененная дата истечения срока действия получается посредством добавления числа к дате истечения срока действия или части даты истечения срока действия. Например, число, такое как 40, может быть добавлено к части года даты истечения срока действия. Если поле даты истечения срока действия сообщения запроса авторизации содержит дату истечения срока действия вида «01/13», указывающую дату истечения срока действия как Январь 2013, то число 40 может быть добавлено к части года 13 и результирующая измененная дата истечения срока действия «01/53» может быть записана в поле даты истечения срока действия. Если транзакция происходит в 2013, то устройство, считывающее часть даты истечения срока действия сообщения запроса авторизации, может иметь возможность определения того, что дата истечения срока действия является измененной датой истечения срока действия, так как платежные устройства, как правило, выпускаются с датами истечения срока действия, которые находятся раньше 20 лет (например, 1-10 лет) с даты выпуска карты. На основании этого может быть определено, что дата истечения срока действия, которая соответствует сроку, который больше чем на двадцать лет находится дальше от настоящей даты, является измененной датой истечения срока действия.

[0085] В некоторых вариантах осуществления последняя цифра PAN может не содержать действительной контрольной цифры. Например, последняя цифра PAN может

не иметь контрольной цифры, как указывается стандартом ISO/IEC 7812-1. В случаях, где последняя цифра PAN не является действительной контрольной цифрой, число 20 может быть добавлено к месяцу даты истечения срока действия, перед тем как измененная дата истечения срока действия записывается в поле даты истечения срока действия сообщения запроса авторизации.

[0086] В некоторых вариантах осуществления поле даты истечения срока действия может отсутствовать в информации, принятой устройством 104 доступа. Например, считывание карты или клавишный ввод может быть выполнен с ошибками или по иным причинам может отсутствовать дата истечения срока действия. Число 40 может быть добавлено к месяцу даты истечения срока действия, созданной в процессе шифрования с сохранением формата, перед тем как измененная дата истечения срока действия записывается в поле даты истечения срока действия сообщения запроса авторизации.

[0087] Ниже описывается примерный алгоритм для шифрования с сохранением формата. Алгоритм шифрования с сохранением формата может функционировать в качестве поточного шифра, который является сохраняющим формат. Например, шифрование с сохранением формата может быть аналогичным Режиму Счетчика (CTR) из стандарта SP800-38A Национального Института Стандартов и Технологий (NIST), распространенного на сложение по модулю 0 вместо сложения по модулю 2.

[0088] В алгоритме с сохранением формата A может быть алфавитом с n разными знаками, где n является натуральным числом больше 1. A^* может быть обозначен набор строк с элементами из A , включающий в себя пустую строку. В данном описании предполагается, что алфавит A является набором $\{0, \dots, n-1\}$. Если это не тот случай, то требуется перевод, основанный на количестве разных знаков в алфавите A . Перевод может выполняться перед шифрованием, и вновь, после дешифрования, так что шифрование и дешифрование будет всегда выполняться по алфавитам в виде $\{0, \dots, n-1\}$ для некоторого положительного целого числа n , больше 1.

[0089] Алгоритм шифрования с сохранением формата может использовать режим Счетчика (CTR), как определено в SP800-38A, с блочным шифром CIPH (AES или TDEA) с размером блока b бит, и ключом K шифрования для CIPH, и последовательность блоков T_1, T_2, \dots , счетчика (именуемых счетчики в SP800-38A), для создания последовательности выходных блоков, один для каждого блока счетчика. Каждый выходной блок состоит из k цифр по основанию n , где k является конфигурируемым параметром, который должен быть выбран из интервала $\{1, \dots, \lfloor \log_n 2^b \rfloor\}$. По причинам, которые объясняются ниже, каждый блок счетчика составляет $b-7$ бит, вместо b бит, как в SP800-38A. Механизм создания выходных блоков также описывается ниже.

[0090] Чтобы зашифровать открытый текст P длиной L , при $1 \leq L$, генерируется столько выходных блоков, сколько необходимо (но не более), так что общее число цифр по основанию n в выходных блоках составляет по меньшей мере L , т.е. мы вычисляем уникальные целые числа p и r , так что $\frac{L}{k} \leq p < \frac{L}{k} + 1$ и $0 \leq r \leq k$, так что

$L = pk - r$, и генерируем выходные блоки G_1, \dots, G_p . Затем каждая цифра $P[i]$ по основанию n открытого текста складывается, по модулю n , с i -ой цифрой по основанию n из конкатенации из выходных блоков, $G_1 \| G_2 \| \dots \| G_p$, для формирования i -ой цифры зашифрованного текста:

$$[0091] \ C[i] = (P[i] + (G_1 \parallel \dots \parallel G_p)[i]) \bmod n$$

[0092] Поскольку k не может разделить L , то некоторые цифры последнего выходного блока, G_p могут быть проигнорированы. Последние r цифры по основанию n G_p не используются.

[0093] Для расшифровки зашифрованного текста C длиной L , при $1 \leq L$, генерируется столько выходных блоков, сколько необходимо (но не более), так что общее число цифр по основанию n в выходных блоках превышает L , что делается способом, аналогичным тому, что используется при шифровании. Затем из каждой цифры $C[i]$ по основанию n зашифрованного текста вычитается, по модулю n , i -ая цифра по основанию n из конкатенации из выходных блоков, $G_1 \parallel \dots \parallel G_p$, для формирования i -ой цифры открытого текста:

$$[0094] \ C[i] = (P[i] + (G_1 \parallel \dots \parallel G_p)[i]) \bmod n$$

[0095] Применительно к шифрованию с сохранением формата, как для самого режима Счетчика, последовательность блоков счетчика должна обладать свойством, при котором каждый блок в последовательности отличается от каждого другого блока. Данное условие не ограничивается единственным шифрованием: по всем сообщениям, которые шифруются при заданном ключе K , все счетчики должны быть отдельными. SP800-38A описывает способы для генерирования счетчиков.

[0096] При условии блочного шифра СРН с длиной b блока, ключа K для СРН, $b - 7$ битного счетчика T , натурального числа $n > 1$, которое является основанием открытого текста, который должен быть зашифрован, и целого числа k при $0 < k \leq \lfloor \log_n(2^b) \rfloor$, выходной блок, состоящий из k цифр по основанию n , создается следующим образом:

[0097] Начальное значение 7-битного счетчика, S , устанавливается равным 0. Затем СРН K применяется к $S \parallel T$ для создания блока B из b бит. B интерпретируется как целое число в интервале $\{0, \dots, 2^b - 1\}$, и если $B < n^k \lfloor \frac{2^b}{n^k} \rfloor$, тогда он принимается, в противном случае S увеличивается и СРН K применяется вновь к $S \parallel T$, и т.д., до тех пор, пока B не будет принят или S не станет равно 127. Если $S = 127$, возникает ошибка, в противном случае B преобразуется к основанию n и является выходным блоком с k цифрами по основанию n , возможно с ведущими нулями. В предположении, что СРН K является псевдослучайной перестановкой, вероятность на каждой итерации того, что B будет принят, составляет по меньшей мере 0,5, а вероятность того, что возникнет ошибка, составляет самое большое 2^{-128} . Представленный ниже псевдокод описывает данный алгоритм:

$i=0$

Входной_Блок = $S \parallel T$;

$\max_B = (n^k) * ((2^b) \text{div} (n^k))$;

$B = \text{СРН}(K, \text{Входной_Блок})$;

пока $((\text{AsInteger}(B) \geq \max_B) \text{ И } (i < 127))\{$

```

i=i+1
Входной_Блок=Si || T;
В=СРН(К, Входной_Блок);
};

```

```

5  если(i=127) возврат ОШИБКА;
    Выходной_Блок=Convert(В,k,n);
    Возврат Выходной_Блок;

```

10 [0098] Здесь предполагается, что S_0, S_1, \dots, S_{127} перечисляет 128 разных 7-битных комбинаций, что функция «AsInteger» берет строку из b бит $B[1], \dots, B[b]$ и преобразует ее в целое число $\sum_{i=1}^b (B[i] \cdot 2^{b-i})$, а «Convert» преобразует B в k цифр по основанию n , с ведущими нулями, при необходимости:

```

Convert(В,k,n){
M=AsInteger(В)
15  для (i=1;i≤k;i++){
D[i]=M mod n;
M=M div n;
};
возврат D;
20 }

```

[0099] Максимальное значение для L , т.е. битовая длина наиболее длинного открытого текста, который может быть зашифрован, составляет $2^{b/2}$.

25 [0100] Верхняя граница $n^k \left\lfloor \frac{2^b}{n^k} \right\rfloor$ для B , интерпретируемая в качестве целого числа,

выбирается как наибольшее возможное кратное n^k , что позволяет равномерно выделять число из k цифр по основанию n из него, предполагая однородным распределение B .

30 [0101] Фиг. 7 является блок-схемой, иллюстрирующей реализацию шифрования с сохранением формата в соответствии с вариантом осуществления. Операции, описываемые со ссылкой на Фиг. 7, могут быть выполнены, например, устройством доступа или хостом. На этапе 702 считывается PAN. PAN может считываться устройством 104 доступа из платежного устройства 102. В качестве альтернативы PAN может считываться из поля PAN сообщения запроса авторизации.

35 [0102] На этапе 704 по меньшей мере часть PAN шифруется таким образом, что длина зашифрованного PAN равна длине первоначального PAN. PAN может шифроваться устройством 104 доступа или хост-сервером 108 торговца. На этапе 706 зашифрованный PAN может быть записан в поле PAN запроса авторизации. На этапе 708 дата истечения срока действия может быть считана из поля даты истечения срока действия сообщения запроса авторизации (или из платежного устройства). На этапе 710 измененная дата истечения срока действия может быть записана в сообщение запроса авторизации. Измененная дата истечения срока действия может генерироваться посредством, например, добавления числа к части года первоначальной даты истечения срока действия. Число, добавленное к первоначальной дате истечения срока действия, может 45 быть числом между 5-99, как, например, число между 10 и 50, например 40. Следует иметь в виду, что альтернативные алгоритмы, такие как вычитание числа из первоначальной даты истечения срока действия, могут быть использованы.

[0103] Фиг. 8 является блок-схемой, иллюстрирующей интерпретацию данных для

определения того, было ли применено шифрование с сохранением формата. Операции, описанные со ссылкой на Фиг. 8, могут выполняться, например, хост-сервером 108 торговца, сетью 112-116 обработки платежей, эмитентом, эквайером и т.д. На этапе 800 принимается сообщение запроса авторизации. Например, сообщение запроса авторизации может быть принято хост-сервером 108 торговца или сетью обработки платежей. В ромбе 802 решений может определяться, является ли часть года даты срока истечения действия, считанная из поля даты истечения срока действия сообщения запроса авторизации, меньше конкретного числа лет от текущей даты, например, 20 лет от текущей даты. Если год истечения срока действия меньше 20 лет с текущей даты, то отсутствует сигнал для шифрования с сохранением формата в сообщении запроса авторизации, как указывается на этапе 804. Если дата истечения срока действия находится дальше 20 лет от текущей даты, то незашифрованные данные PAN могут быть считаны из поля PAN, как указывается на этапе 806. Незашифрованные данные PAN могут быть использованы для маршрутизации (например, посредством хост-сервера 108 торговца), обнаружения мошенничества, определения авторизации или иных целей.

КОМПЬЮТЕРНАЯ СИСТЕМА

[0104] Фиг. 9 является иллюстративной высокоуровневой структурной схемой компьютерной системы, которая может быть использована для реализации любого из объектов или компонентов описанных выше (например, устройства доступа, хоста, сети обработки платежей, процессора эквайера, и т.д.). Подсистемы, показанные на Фиг. 9, взаимосвязаны через системную шину 902. Дополнительные подсистемы, такие как принтер 904, клавиатура 906, несъемный диск 908, и монитор 910 связаны с адаптером 912 дисплея. Периферийные устройства и устройства ввода/вывода (I/O), которые связаны с контроллером 914 I/O, могут быть соединены с компьютерной системой посредством любого количества средств, известных в соответствующей области техники, таких как последовательный порт 916. Например, последовательный порт 916 или внешний интерфейс 918 может быть использован для соединения компьютерного устройства с глобальной сетью, такой как Интернет, устройством ввода типа мышь, или сканером. Обеспечение взаимосвязи через системную шину 902 позволяет центральному процессору 920 осуществлять связь с каждой подсистемой и управлять исполнением инструкций из системной памяти 922 или фиксированного диска 908, как, впрочем, и осуществлять обмен информацией между подсистемами. Системная память 922 и/или фиксированный диск 908 могут воплощать машиночитаемый носитель информации.

[0105] Как описано, изобретательский сервис может задействовать реализацию одной или более функций, процессов, операций или этапов способа. В некоторых вариантах осуществления функции, процессы, операции или этапы способа могут быть реализованы в результате исполнения набора инструкций или кода программного обеспечения посредством приемлемым образом запрограммированного вычислительного устройства, микропроцессора, процессора данных или подобного. Набор инструкций или код программного обеспечения может храниться в памяти или другом виде элемента хранения данных, доступ к которому может быть получен посредством вычислительного устройства, микропроцессора и т.д. В других вариантах осуществления, функции, процессы, операции или этапы способа могут быть реализованы посредством встроенного программного обеспечения или выделенного процессора, интегральной микросхемы и т.д.

[0106] Следует понимать, что настоящее изобретение, как описано выше, может быть реализовано в виде логики управления, использующей компьютерное программное

обеспечение в модульном или комплексном виде. На основании предоставленного в данном документе раскрытия и идей специалисту в соответствующей области станут известны и понятны другие варианты и/или способы для реализации настоящего изобретения, используя аппаратное обеспечение и сочетание аппаратного обеспечения

5 и программного обеспечения.
 [0107] Любой из компонентов или функций программного обеспечения, описанного в данной заявке, может быть реализован в качестве кода программного обеспечения, который должен исполняться процессором, используя любой приемлемый компьютерный язык, такой как, например, Java, C++ или Perl, используя, например, 10 традиционные или объектно-ориентированные методики. Код программного обеспечения может быть сохранен в качестве ряда инструкций или команд на машиночитаемом носителе информации, таком как оперативное запоминающее устройство (RAM), постоянное запоминающее устройство (ROM), магнитный носитель информации, такой как жесткий диск или гибкий диск, или оптический носитель информации, такой как CD-ROM. Любой такой машиночитаемый носитель информации 15 может размещаться в или внутри одного вычислительного устройства и может быть представлен на или в разных вычислительных устройствах в системе или сети.

[0108] Несмотря на то, что примерные варианты осуществления были подробно описаны и показаны на сопроводительных чертежах, следует понимать, что такие 20 варианты осуществления являются лишь иллюстративными и не предназначены ограничивать более широкое изобретение и что данное изобретение не должно ограничиваться конкретными показанными и описанными компоновками и конструкциями, поскольку различные другие модификации могут быть очевидны специалистам в соответствующей области.

25 [0109] Используемые в данном документе формы единственного числа означают «по меньшей мере один» до тех пор, пока конкретно не указано обратное.

(57) Формула изобретения

1. Способ защиты данных, ассоциированных с транзакцией, содержащий этапы, на 30 которых:

принимают посредством устройства доступа личный идентификационный номер (PIN) и уязвимые данные, включающие в себя идентификатор счета;

шифруют посредством устройства доступа PIN, при этом шифрование PIN использует первый вариант ключа шифрования, основанный на исходном ключе;

35 шифруют посредством устройства доступа уязвимые данные, включающие в себя идентификатор счета, при этом зашифрованный идентификатор счета имеет тот же формат, что и идентификатор счета, и поднабор цифр зашифрованного идентификатора счета представляет собой зашифрованные цифры идентификатора счета;

40 записывают зашифрованный идентификатор счета в поле сообщения запроса авторизации, причем поле предназначено для приема идентификатора счета;

используют элемент данных сообщения запроса авторизации в качестве сигнала для идентификации наличия зашифрованного идентификатора счета в сообщении запроса авторизации; и

45 передают хост-серверу сообщение запроса авторизации, включающее в себя зашифрованный PIN и зашифрованные уязвимые данные.

2. Способ по п. 1, в котором исходный ключ генерируется посредством схемы управления ключами с извлекаемым уникальным ключом для каждой транзакции (DUKPT).

3. Способ по п. 1, в котором по меньшей мере одно из следующего: PIN и уязвимые данные, шифруются, используя Алгоритм Шифрования Трехкратного DES (TDEA).

4. Способ по п. 1, в котором уязвимые данные дополнительно включают в себя по меньшей мере одно из следующего: имя держателя карты, адрес держателя карты, и дискреционные данные.

5. Способ по п. 1, в котором поднабор дискреционных данных остается незашифрованным, когда дискреционные данные включаются в зашифрованные уязвимые данные.

6. Способ по п. 1, в котором шифрование уязвимых данных включает в себя шифрование, используя второй вариант ключа шифрования, основанный на исходном ключе.

7. Способ по п. 6, в котором идентификатор счета представляет собой личный номер счета.

8. Способ по п. 6, в котором поле даты истечения срока действия сообщения запроса авторизации переписывается на измененную дату истечения срока действия, для указания того, что сообщение запроса авторизации содержит зашифрованный идентификатор счета.

9. Способ по п. 1, в котором устройство доступа является терминалом точки продаж.

10. Способ по п. 1, в котором устройство доступа принимает информацию, ассоциированную с транзакцией электронной коммерции.

11. Способ защиты данных, ассоциированных с транзакцией, содержащий этапы, на которых:

принимают посредством хост-сервера сообщение запроса авторизации, при этом сообщение запроса авторизации включает в себя зашифрованные уязвимые данные;

25 дешифруют посредством модуля безопасности, соединенного с возможностью осуществления связи с сервером торговца, зашифрованные уязвимые данные;

повторно шифруют посредством модуля безопасности дешифрованные уязвимые данные, при этом повторное шифрование уязвимых данных использует первый ключ шифрования зоны уязвимых данных, ассоциированный с первой сетью обработки

30 платежей; и

передают посредством хост-сервера первое переведенное сообщение запроса авторизации первой сети обработки платежей, при этом переведенное сообщение запроса авторизации включает в себя повторно зашифрованные уязвимые данные.

12. Способ по п. 11, в котором сообщение запроса авторизации дополнительно включает в себя зашифрованный PIN, причем способ дополнительно содержит этапы, на которых:

дешифруют посредством модуля безопасности зашифрованный PIN; и

повторно шифруют посредством модуля безопасности дешифрованный PIN, при этом повторное шифрование PIN использует первый ключ шифрования зоны PIN,

40 ассоциированный с первой сетью обработки платежей; и

при этом первое переведенное сообщение запроса авторизации включает в себя повторно зашифрованный PIN.

13. Способ по п. 12, в котором модуль безопасности выполнен с возможностью передачи второго переведенного сообщения запроса авторизации второй сети обработки платежей, при этом второй ключ шифрования зоны PIN используется для повторного шифрования PIN для второго переведенного сообщения запроса авторизации и второй ключ шифрования зоны уязвимых данных используется для повторного шифрования уязвимых данных для второго сообщения запроса авторизации.

14. Способ по п. 11, в котором зашифрованный PIN шифруется, используя первый вариант ключа шифрования, основанный на исходном ключе, а зашифрованные уязвимые данные шифруются, используя второй вариант ключа шифрования, основанный на исходном ключе.

5 15. Способ по п. 14, в котором исходный ключ генерируется посредством схемы управления ключами с извлекаемым уникальным ключом для каждой транзакции (DUKPT).

16. Способ по п. 11, в котором устройство безопасности является модулем безопасности с защитой от вмешательства.

10 17. Способ по п. 11, в котором устройство безопасности является модулем безопасности аппаратного обеспечения.

18. Способ по п. 11, в котором уязвимые данные дополнительно включают в себя по меньшей мере одно из следующего: имя держателя карты, адрес держателя карты, и дискреционные данные.

15 19. Система защиты данных, ассоциированных с транзакцией, содержащая: процессор; и

машиночитаемый носитель информации, связанный с процессором, при этом машиночитаемый носитель информации содержит код, исполняемый процессором для реализации способа маршрутизации транзакций, причем способ содержит этапы, на

20 которых:

шифруют посредством устройства доступа личный идентификационный номер (PIN), при этом шифрование PIN использует первый вариант ключа шифрования, основанный на исходном ключе;

25 шифруют посредством устройства доступа уязвимые данные, включающие в себя идентификатор счета, при этом зашифрованный идентификатор счета имеет тот же формат, что и идентификатор счета, и поднабор цифр зашифрованного идентификатора счета представляет собой зашифрованные цифры идентификатора счета;

записывают зашифрованный идентификатор счета в поле сообщения запроса авторизации, причем поле предназначено для приема идентификатора счета;

30 используют элемент данных сообщения запроса авторизации в качестве сигнала для идентификации наличия зашифрованного идентификатора счета в сообщении запроса авторизации; и

передают хост-серверу сообщение запроса авторизации, включающее в себя зашифрованный PIN и зашифрованные уязвимые данные.

35 20. Система по п. 19, в которой процессор является криптопроцессором безопасности.

21. Система по п. 19, при этом система включает в себя модуль безопасности с защитой от вмешательства.

22. Система защиты данных, ассоциированных с транзакцией, содержащая: процессор; и

40 машиночитаемый носитель информации, связанный с процессором, при этом машиночитаемый носитель информации содержит код, исполняемый процессором для реализации способа, содержащего этапы, на которых:

принимают посредством хост-сервера сообщение запроса авторизации, при этом сообщение запроса авторизации включает в себя зашифрованные уязвимые данные;

45 дешифруют посредством модуля безопасности, соединенного с возможностью осуществления связи с сервером торговца, зашифрованные уязвимые данные;

повторно шифруют посредством модуля безопасности дешифрованные уязвимые данные, при этом повторное шифрование уязвимых данных использует первый ключ

шифрования зоны уязвимых данных, ассоциированный с первой сетью обработки платежей; и

передают посредством хост-сервера первое переведенное сообщение запроса авторизации первой сети обработки платежей, при этом переведенное сообщение запроса авторизации включает в себя повторно зашифрованные уязвимые данные.

23. Система по п. 22, в которой сообщение запроса авторизации дополнительно включает в себя зашифрованный PIN, причем машиночитаемый носитель информации дополнительно содержит код, исполняемый процессором для реализации способа, содержащего этапы, на которых:

дешифруют посредством модуля безопасности зашифрованный PIN; и

повторно шифруют посредством модуля безопасности дешифрованный PIN, при этом повторное шифрование PIN использует первый ключ шифрования зоны PIN, ассоциированный с первой сетью обработки платежей; и

при этом первое переведенное сообщение запроса авторизации включает в себя повторно зашифрованный PIN.

24. Система по п. 22, в которой модуль безопасности выполнен с возможностью передачи второго переведенного сообщения запроса авторизации второй сети обработки платежей, при этом второй ключ шифрования зоны PIN используется для повторного шифрования PIN для второго переведенного сообщения запроса авторизации и второй ключ шифрования зоны уязвимых данных используется для повторного шифрования уязвимых данных для второго сообщения запроса авторизации.

25. Система по п. 22, в которой процессор является криптопроцессором безопасности.

26. Система по п. 22, при этом система включает в себя модуль безопасности с защитой от вмешательства.

27. Система по п. 22, при этом система включает в себя модуль безопасности аппаратного обеспечения.

28. Способ защиты данных, ассоциированных с транзакцией, содержащий этапы, на которых:

принимают данные, ассоциированные с идентификатором личного счета (PAI);

шифруют посредством устройства доступа PAI, при этом зашифрованный PAI имеет тот же формат, что и у PAI;

записывают зашифрованный PAI в поле сообщения запроса авторизации, при этом поле предназначено для приема PAI, причем PAI является первичным номером счета (PAN), и поднабор цифр зашифрованного PAN в сообщении запроса авторизации представляет собой зашифрованные цифры PAN;

используют элемент данных сообщения запроса авторизации в качестве сигнала для идентификации наличия зашифрованного PAI в сообщении запроса авторизации; и передают сообщение запроса авторизации.

29. Способ по п. 28, в котором первые шесть цифр зашифрованного PAN являются точно такими же, что и первые шесть цифр незашифрованного PAN, и при этом последние четыре цифры зашифрованного PAN являются точно такими же, что и последние шесть цифр незашифрованного PAN.

30. Способ по п. 28, дополнительно содержащий этап, на котором вычисляют значение для назначенной цифры зашифрованного PAN таким образом, что последняя цифра незашифрованного PAN точно такая же, что и последняя цифра зашифрованного PAN, и при этом последняя цифра зашифрованного PAN является действительной контрольной цифрой для зашифрованного PAN.

31. Способ по п. 30, в котором назначенная цифра является двенадцатой цифрой

зашифрованного PAN.

32. Способ по п. 28, в котором сообщение запроса авторизации включает в себя дату истечения срока действия, и при этом поле даты истечения срока действия сообщения запроса авторизации переписывается на измененную дату истечения срока действия,
5 когда поле PAI сообщения запроса авторизации содержит зашифрованный PAI.

10

15

20

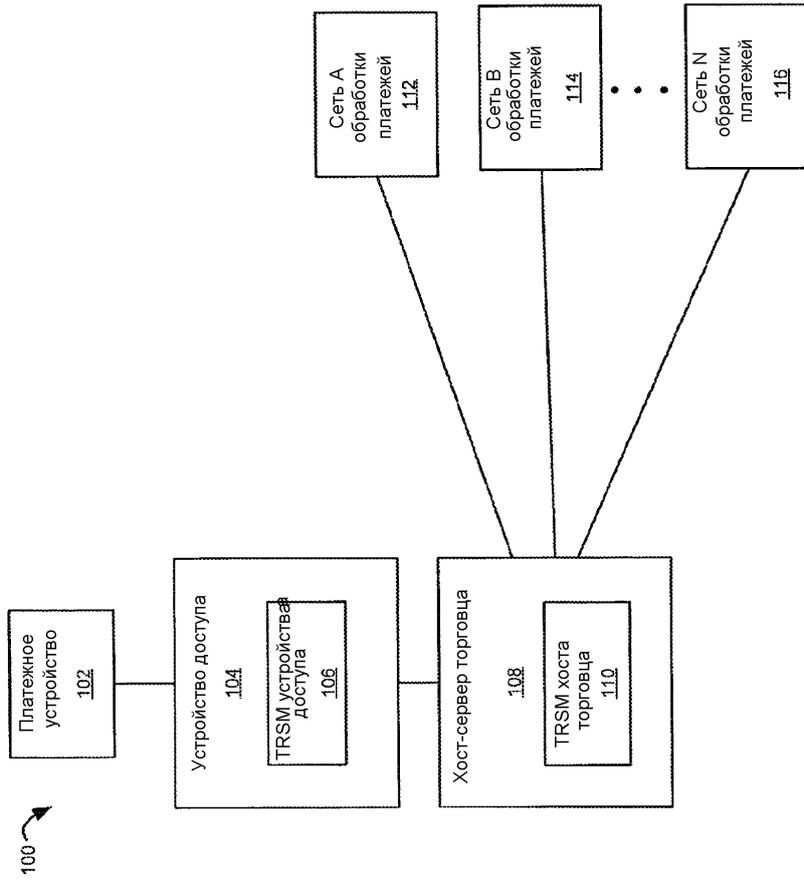
25

30

35

40

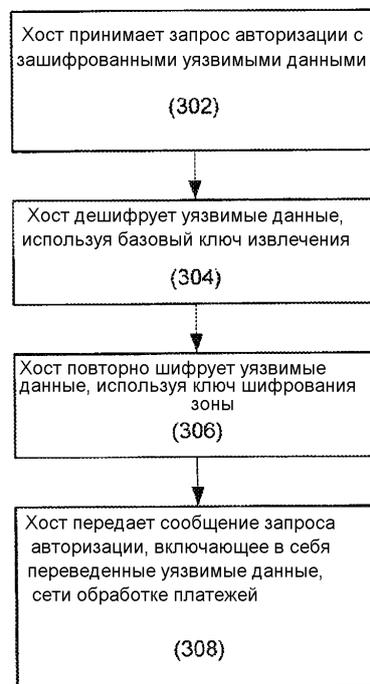
45



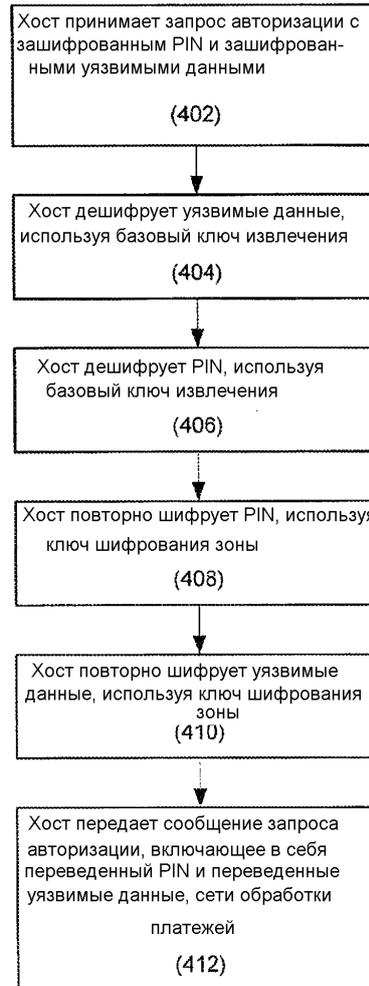
ФИГ.1



ФИГ.2



ФИГ.3



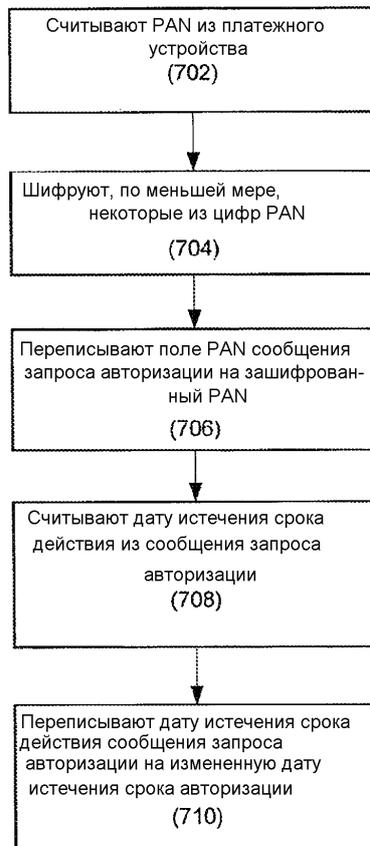
ФИГ.4

Символ	Описание	Код знака/ № знаков
STX	Начальная граничная метка	%
FC	Код формата	В
PAN	Первичный Номер Счета	Вплоть до 19 цифр
FS	Разделитель	^
NM	Имя	От 2 до 26 знаков
FS	Разделитель	^
ED	Дата истечения срока действия	Четыре цифры или ^
SC	Служебный код	Три цифры или ^
DD	Дискреционные данные	Остаток знаков
ETX	Конечная граничная метка	?
LRC	Продольный контроль избыточным кодом (смотри ISO/IEC 7811-2)	1 знак
	Максимальная длина записи	79 буквенно-цифровых знаков

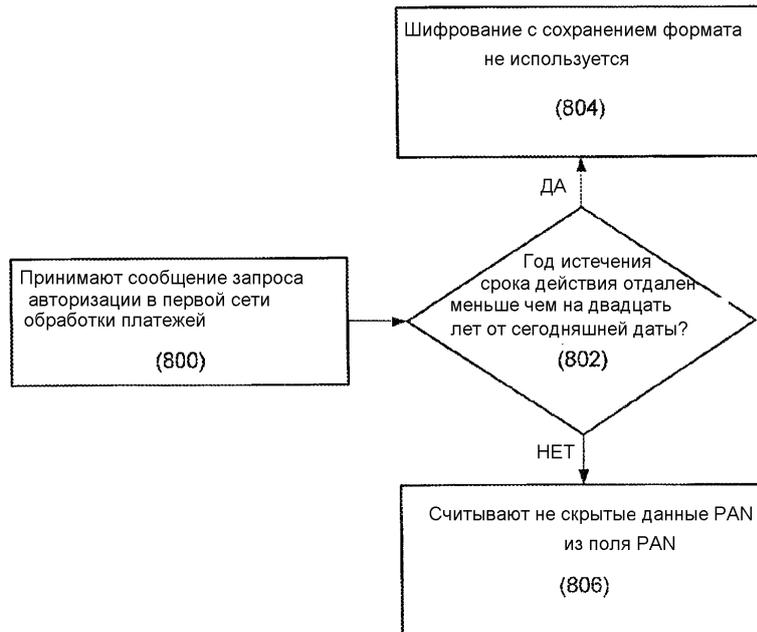
ФИГ.5

Символ	Описание	Код знака/ № знаков
STX	Начальная граничная метка	:
PAN	Первичный Номер Счета	Вплоть до 19 цифр
FS	Разделитель	=
ED	Дата истечения срока действия	Четыре цифры или =
SC	Служебный код	Три цифры или =
DD	Дискреционные данные	Остаток доступных цифр
ETX	Конечная граничная метка	?
LRC	Продольный контроль избыточным кодом (смотри ISO/IEC 7811-2)	1 знак
	Максимальная длина записи	40 цифровых знаков

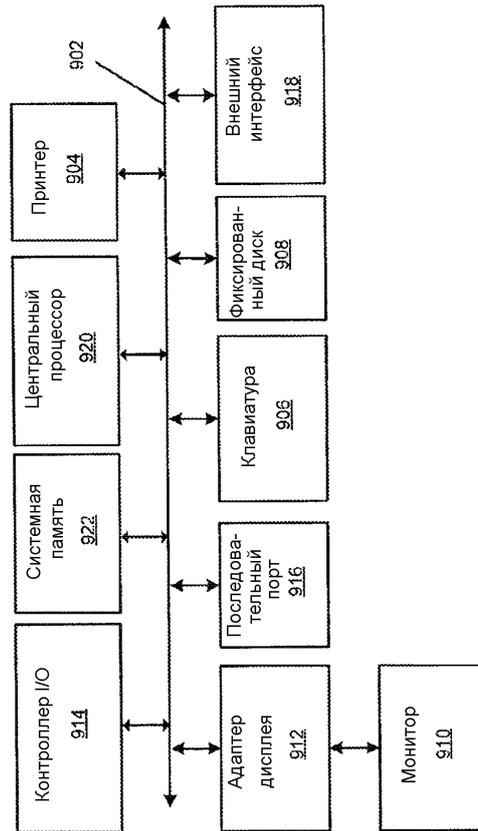
ФИГ.6



ФИГ.7



ФИГ.8



ФИГ.9