Предшествующий уровень техники

Изобретение относится к способу дебетования электронного платежного средства, например электронной платежной карты, содержащей интегральную схему ("чип-карты"). В частности, хотя не исключительно, изобретение относится к способу защищенного дебетования предварительно оплаченных электронных платежных карт ("предоплаченных карт"), применяемых, например, в уличных телефонах. В настоящем описании термин "платежные средства" будет использоваться независимо от формы или типа конкретных платежных средств. Поэтому платежные средства могут быть выполнены, например, в виде возобновляемой платежной карты или электронных платежных средств, имеющих форму, отличную от карты.

В последние годы электронные платежные средства используются все шире и не только для оплаты разговора по телефонам общественного пользования, но также и для многих других видов платежей. Так как такие платежные средства обычно включают (кредитный) баланс, который представляет собой денежную величину, необходимо осуществлять обмен данными между такими платежными средствами и пунктом оплаты (например, телефонным аппаратом, предназначенным для электронной оплаты, или электронным кассовым аппаратом) в соответствии с защищенным способом (протоколом оплаты). То есть нужно проверить, например, что некая сумма (денег или расчетных единиц), снимаемая с платежного средства, соответствует количеству (денег или расчетных единиц), кредитованных в других местах, и сумма, оплаченная клиентом, должна соответствовать сумме, которая будет получена поставщиком. Кредитованная сумма может быть записана, например, в защищенном модуле, имеющемся в пункте оплаты.

Известные способы оплаты, раскрытые, например, в заявке ЕР 0637004, включают первый шаг, на котором баланс платежного средства извлекают из памяти с помощью пункта оплаты; второй шаг, на котором баланс платежного средства понижают (дебетование платежного средства); и третий шаг, на котором баланс платежного средства извлекают из памяти снова. По разности между балансами на первом и третьем шагах может быть определена дебетованная сумма и этой же суммой кредитуется пункт оплаты. Второй шаг может быть повторен несколько раз, возможно вместе с третьим шагом.

Чтобы предотвратить мошенничество, на первом шаге используется случайное число, которое генерируется пунктом оплаты и передается в платежное средство, например, как часть кода, с помощью которого находят баланс. На основе первого случайного числа платежное средство в качестве первого отклика генерирует аутентификационный код, который может включать, среди прочего, преобразованные (например, криптографически) указанное случайное число и баланс. При использовании различных случайных чисел для каждой транзакции предотвращается имитация транзакции с помощью ответа. Кроме того, на третьем шаге используется второе случайное число, которое также генерируется пунктом оплаты и передается в платежное средство. На основе второго случайного числа платежное средство в качестве второго отклика генерирует второй, новый, аутентификационный код, который может включать, среди прочего, преобразованные второе случайное число и новый баланс. На основе различия между двумя переданными балансами пункт оплаты (или, в некоторых случаях, защищенный модуль пункта оплаты) определяет, на какую сумму нужно кредитовать баланс пункта оплаты.

Указанный известный способ в основном успешно противостоит мошенничеству, пока платежное средство связано с одним пунктом оплаты (или защищенным модулем). Недостаток известного способа, однако, заключается в том, что первый и второй аутентификационные коды являются независимыми. Если второй или третий пункт оплаты (или защищенный модуль) связывается с платежным средством, то вследствие указанной независимости можно отделить первый шаг от второго и третьего шагов. В результате полная на вид транзакция может быть произведена без дебетования платежных средств, о которых идет речь, на ту же самую сумму, на которую кредитуется пункт оплаты (или защищенный модуль) в целом. Понятно, что это нежелательно.

В патенте США № 5495098 и заявке ЕР 0621570 раскрыт способ, в котором для обеспечения обмена данных только между картой и терминалом используется идентификация модуля безопасности в пункте оплаты. Защита обмена данными между модулем безопасности, пунктом оплаты и картой является относительно сложной и требует большого объема криптографических вычислений.

Другие известные способы раскрыты, например, в заявках ЕР 0223213 и ЕР 0570924, но и они не предлагают решения вышеупомянутых проблем.

Сущность изобретения

Целью изобретения является устранение вышеупомянутых и других недостатков известных способов и создание способа, который предлагает еще большую степень защиты транзакций дебетования. В частности, целью изобретения является создание способа, который гарантирует, что в течение транзакции имеет место связь только между платежным средством и одним пунктом оплаты или защищенным модулем. Более конкретно, целью изобретения является создание способа, который гарантирует, что сумма, на которую уменьшен баланс

платежного средства в течение транзакции, соответствует сумме, на которую увеличен баланс только одного пункта оплаты или защищенного модуля.

Соответственно, настоящее изобретение обеспечивает способ выполнения транзакции с использованием платежного средства и пункта оплаты, причем этот способ включает повторное выполнение шага опроса, на котором пункт оплаты опрашивает платежное средство и получает в ответ из платежного средства данные, содержащие аутентификационный код, выработанный в результате заранее заданного процесса, причем последующий аутентификационный код связан с предшествующим аутентификационным кодом той же самой транзакции с помощью аутентификационной величины, выработанной как в платежном средстве, так и в пункте оплаты. За счет связи аутентификационных кодов с помощью аутентификационных величин, можно отличить аутентификационные коды исходной транзакции от аутентификационных кодов посторонней транзакции. Предпочтительно, аутентификационную величину изменяют на каждом шаге опроса, таким образом обеспечивая повышенную безопасность.

Более конкретно, настоящее изобретение обеспечивает способ защищенного выполнения транзакции с использованием электронного платежного средства и пункта оплаты, включающий

начальный шаг, на котором

- пункт оплаты передает в платежное средство первое случайное число,

- в ответ на первое случайное число платежное средство передает в пункт оплаты первый аутентификационный код, который определен на основе, по меньшей мере, первого случайного числа и первой аутентификационной величины, и

- пункт (12) оплаты проверяет первый аутентификационный код (MAC1),

промежуточный шаг, на котором

- пункт оплаты передает в платежное средство команду, и баланс платежного средства изменяется на основе этой команды, и

дальнейший шаг, на котором

- пункт (12) оплаты передает платежному средству (11) второе случайное число (R2),

- платежное средство передает в пункт оплаты второй аутентификационный код, который определен на основе, по меньшей мере, второго случайного числа и второго аутентификационного кода, причем второй аутентификационный код определен на основе, по меньшей мере, второго случайного числа и второй аутентификационной величины, а вторая аутентификационная величина получена из первой аутентификационной величины, и

- пункт оплаты определяет вторую аутентификационную величину из первой аутентификационной величины и проверяет второй аутентификационный код.

За счет формирования аутентификационных кодов на основе, помимо прочего, взаимосвязанных аутентификационных величин, предоставляется возможность проверить, связан ли второй аутентификационный код (на третьем шаге) с первым аутентификационным кодом (на первом шаге). Поскольку теперь при генерации новой аутентификационной величины каждый раз должен быть определен аутентификационный код, имеется возможность различения последовательных аутентификационных кодов и к тому же различения аутентификационных кодов, связанных с разными транзакциями. Если каждый раз при выполнении первого или третьего шагов генерируется уникальная аутентификационная величина, то может быть достоверно определено, с каким первым аутентификационным кодом связан второй аутентификационный код. К тому же может быть также определено, генерировался ли уже второй аутентификационный код в пределах транзакции.

Аутентификационные величины в основном генерируются автономно платежными средствами. Предпочтительно, не имеется возможности влиять на этот процесс извне, чтобы предотвратить мошенничество. Аутентификационные величины могут генерироваться различными способами, например, с помощью генератора случайных чисел или счетчика.

Первая и вторая аутентификационные величины транзакции могут быть связаны тем, что имеют, например, одинаковые значения или являются взаимозависимыми величинами, например последовательными значениями счетчика. Кроме того, первая аутентификационная величина может быть случайным числом, а вторая аутентификационная величина может быть сформирована из первой добавлением к ней определенного числа. В принципе, каждая пара аутентификационных величин должна быть связана таким способом, который можно достоверно проверить.

Еще одной целью изобретения является создание электронного платежного средства и пункта оплаты, в которых использован описанный способ.

Краткое описание чертежей

Изобретение будет описано подробнее со ссылками на чертежи, где

на фиг. 1 схематично показана система оплаты, в которой может применяться изобретение;

на фиг. 2 схематично иллюстрируется способ, в котором используется изобретение;

на фиг. 3 схематично показана выработка аутентификационного кода, используемого в способе, иллюстрируемом на фиг. 2;

на фиг. 4 схематично иллюстрируется альтернативный вариант способа, показанного на фиг. 3;

на фиг. 5 схематично показана интегральная схема платежного средства, которое может использоваться в изобретении.

Предпочтительные варианты выполнения изобретения

Система 10 электронной оплаты, показанная на фиг. 1 в качестве примера, включает электронное платежное средство, например, так называемую "чип-карту" или интеллектуальную карту ("смарт-карту") 11, пункт 12 оплаты, первое финансовое учреждение 13 и второе финансовое учреждение 14. Пункт 12 оплаты (терминал) показан на фиг. 1 в виде кассового аппарата, но он может также включать, например, телефон (общего пользования). Оба финансовых учреждения 13 и 14 обозначены на фиг. 1 как банки, но они могут быть не только банками, но и другими учреждениями, имеющими в своем распоряжении средства (компьютеры) для осуществления платежей. На практике финансовые учреждения 13 и 14 могут представлять собой одно финансовое учреждение. В показанном примере платежное средство 11 содержит подложку и интегральную схему с контактами 15, которая предназначена для обработки транзакций (оплаты). Платежное средство может также содержать электронный бумажник.

В течение транзакции между платежным средством 11 и пунктом 12 оплаты имеет место обмен платежными данными PD1. Платежное средство 11 связано с финансовым учреждением 13, в то время как пункт 12 оплаты - с финансовым учреждением 14. Между финансовыми учреждениями 13 и 14 после транзакции происходит расчет путем обмена платежными данными PD2, которые получены из платежных данных PD1. В течение транзакции в принципе отсутствует связь между пунктом 12 оплаты и соответствующим финансовым учреждением 14 (так называемая автономная система). Поэтому транзакции должны происходить управляемо для предотвращения злоупотребления системой. Таким злоупотреблением может быть, например, увеличение баланса платежного средства 11, которое не согласовано с изменением баланса соответствующего счета в финансовом учреждении 13.

На диаграмме, изображенной на фиг. 2, показан обмен данными между платежным средством (его интегральной схемой), обозначенным как "Карта" (позиция 11 на фиг. 1) и пунктом оплаты (его модулем безопасности), обозначенным как "Терминал" (позиция 12 на фиг. 1), причем последовательные события показаны одно под другим.

На первом шаге, обозначенном I, терминал (пункт оплаты) вырабатывает первое случайное число R1 и передает его в карту (платежное средство) (подшаг 1а). На практике случайное число R1 может быть частью кода для нахождения аутентификационного кода. Согласно изобретению, карта и терминал вырабатывают первую аутентификационную величину A1, например, увеличивая значение счетчика, активизируя генератор случайных чисел или обоими этими способами. На основе случайного числа R1 первой аутентификационной величины A1 и других данных, включающих баланс S1 платежного средства, карта вырабатывает аутентификационный код MAC1 = F(R1, A1, S1, ...), где F может быть известной криптографической функцией (подшаг 1б). Данные S1 и A1 из карты, а также аутентификационный код MAC1 передают в терминал (подшаг 1в). Терминал проверяет аутентификационный код на основе, в частности, R1, S1 и A1 и, в случае положительного результата проверки, записывает баланс S1.

Следует отметить, что передача величины A1 в терминал не существенна для настоящего изобретения, но служит дополнительной защитой против мошенничества.

На втором шаге, обозначенном II, терминал вырабатывает команду D дебетования, которая содержит величину (сумму), на которую должно быть дебетовано платежное средство. Команда D дебетования передается в карту, после чего баланс S1 карты уменьшается на сумму дебетования до баланса S2. Шаг II может быть повторен несколько раз.

На третьем шаге, обозначенном III, терминал вырабатывает второе случайное число R2 и передает его в карту (подшаг IIIа). Карта вырабатывает вторую аутентификационную величину A2. На основе случайного числа R2, второй аутентификационной величины A2 и других данных, включая новый баланс S2 карты, эта карта вырабатывает (подшаг IIIб) аутентификационный код MAC2 = F(R2, S2, ...), где F может быть известной криптографической функцией. Баланс S2 карты, аутентификационная величина A2 и аутентификационный код MAC1 передаются (подшаг IIIв) в терминал. Таким образом, третий шаг может проходить полностью аналогично первому шагу.

Терминал проверяет принятый второй аутентификационный код MAC2, например, воспроизводя аутентификационный код и сравнивая случайное число R2. Кроме того, терминал проверяет, равна ли принятая вторая аутентификационная величина A2 соответствующей величине, выработанной в терминале. Если аутентификационные величины A2 не равны, транзакцию прекращают и, следовательно, баланс в терминале не изменяется.

Если проверка аутентификационного кода MAC2 дала положительный результат, терминал записывает баланс S2. Вместо воспроизведения аутентификационных кодов MAC1 и MAC2, может иметь место расшифровка, например, путем выполнения функции, обратной функции F.

На четвертом шаге, обозначенном IV, в терминале определяют разность балансов S1 и S2 и записывают ее в терминал. Такую разность

можно запомнить независимо или добавить к существующей величине (балансу в терминале) для последующего осуществления платежа. Указанный четвертый шаг, также как и возможные последующие шаги, не существенен для изобретения. Шагам, показанным на фиг. 2, могут предшествовать шаги аутентификации или верификации, что, однако, также не существенно для настоящего изобретения.

На диаграмме, обсуждаемой выше, случайные числа R1 и R2 различны. Однако случайные числа R1 и R2 могут быть и равны (R1=R2=R), поэтому на шаге III может быть проверено, используется ли в аутентификационном коде MAC2 все еще то же самое случайное число R (= R1).

Следует отметить, что, строго говоря, число R1, как и число R2, не обязательно должно быть случайным числом: оно служит для безошибочной идентификации аутентификационного кода MAC1 в ответ на R1 ("запрос"). Существенно только, чтобы карта не могла знать число R1.

Согласно известным способам аутентификационные величины MAC1 и MAC2 в принципе независимы. То есть если случайные числа R1 и R2 различны, то не имеется ни прямой, ни косвенной связи между кодами MAC1 и MAC2. Вследствие этой независимости, не имеется в сущности никакой гарантии, что шаги I и III осуществлены между теми же самыми картой и терминалом.

Согласно изобретению, однако, при определении второго аутентификационного кода предполагается, что аутентификационная величина непосредственно связана с аутентификационной величиной, используемой при определении первого аутентификационного кода. В результате устанавливается связь между двумя аутентификационными кодами рассматриваемой транзакции. Предпочтительно, это связь имеет простой вид (например, A2=A1+1), что допускает простую проверку.

Если, например, карта принимает (первое) случайное число R1' от второго терминала после того, как карта выдала первый аутентификационный код MAC1 в первый терминал, то карта выдает аутентификационный код MAC2. Если затем первый терминал после выдачи команды дебетования еще раз определяет аутентификационный код, то карта выдает следующий аутентификационный код MAC3, который основан, помимо прочего, на следующей аутентификационной величине A3. Терминал обнаружит, что аутентификационные коды MAC1 и MAC3 не связаны и не сможет использовать величину S3 баланса , которая входит в аутентификационный код MAC3. Аналогично, аутентификационный код MAC4, который найден вторым терминалом, не обеспечивает подтверждения подлинности и, следовательно, истинного значения баланса. Таким способом эффективно предотвращается передача измененных величин баланса нескольким терминалам.

Аутентификационные величины предпочтительно формируются в виде последовательных чисел, например, значений счетчика. Однако можно также использовать счетчик, значения которого увеличиваются через раз (каждый второй раз при генерации аутентификационной величины), так что каждый раз две последовательных аутентификационных величины равны. Следует отметить, что платежные средства могут различать первый и третий шаги, но это не обязательно.

Указанная зависимость аутентификационных величин в соответствии с изобретением гарантирует, что все шаги транзакции, при которой использован способ согласно изобретению, имеют место между тем же самым платежным средством и тем же самым терминалом.

На фиг. 3 схематично показано, как генерируется аутентификационный код MAC ("Код установления подлинности сообщения"), например, MAC1 и MAC2. В устройство 20 обработки, которое реализует функцию, обозначенную "F", поступает несколько параметров. Эта функция F может быть криптографической функцией (например, хорошо известной функцией DES (Стандарт шифрования данных Национального бюро стандартов США) или функцией хеширования - обе хорошо известны специалистам в данной области. Альтернативно, функция F может быть относительно простой комбинаторной функцией, в этом случае устройство 20 обработки может содержать сдвиговый регистр с избирательной обратной связью. Входными параметрами устройства 20 обработки и, следовательно, функции F, в примере, показанном на фиг. 3, являются случайное число R, баланс S карты, аутентификационная величина A, ключ K и вектор Q инициализации. Случайное число R соответствует, например величинам R1 и R2, переданным в карту на шагах I и III соответственно. Баланс S карты соответствует, например, балансам S1 и S2, хранимым в карте. Ключ K может быть (секретным) ключом, который предпочтительно является уникальным для конкретной карты или группы карт. Обмен идентификатором ключа с терминалом может быть произведен во время шагов аутентификации и верификации до шага I на фиг. 2.

Вектор Q инициализации, который инициализирует процесс F, может всегда иметь фиксированную величину, например нуль. Альтернативно, вектор Q зависит от остатка (заключительного состояния) функции F после предыдущего шага транзакции. Предпочтительно, в начале новой транзакции вектор Q сбрасывается в исходное состояние.

В качестве примера показано, что аутентификационная величина вырабатывается счетчиком 21. Предпочтительно, показания счетчика увеличиваются на каждом шаге опроса (напри-

мер, шаге I и шаге III), т.е. на каждом шаге, в котором аутентификационный код (MAC) вырабатывается в ответ на случайное число (R). В результате для каждого аутентификационного кода используется разная аутентификационная величина A. Поскольку инкремент (в этом случае +1, но возможны также +2 или +10) заранее задан, то терминал способен проверить на подлинность аутентификационный код. Предпочтительно, аутентификационная величина также передается и проверяется на подлинность терминалом. Счетчик 21 сбрасывается в начале новой транзакции.

В примере, изображенном на фиг. 3, аутентификационная величина A вырабатывается счетчиком. Альтернативно, счетчик 21 может быть заменен генератором случайных чисел, который вырабатывает новую аутентификационную величину A для каждого шага опроса (например шаги I и III) транзакции. В этом случае аутентификационная величина из предыдущего шага должна использоваться в качестве вектора инициализации (начального числа) генератора случайных чисел для сохранения взаимной зависимости и воспроизводимости аутентификационных величин.

Понятно, что схема, изображенная на фиг. 3, относится как к карте, так и к терминалу. Таким образом, терминал также вырабатывает аутентификационные величины A1, A2, ... и аутентификационные коды MAC1, MAC2, ... и сравнивает их с соответствующими аутентификационными кодами и величинами, принятыми от карты. Баланс (например, S2) будет принят терминалом, только если выработанный и принятый аутентификационные коды и величины равны.

На основе фиг. 4 объяснено, как способ согласно изобретению может быть применен к платежным картам.

На диаграмме фиг. 4 показана схема 100, имеющая управляющий блок 101, запоминающее устройство 102 и блок 103 ввода/вывода, которые соединены между собой. Управляющий блок может быть, например, микропроцессором или микроконтроллером. Запоминающее устройство 102 может содержать оперативное запоминающее устройство с произвольной выборкой или постоянное запоминающее устройство. Запоминающее устройство 102 предпочтительно содержит электрически программируемое постоянное запоминающее устройство с возможностью перезаписи.

Согласно изобретению схема 100 содержит также дополнительное запоминающее устройство 105 для хранения аутентификационных величин. Как показано на фиг. 4, указанное запоминающее устройство 105 может быть выполнено в виде отдельного блока, но может также быть частью запоминающего устройства 102 и, например, занимать несколько ячеек памяти запоминающего устройства 102.

Предпочтительно, запоминающее устройство 105 выполнено в виде схемы счетчика. Альтернативно, может быть использована отдельная схема счетчика, как показано на фиг. 3.

В предпочтительном варианте выполнения изобретения последовательные аутентификационные величины сформированы последовательными значениями счетчика. Первая аутентификационная величина A1, которая используется для формирования аутентификационного кода MAC1, соответствует значению счетчика, которое записано в запоминающем устройстве 105. После второго шага (см. также фиг. 2) значение счетчика увеличивается на единицу. Начальное значение счетчика может быть вообще случайным, но может также быть сброшено в заранее заданное значение, например нуль.

Выработка аутентификационных величин происходит автономно, т.е. без (возможного) влияния извне. В результате защита от мошенничества еще более увеличивается.

Понятно, что вместо того, чтобы каждый раз увеличивать значение счетчика на единицу, его можно каждый раз уменьшать на единицу. Аналогично, значение счетчика может каждый раз увеличиваться или уменьшаться больше, чем на единицу, например на два или четыре. Также можно выполнить схему 100 так, чтобы аутентификационная величина (величины) не менялась во время транзакции, а менялась только между транзакциями. В таком случае, конечно, пункт оплаты должен быть сконструирован соответственно.

Пункт оплаты для использования согласно изобретению содержит средства (например, устройство считывания карты) связи с платежным средством, средства выполнения аутентификации (например, процессор) и средства записи величин баланса (например, полупроводниковую память). Пункт оплаты организован так, что аутентификация, завершившаяся неудачей, делает невозможной запись нового значения баланса. Аутентификация согласно изобретению включает также аутентификационные величины. Операции способа согласно изобретению могут быть реализованы как аппаратным путем (с помощью специализированной микросхемы, например матрицы ASIC), так и с помощью программного обеспечения (соответствующей программы для процессора).

Специалистам в данной области понятно, что изобретение не ограничено рассмотренными вариантами его выполнения и возможно много модификаций и изменений в объеме изобретения. Так, например, принцип изобретения описан выше на основе дебетования платежных средств, но такой же принцип может быть применен к кредитованию платежных средств.

ФОРМУЛА ИЗОБРЕТЕНИЯ

1. Способ защищенного выполнения транзакции с использованием электронного платежного средства (11) и пункта (12) оплаты, согласно которому выполняют начальный шаг (I), на котором

с помощью пункта (12) оплаты передают в платежное средство (11) первое случайное число (R1),

в ответ на первое случайное число (R1) с помощью платежного средства (11) передают в пункт (12) оплаты первый аутентификационный код (MAC1), который определен на основе, по меньшей мере, первого случайного числа (R1) и первой аутентификационной величины (A1), и

с помощью пункта (12) оплаты проверяют первый аутентификационный код (MAC1) и выполняют дальнейший шаг (III), на котором

с помощью пункта (12) оплаты передают платежному средству (11) второе случайное число (R2),

с помощью платежного средства (11) передают в пункт (12) оплаты второй аутентификационный код (MAC2), который определен на основе, по меньшей мере, второго случайного числа (R2) и второй аутентификационной величины (A2), причем вторая аутентификационная величина (A2) основывается на первой аутентификационной величине (A1), и

с помощью пункта (12) оплаты получают вторую аутентификационную величину (A2) из первой аутентификационной величины (A1) и проверяют второй аутентификационный код (MAC2).

2. Способ по п.1, отличающийся тем, что первая и вторая аутентификационные величины (A1, A2) идентичны.

3. Способ по п.2, отличающийся тем, что первая и вторая аутентификационные величины (A1, A2) содержат последовательные значения счетчика.

4. Способ по п.1, отличающийся тем, что аутентификационная величина (например, A2) каждый раз формируется на основе случайного числа (например, R2) и предыдущей аутентификационной величины (A1).

5. Способ по любому из пп.1-4, отличающийся тем, что выполняют промежуточный шаг (II), на котором с помощью пункта (12) оплаты передают команду (D) в платежное средство (11) и баланс платежного средства (11) изменяют на основе команды (D).

6. Способ по любому из пп.1-5, отличающийся тем, что первое случайное число (R1) равно второму случайному числу (R2).

7. Способ по любому из пп.1-6, отличающийся тем, что аутентификационный код (например, MAC2) определяют также на основе ключа и идентификационного кода.

8. Способ по любому из пп.1-7, отличающийся тем, что аутентификационный код (например, MAC1) определяют при помощи криптографической функции (F).

9. Способ по любому из пп.1-8, отличающийся тем, что на первом и третьем шагах (I, III) с помощью платежного средства (11) передают баланс (например, S1) в пункт (12) оплаты.

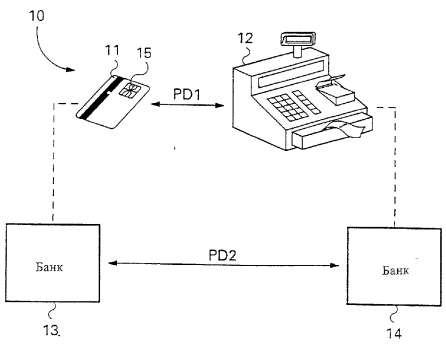
10. Способ по любому из пп.1-9, отличающийся тем, что на первом и третьем шагах (I, III) с помощью платежного средства (11) передают текущую аутентификационную величину (например, A1) в пункт (12) оплаты.

11. Способ по любому из пп.1-10, отличающийся тем, что третий шаг (III) выполняют неоднократно.

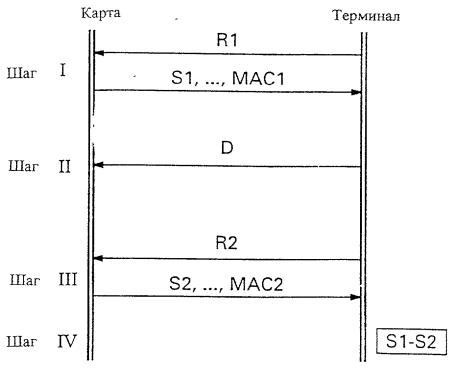
12. Способ по любому из пп.1-11, отличающийся тем, что дополнительно выполняют четвертый шаг (IV), на котором разность (S1-S2) между балансами первого и третьего шагов записывают в пункте (12) оплаты.

13. Способ по любому из пп.1-12, отличающийся тем, что пункт (12) оплаты содержит модуль для защищенной записи данных.

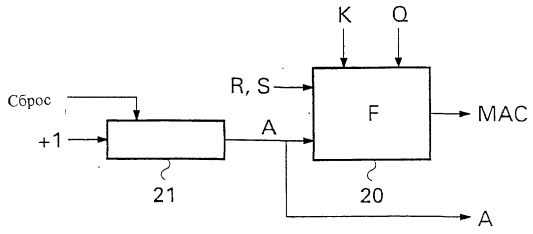
14. Способ по любому из пп.1-13, отличающийся тем, что команда (D) является командой дебетования, уменьшающей на втором шаге (II) баланс (S1) платежного средства (11).



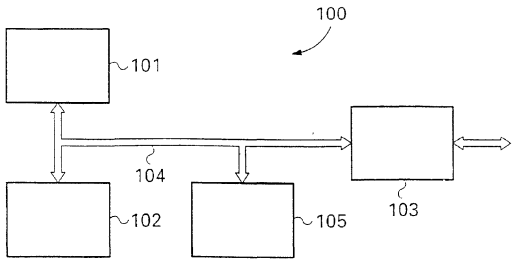
Фиг. 1



Фиг. 2



Фиг. 3



Фиг. 4