(19) Deutsches Patent- und Markenamt

(10) **DE 10 2012 112 967 B4** 2016.06.16

(12) **Patentschrift**

(21) Aktenzeichen: **10 2012 112 967.3**
(22) Anmeldetag: **21.12.2012**
(43) Offenlegungstag: **26.06.2014**
(45) Veröffentlichungstag der Patenterteilung: **16.06.2016**

(51) Int Cl.: ***G06Q 20/32*** (2012.01)

Innerhalb von neun Monaten nach Veröffentlichung der Patenterteilung kann nach § 59 Patentgesetz gegen das Patent Einspruch erhoben werden. Der Einspruch ist schriftlich zu erklären und zu begründen. Innerhalb der Einspruchsfrist ist eine Einspruchsgebühr in Höhe von 200 Euro zu entrichten (§ 6 Patentkostengesetz in Verbindung mit der Anlage zu § 2 Abs. 1 Patentkostengesetz).

(73) Patentinhaber:
SQWIN SA, Auvernier, CH

(74) Vertreter:
2K Patentanwälte Blasberg Kewitz & Reichel Partnerschaft mbB, 60325 Frankfurt, DE

(72) Erfinder:
Gulchenko, Victor, Dr., Moskau, RU

(56) Ermittelter Stand der Technik:

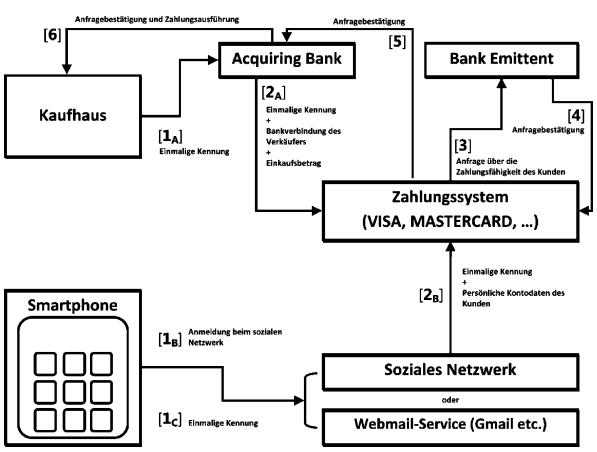
DE	**103 31 733**	**A1**
WO	**2008/ 050 132**	**A2**
WO	**2010/ 129 357**	**A2**

Handypayment. Aus: Wikipedia, der freien Enzyklopädie; Berabeitungsstand: 10.12.2012 um 16:33 Uhr; URL: https://de.wikipedia.org/w/index.php?title=Handypayment&oldid=111517156 [aberufen am 17.12.2015]

Mobile-Payment. Aus: Wikipedia, der freien Enzyklopädie; Bearbeitungsstand: 30.10.2012 um 12:37 Uhr; URL: https://de.wikipedia.org/w/index.php?title=Mobile-Payment&oldid=109904086 [abgerufen am 17.12.2015]

(54) Bezeichnung: **online Transaktionssystem**

(57) Hauptanspruch: Verfahren zur Durchführung einer digitalen Transaktion über ein mobiles Endgerät, mit einem Kassensystem, umfassend die Schritte:
– Erzeugen eines einmaligen digitalen Codes durch das Kassensystem, der die Transaktion identifiziert, wobei der einmalige digitale Code nur einmalig als Passwort verwendet werden kann, um ein mobiles Endgerät mit einem lokalen, drahtlosen Netzwerk des Kassensystems zu verbinden;
– Eingabe des digitalen Codes in das mobile Endgerät, manuell, durch Ausdrucken des digitalen Codes auf einer Quittung vom Kassensystem, um diesen dann im mobilen Endgerät einzutippen, oder automatisch durch Übertragung über NFC, Barcode, SMS, WiFi oder Bluetooth;
– Verbinden des mobilen Endgeräts mit einem lokalen, drahtlosen Netzwerk des Kassensystems, wobei aufgrund der Verbindung eine IMSI, IMEI oder MAC-Adresse des mobilen Endgerätes erlangt wird, wobei das Netzwerk das mobile Endgerät im Moment seines Anschlusses durch eine IMSI-Nummer (International Mobile Subscriber Identity) oder IMEI (International Mobile Equipment Identity) oder MAC (Media Access Control Address) identifiziert und die Daten an das Kassensystem weiterleitet, wobei das mobile Endgerät umgekehrt die IMSI, IMEI oder MAC-Adresse des Netzwerks des Verkäufers erhält;
– Übermitteln der Transaktionsdaten mit dem einmaligen digitalen Code vom Kassensystem an eine Bank/Emittent des Besitzers des Endgerätes über einen ersten digitalen Netzwerkpfad, wobei sowohl die IMSI, IMEI oder MAC-Adresse des mobilen Endgerätes als auch die in die IMSI, IMEI oder MAC-Adresse des Netzwerks des Verkäufers in die Transaktionsdaten einfließen;
– paralleles Übermitteln des digitalen Codes, der Kontoinformationen und der IMSI, IMEI oder MAC-Adresse des Netzwerks des Verkäufers, ausgelöst durch das ...



Beschreibung

Gebiet der Erfindung:

[0001] Ein Finanztransaktionssystem ist ein computergestütztes Anwendungssystem, mit der überwiegend bargeldlose Transaktionen durchgeführt werden. I. d. R. basieren diese Systeme auf Datenbanksystemen, mit denen Transaktionen ausgeführt werden. Für die ordnungsgemäße Ausführung einer Transaktion bestehen Schutzmaßnahmen, die gewährleisten, dass eine Datenbank stets einen korrekten Zustand aufweist. Im mobilen payment bzw. Zahlungsverkehr ist es wichtig die Identität des Zahlenden festzustellen und einen Missbrauch zu vermeiden. Die WO 2008/050132 A2 zeigt ein Verfahren, bei dem die Transaktionsdaten parallel durch ein mobiles Endgerät und ein Kassensystem übertragen werden und nur dann zur Ausführung kommen, wenn beide Daten identisch sind.

[0002] Die WO 2010/129357 A2 offenbart ein Verfahren zur Bereitstellung einer dynamischen Karten-Verifikation von mobilen Endgeräten.

[0003] Aus der DE10331733A1 ein Verfahren zu entnehmen, bei der eine besondere Art der Verschlüsselung zwischen Kundenhändler und Hintergrundsystem erfolgt.

[0004] Aus den Druckschriften Wikipedia Mobil-Payment und Handypayment sind weitere Techniken zur Zahlung bekannt, in die die Kennung des mobilen Endgerätes einfließt.

Übersicht über die Erfindung:

[0005] Grundsatz der vorliegenden Erfindung ist die Auseinanderziehung der Informationsfluten vom Käufer und Verkäufer im Moment des Einkaufs. Jede Partei sendet an das Zahlungssystem ihr Informationspaket über ihren Verbindungskanal. So werden bei jedem Einkauf zwei unabhängige Informationspakete an das Zahlungssystem geschickt. Dabei enthält jedes Informationspaket ein Pflichtelement – eine einmalige Nummer des Kassenbelegs. Nur dank dieses Elements kann das Zahlungssystem bzw. das Banksystem zwei Informationspakete finden und sie miteinander verbinden. Dieser Ansatz kann sowohl im realen, mit Kassensystemen, als auch im Internethandel erfolgen. Die Aufgabe der vorliegenden Erfindung besteht darin, ein Verfahren zur Durchführung einer digitalen Transaktion über ein mobiles Endgerät, mit einem Kassensystem bereitzustellen.

[0006] Die Erfindung umfasst ein Verfahren zur Durchführung einer digitalen Transaktion über ein mobiles Endgerät, mit einem Kassensystem.

[0007] Damit die Bank die Kontodaten kennt, werden die Kontodaten z. B. in einem Internet-Dienst abgelegt, wie einem Email-Account oder einem Account in einem sozialen Netzwerk, und das mobile Endgerät kann durch Anmeldung bei diesem Internet-Dienst eine Übermittlung der Kontodaten und des digitalen Codes auslösen. Der Code kann dabei manuell oder automatisch in das Gerät eingegeben werden, wie weiter unten ausgeführt wird. Die einmalige Kennung kann weiterhin, über ein Pattern Password, (Mustersperre), das auf dem Kassengerät oder auf dem Kassenbeleg abgebildet ist, eingegeben werden. Auch die Stimmeingabe ist denkbar. Die automatische Übertragung durch NFC während der Verbindung mit dem Kassengerät wird weiter unten beschrieben.

[0008] Erfindungsgemäß kann der einmalige digitale Code, nur einmalig verwendet werden, um sich mit einem lokalen drahtlosen Netzwerk des Kassensystems zu verbinden, wobei aufgrund der Verbindung eine IMSI, IMEI oder MAC-Adresse des mobilen Endgerätes erlangt wird, die in die Transaktionsdaten einfließt, wobei parallel das mobile Endgerät die IMSI, IMEI oder MAC-Adresse an die Bank übermittelt, und eine Transaktion nur freigegeben wird, wenn auch die IMSI, IMEI oder MAC-Adressen übereinstimmen. Hierdurch wird nicht nur der Code sondern auch die Adresse des Endgerätes überprüft. In einer alternativen Ausführungsform ist die IMSI, IMEI oder MAC-Adresse der Code selber.

[0009] In der bevorzugten Ausführungsform wird der digitale Code auf eine Quittung vom Kassensystem ausgedruckt, um diesen dann manuell im mobilen Gerät einzutippen. Alternativ kann der Code auch über ein Netzwerk an das mobile Endgerät übergeben werden. Dabei wird der einmalige digitale Code über eine drahtlose Verbindung vom Kassensystem and das mobile Endgerät übertragen, vorzugsweise per NFC oder Bluetooth oder WIFI, so dass das mobile Endgerät die Daten ohne manuelles Eintippen weiterleiten kann.

[0010] Das Netzwerk des Kassensystems identifiziert das mobile Endgerät im Moment seines Anschlusses an dem Netzwerk durch eine IMSI – Nummer (International Mobile Subscriber, Identity) oder IMEI (International Mobile Equipment Identity), oder MAC (Media Access Control Address) und leitet die Daten an das Kassensystem weiter.

[0011] Zusätzlich können durch eine Abfrage bei einem Telefonprovider die Standortkoordinaten des mobilen Endgerätes und die tatsächliche geografische Lage des Kassensystems verglichen werden, und wenn die Koordinaten nicht übereinstimmen, so kann die Transaktion blockiert werden. Die Koordinaten können somit ein weiteres Vergleichskriterium

sein, um die Daten sicher zusammenzuführen und die Transaktion auszulösen.

[0012] Nach einem erfolgreichen Abschluss der Transaktion wird der Zugang zu dem lokalen Netzwerk auf der Basis des Codes automatisch abgeschaltet. Hierbei ist das drahtlose lokale Netzwerk ein WIFI.

[0013] In einer weiteren Ausführungsform umfasst die Erfindung ein System, umfassend ein mobiles Endgerät, ein Kassensystem und ein Banksystem, das durch eine Einrichtung gekennzeichnet ist, die das Verfahren nach dem Hauptanspruch implementiert.

[0014] Weiterhin ist im Bereich des Internets ein Verfahren zur Durchführung einer digitalen Transaktion über ein mobiles Endgerat, mit einem Kassensystem möglich, das mit einem drahtlosen lokalen Netzwerk verbunden ist, umfassend die Schritte:

– Erzeugen eines einmaligen digitalen Codes durch das Kassensystem, das zum Einleiten der Transaktion dient;
– automatisches Freischalten eines Netzzugangs zum lokalen drahtlosen Netzwerk nach dem Erzeugen des einmaligen digitalen Codes, wobei der Zugriff auf das drahtlose Netzwerk durch den digitalen Code erlaubt wird;
– Verbinden des mobilen Endgerätes mit dem lokalen Netzwerk mit Hilfe des digitalen Codes und Bereitstellen von Informationen des Endgerätes an das Kassensystem,
– Nach dem Erhalten der Informationen von dem Endgerät durch das Kassensystem erfolgt eine Freigabe der Transaktion durch das Kassensystem.

[0015] Bei dem drahtlosen Netzwerk handele es sich vorzugsweise um ein WLAN Netzwerk, das im lokalen Kassenbereich ausgebildet ist.

[0016] In einer bevorzugten Ausführungsform verwaltet das Kassensystem über ein Benutzerkonto die Zuordnung der Identität des mobilen Endgerätes zu einem Kundenkonto, indem die Bank-Informationen wie Kreditkarteninformationen oder Kontonummer, Bankleitzahl etc. abgelegt sind. Durch die Zuordnung der Mac-Adresse zu diesen Transaktionsinformationen wird erreicht, dass der Besitzer des mobilen Gerätes keinerlei weitere Kontodaten übermitteln muss. Anhand der Mac Adresse erfolgt eine Zuordnung zu den Kontodaten und eine Freigabe kann erfolgen. Um einen Betrug zu vermeiden, sind bei den Kundendaten ebenfalls die Daten des mobilen Providers hinterlegt, so dass der Mobile Provider überprüfen kann, ob sich das Gerät tatsächlich örtlich in dem Bereich der Kasse bewegt und kein Diebstahl der Mac-Adresse vorliegt. Neben der Mac-Adresse können auch andere Kennzeichnungen des mobilen Endgerätes verwendet werden, wie sie weiter unten beschrieben werden. Alternativ überträgt das mobile Endgerät Kontodaten durch eine Anwendung auf dem mobilen Endgerät an eine Zieladresse im mobilen Netzwerk. Anhand der eindeutigen Kennung und der Kontodaten kann erneut vom Provider des mobilen Netzwerkes des mobilen Endgerätes der Standort des mobilen Endgerätes überprüft werden und eine Freigabe kann von Seiten des mobilen Providers erfolgen. Es ist zu beachten, dass ebenfalls eine Abbuchung vom Konto des mobilen Providers erfolgen kann, so dass eine Rechnungsstellung über die Telefonrechnung erfolgen kann.

[0017] Erfindungsgemäß ist der einmalige digitale Code nur einmalig zu verwenden, um sich mit dem lokalen drahtlosen Netzwerk zu verbinden. Es handelt sich somit um einen Einmalcode, der nach einer einmaligen Benutzung keinerlei Zugang erlaubt.

[0018] Der einmalige Code kann eine beliebige Anzahl von Ziffern oder Buchstaben enthalten. Der Kunde darf aber bei einer manuellen Eingabe nur die letzten vier Ziffern eingeben. Das System kann einen ziemlich langen Code (damit beim vielen Einkäufen keine Wiederholungen auftreten) generieren, wählt aber dabei entweder die ersten oder die letzten vier Symbole als einen einmaligen Code für das Netzwerkbetreten aus. Sobald der verkürzte Code eingegeben ist, leitet das System dem Smartphone den kompletten (langen) Originalcode weiter.

[0019] Der einmalige Code kann in unterschiedlicher Form übermittelt werden. Der digitale Code kann auf einer Quittung vom Kassensystem ausgedruckt werden, um diesen dann manuell in ein mobiles Gerät einzutippen. In einer alternativen Ausführungsform wird diese auch als Barcode erzeugt, der dann von einer Anwendung des mobilen Endgerätes eingelesen werden kann. Dieser Barcode kann in der Regel über die Kamera des mobilen Endgerätes detektiert werden. In einer alternativen Ausführungsform kann die Quittung auch über eine mobile Funkschnittstelle per Bluetooth, NFC oder als SMS an das mobile Endgerät übermittelt werden. Wenn auf dem mobilen Endgerät eine spezielle Anwendung installiert ist, kann dieser Code gleich interpretiert werden und zur Autorisierung im mobilen Netzwerk genutzt werden. Vorzugsweise muss der Benutzer noch die Eingabe bestätigen, bevor ein Zugang zum mobilen Netzwerk bzw. drahtlosen Netzwerk freigeschaltet wird.

[0020] Im ersten Informationsfluss erfolgt eine Codeeingabe für den Netzzugang. Dadurch ist der Kunde im Netz; das Netzwerk kann jetzt die MAC-Adresse des Kunden zuordnen, und der Kunde wird danach vom Netz getrennt. Daraufhin schickt das Kassensystem ein Informationspaket (enthält MAC-Adresse des Käufers, den Zahlungsbetrag und den Kassenbeleg,

eigene Verkäuferangaben) an das Zahlungssystem (z. B. Bank oder VISA usw.) weiter.

[0021] Parallel dazu im zweiten Informationsfluss sendet das Smartphone den Kassenbeleg an den Anwendungsanbieter/Soziale Netzwerk (z. B. Facebook oder Googlemail). Die Anwendung fügt die Bankdaten des Käufers dem Informationspaket zu und sendet dieses an das Zahlungssystem (z. B. Bank oder VISA usw.). Das Zahlungssystem vergleicht beide Informationspakete. Der Verkäufer bekommt eine Zusage vom Zahlungssystem. Die Kundenbank bekommt eine Zusage vom Zahlungssystem.

[0022] Bei einer der nichtmanuellen Codeeingabe ist eine automatische Eingabe durch die NFC – Technologie möglich.

[0023] Um den Zugang zum lokalen mobilen/drahtlosen Netzwerk zu erreichen, ist das Kassensystem mit einem Steuerungssystem für das mobile Netzwerk verbunden, um den digitalen Code austauschen. So kann zum Beispiel das Steuerungssystem über das RADIUS Protokoll die Zugangspunkte für das kabellose Netzwerk steuern. Sollte sich ein Benutzer am kabellosen Netzwerk anmelden, so können entsprechende Anfragen beim Steuerungssystem vom Zugangspunkt des kabellosen Netzwerkes gestellt werden. Andere Technologien sind natürlich denkbar. Grundsätzlich sollte jedoch ein Standard verwendet werden um die kabellosen Zugangspunkte zu steuern, so dass das Einmal-Passwort effektiv genutzt wird. Nachdem eine Anmeldung erfolgt ist und die notwendigen Daten ausgetauscht wurden setzt das Steuerungssystem sofort den Zugang zurück.

[0024] In einer möglichen Ausführungsform, wie oben beschrieben, läuft eine Anwendung auf dem mobilen Endgerät, über die der digitale Code eingegeben wird und eine Anmeldung am mobilen Netzwerk erfolgt, und wobei nach der Anmeldung Kontoinformationen, Kreditkarteninformationen oder IMSI-Informationen an das mobile Netzwerk von der Anwendung übermittelt werden, um eine Transaktion abzuschließen. Um die Informationen an die richtige Stelle im Netzwerk zu übermitteln, wird bei der Anmeldung des mobilen Endgerätes eine Adresse übermittelt, (zum Beispiel über das DHCP-Protokoll) an die die relevanten Identifikationsdaten des mobilen Endgerätes zu übertragen sind. Hierdurch ist es ebenfalls möglich Kontoinformationen und weitere Details zu übertragen. Mit der Anmeldung am mobilen Netzwerk wird eine Netzwerkadresse dem mobilen Endgerät mitgeteilt, an die die Kontoinformationen, Kreditkarteninformationen oder IMSI-Informationen zu übermitteln sind. Nachdem diese Informationen erlangt wurden, erfolgt eine Übermittlung dieser Informationen in der Regel nur auf Basis einer Zustimmung. Weiterhin können Zertifikate und ähnliche Details abgefragt werden, um sicherzustellen, dass nur vertrauenswürdige Instanzen diese Informationen enthalten.

[0025] In einer alternativen Ausführungsform spricht das Steuersystem für das mobile Netzwerk das mobile Endgerät nach der Anmeldung über das Netzwerk an, um Informationen für die Durchführung einer digitalen Transaktion vom mobilen Endgerät zu erlangen. Wobei das Steuersystem des Netzwerks das mobile Endgerät im Moment seines Anschlusses (durch eine IMSI – Nummer (International Mobile Subscriber, Identity) oder IMSI (International Mobile Equipment Identity), oder MAC (Media Access Control address) identifiziert und die Daten an das Kassensystem weiterleitet.

[0026] Sollte ein Kundenkonto beim Unternehmen vorhanden sein, greift das Kassensystem anhand der Netzwerkidentifizierung auf eine Datenbank zu, in der die Kontoinformationen und/oder ein Netzwerkprovider in Relation zu der Netzwerkidentifizierung abgelegt sind. Durch die Transaktionsdaten und/oder die Kennung vom Kassensystem können die Zugangsdaten wie oben beschrieben wurde durch einen Telefonprovider über ein Telefonnetzwerk an das mobile Endgerät übermittelt werden, wobei der Telefonprovider die Korrektheit der Identifizierung überprüft. Hierbei überprüft der Telefonprovider die IMSI, IMEI oder MAC. Vorzugsweise überprüft der Telefonprovider die Standortkoordinaten des mobilen Endgerätes und die tatsächliche geografische Lage des Kassensystems, indem er diese vergleicht, und wenn die Koordinaten nicht übereinstimmen, so kann die Transaktion blockiert werden bzw. eine entsprechende Warnmeldung an das Kassensystem gesendet werden.

[0027] Sollte sich herausstellen, dass sowohl die Transaktions-Daten als auch die Standortkoordinaten korrekt sind, so werden die Transaktionsdaten an eine entsprechende Clearingstelle übermittelt (eine Bank), die die Transaktion letztendlich auf den Banksystemen durchführt.

[0028] Nach einem erfolgreichen Abschluss der Transaktion wird der Zugang zu dem lokalen Netzwerk auf der Basis des Codes automatisch abgeschaltet.

Figuren Beschreibung:

[0029] **Fig.** 1 zeigt schematisch den Ablauf des Verfahrens ohne WLAN;

[0030] **Fig.** 2 zeigt schematisch den Ablauf des Verfahrens mit WLAN;

[0031] **Fig.** 3 zeigt schematisch den Ablauf des Verfahrens mit WLAN und MAC Adresse;

[0032] **Fig.** 4 zeigt schematisch den Ablauf des Verfahrens, wobei die Kennung nicht manuell, sondern per NFC-Netz auf das mobile Endegerät eingegeben wird.

Beschreibung einer Ausführungsform:

[0033] Grundlage der Idee ist die Auseinanderziehung der Informationsflüsse vom Käufer und Verkäufer im Moment des Einkaufs. Jede Partei schickt an das Zahlungssystem ihr Informationspaket über ihren Verbindungskanal. So werden bei jedem Einkauf zwei unabhängige Informationspakete an das Zahlungssystem geschickt.

[0034] Dabei enthält jedes Informationspaket ein Pflichtelement – eine einmalige Nummer des Kassenbelegs. Nur dank diesem Element kann das Zahlungssystem zwei Informationspakete finden und sie zusammen verbinden. **Fig.** 1 zeigt schematisch den Ablauf eines Verfahrens bei dem kein WLAN eingesetzt wird und eine Zahlung im Internet erfolgt.

[0035] Grundelement ist, dass der Käufer Nutzer eines sozialen Netzwerkes/Messenger ist, indem er seine Zahlungsdaten angegeben hat. Hierüber erfolgt eine vereinzelte Informationsversendung über die Zahlung vom Käufer und Verkäufer. Es wird dabei eine einmalige Kassenbelegnummer als Verbindungsmöglichkeit verwendet.

[0036] Gemäß **Fig.** 1, wird in Schritt **1A** Folgendes durchgeführt.

[0037] Der Online-Händler generiert eine einmalige Kassenbelegnummer und sendet sie an das Zahlungssystem (samt Zahlungsbetrag und eigene Bankverbindung) (**1A**).

[0038] Parallel dazu meldet sich der Käufer bei seinem sozialen Netzwerk an oder ist bereits angemeldet (**1B**).

[0039] Der Käufer sendet seine Kassenbelegnummer an das soziale Netzwerk (**1c**). Das soziale Netzwerk sendet diese Kassenbelegnummer mit den persönlichen Käuferdaten an das Zahlungssystem weiter (**2B**). Das Zahlungssystem bekommt zwei Informationspakete mit der gleichen Kassenbelegnummer und verbindet sie für die Bearbeitung (**2A**). Das Zahlungssystem prüft dann beim Bank Emittent der Karte die Zahlungsfähigkeit des Kunden (**3**) und bekommt ggfs. eine Anfragebestätigung (**4**). Das Zahlungssystem sendet dann eine Anfragebestätigung (**5**) an die Acquiring Bank, die dann wieder an das Kaufhaus (**6**) bzw. das Kassensystem weitergeleitet wird die die Information für die Zahlung freigeben.

[0040] In **Fig.** 2 sind die Grundelemente, dass der Käufer ein Nutzer eines sozialen Netzwerkes/Messenger ist, wo er seine Zahlungsdaten angegeben hat. Es erfolgt eine vereinzelte Informationsversendung über die Zahlung vom Käufer und Verkäufer. Es erfolgt eine Verwendung der einmaligen Kassenbelegnummer als Verbindungsmöglichkeit zwischen zwei Informationspaketen. So erfolgt eine Verwendung der MAC-Adresse des WLAN-Netzwerkes des Verkäufers (Kaufhaus, Cafe, Parkhaus usw.) für die Verbindungsmöglichkeit zwischen zwei Informationspaketen. Die Handlungsreihenfolge ist grundsätzlich ähnlich wie bei der **Fig.** 1, jedes Informationspaket enthält aber hier eine MAC-Adresse des WLAN-Netzwerkes des Verkäufers.

[0041] Neben der Kassenbelegnummer dient die MAC-Adresse für die Zusammenführung der Informationen seitens des Zahlungssystems bei einem Einkauf. Der Käufer sucht sich das WLAN-Netzwerk des Verkäufers in seinem Smartphone aus und meldet sich mit einem Passwort (einmalige Kassenbelegnummer) an.

[0042] Das Smartphone bekommt Informationen über die MAC-Adresse des WLAN-Netzes des Verkäufers, die an das Zahlungssystem mitgeschickt wird.

[0043] Das WLAN-Netzwerk des Verkäufers erhält ein Signal über den Einkaufswunsch und sendet die Daten an das Zahlungssystem (**1**). Die weiteren Schritte entsprechen **Fig.** 1 wobei zusätzlich noch die MAC-Adresse des WLAN-Netzwerkes verglichen wird.

[0044] Die **Fig.** 3 zeigt wiederum eine abgewandelte Version. Die Grundelemente sind wiederum, dass der Käufer Nutzer eines sozialen Netzwerkes/Messenger ist, wo er seine Zahlungsdaten angegeben hat. Es erfolgt eine vereinzelte, aufgespaltene Informationsversendung über die Zahlung vom Käufer und Verkäufer. Die Verwendung der einmaligen Kassenbelegnummer als Verbindungsmöglichkeit zwischen zwei Informationspaketen wird unter Verwendung der MAC-Adresse des WLAN-Netzwerkes des Verkäufers (Kaufhaus, Cafe, Parkhaus usw.) und unter Verwendung der MAC-Adresse des Käufers zusammengeführt. Hierdurch werden 3 Parameter verglichen.

[0045] Die Handlungsreihenfolge ist dieselbe wie bei den Varianten 1 und 2, jedes Informationspaket enthält aber hier außerdem eine MAC-Adresse des Smartphones des Käufers.

[0046] Neben der Kassenbelegnummer dient diese MAC-Adresse für die Zusammenführung auf Seiten des Zahlungssystems.

[0047] Der Käufer sucht das WLAN-Netzwerk des Verkäufers in seinem Smartphone aus und meldet

sich mit einem Passwort (einmalige Kassenbelegnummer) an.

[0048] Das WLAN-Netzwerk des Verkäufers erhält die MAC-Adresse des Käufersmartphones und umgekehrt. Jede Partei sendet die MAC-Adresse ihres Kontrahenten zusammen mit dem kompletten Informationspaket an das Zahlungssystem. (**1**)(**2**)(**3**) Beide MAC-Adressen sind in diesem Fall Zusatzkomponenten bei der Suche nach zwei an das Zahlungssystem verschickte Informationspakete im Rahmen eines Einkaufs.

[0049] Die **Fig.** 2 und **Fig.** 3 zeigen schematisch den Ablauf des vorliegenden Verfahrens. In einem ersten Schritt erzeugt ein Kassensystem einen Kassenzettel für eine Transaktion mit einem einmaligen Zugangskennwort für das lokale drahtlose Netzwerk. Das Kassensystem gibt diese Nummer weiter an ein Zugangssteuerungssystem, das für den Zugang zu dem mobilen lokalen Netzwerk zuständig ist. Nachdem sich das mobile Endgerät angemeldet hat, erlangt das Kassensystem die entsprechende Information über die Anmeldung vom Zugangssystem (das nicht dargestellt ist). Das Kassensystem fragt dann bei der Hausbank des Kaufhauses an, ob mit der Kennung des mobilen Endgerätes ein Konto verknüpft ist, auf dem die entsprechenden Bankdaten des Kunden abgelegt sind. Die Acquiring Bank gibt diese dann an ein Zahlungssystem (VISA, MasterCard) weiter, das vom Sozialen Netzwerk ebenfalls Informationen erlangt. Sollte ggfs. auch noch die Identifikation des mobilen Endgerätes mit dem Standort übereinstimmen, was beim Telefonprovider abgefragt wurde, so gibt es noch zusätzliche Daten. Sollte der Telefonanbieter/Provider feststellen, dass Standort und Kennung des mobilen Gerätes übereinstimmen und kein Missbrauch vorliegt, so wird eine Rückmeldung an das Zahlungssystem gegeben. Das Serversystem teilt dies der Hausbank wiederum mit, so dass sichergestellt ist, dass kein Missbrauch vorliegt. Nachdem diese Details ausgetauscht wurden, übernimmt das Zahlungssystem den Abschluss der Transaktion über den Bank Emittent. Nachdem diese erfolgte, wird dann eine Überweisung an das Kaufhaus übermittelt. Das Kassensystem wird ebenfalls über den erfolgreichen Abschluss der Transaktion informiert. Die **Fig.** 4 zeigt zusätzlich, dass die einmalige Kennung über ein NFC-Netz an das Smartphone übermittelt wird. Dieses sendet die Daten dann an das soziale Netzwerk bzw. Netzwerkdienste, die dann die Daten wiederum an die Bank weiterleiten. Parallel werden die Daten auch vom Kaufhaus zur Bank übermittelt.

[0050] In einer möglichen Ausführungsform erfolgt das Verfahren wie folgt:
Der Käufer wählt die Ware aus [oder ein Produkt, bzw. Leistung im Cafe]. Im Weiteren wird die Reihenfolge der Tätigkeiten beim Kauf der Ware und der Bezahlung der Ware oder der Leistungen (der Geldempfänger wird „Kaufhaus [Cafe]" genannt) beschrieben

[0051] Die Kasse/Kassensystem im Kaufhaus [Cafe] ist mit dem drahtlosen lokalen Netzwerk des Kaufhauses [Cafés] unmittelbar oder mittelbar verbunden. Zumindest besteht eine Verbindung zu einem Steuersystem, das den Zugang zum mobilen Netzwerk verwaltet. Das Steuersystem kann z. B. über Regeleinheiten und Standardprotokolle den Zugriff für die Authentifizierung vorgeben.

[0052] Der Mitarbeiter des Kaufhauses [Cafés] scannt die ausgewählte Ware ein, eine Quittungsnummer mit einem Endbetrag des Einkaufs wird vom Kassengerät/Kassensystem (der Verkäufer kann durch einen Computer ersetzt werden) erzeugt. Die Nummer ist vorzugsweise eine Zufallszahl, die durch einen Generator erzeugt wird.

[0053] Beim Kauf und während der Bezahlung wird eine einmalige Quittungs-, bzw. Belegnummer generiert. Die Zahl der Ziffer (Zahlenreihe) kann beliebig sein.

[0054] Mit dem Generieren des Kassenbelegs wird für das WLAN des Kaufhauses [Cafés] ein einmaliges Kennwort/Zutritts Code für den Netzzutritt erzeugt:

a) Entweder mit einer Zahlenreihe, die genau mit der Kassenzettelnummer übereinstimmt
b) Oder mit einer komplett anderen Nummer, die aber mit der Kassenzettelnummer „verbunden" ist, so dass der Benutzer dieses erkennt.

[0055] Hierbei kann es sich um einen N-stelligen Code als Kennwort handeln. Dieser ist komfortabel und kundenfreundlich und für die Wahrnehmung und schnelle Eingabe geeignet.

[0056] Dieses einmalige Kennwort ist ausschließlich für einen einzigen Netzzutritt von einem Außengerät gültig.

[0057] Der Kunde sieht auf seinem Smartphone eine Liste der möglichen drahtlosen Netzwerke, wählt das im Moment benötigte Netz und aktiviert dieses über den Code. Das WLAN des Cafés oder Kaufhauses fordert ein Kennwort für eine Freischaltung.

[0058] Der Kunde gibt als Code die N-Nummer seines Kassenbelegs ein. Die Wi-Fi-Nutzung vom Kunden und die Eingabe der Kassenbelegnummer (gleichzeitig eines Kennwortes) bestätigt den Kundenwunsch einen bestimmten Betrag von seinem Konto abzubuchen. Das Konto kann hierbei ein lokales Konto beim Verkäufer sein, auf dem die eindeutige Kennung des mobilen Telefons und die Bankinformationen abgelegt sind. Alternativ kann anhand der Netzwerkkennung auch der Mobil-Funk-Provider festgestellt werden und eine Abbuchung über die

Telefonrechnung erfolgen. In einer weiteren Ausführungsform überträgt das mobile Endgerät Bank-Information (Kredit-Karte, EC-Karte etc.)

[0059] Der kurzzeitige Anschluss zum WLAN eines Cafés oder Kaufhauses an sich gibt dem Kunden grundsätzlich keine weiteren Netzoptionen (wie z. B. die Möglichkeit eines Internetzugangs) außer einer Wunschbestätigung einen bestimmten Betrag (auf dem Kassenzettel) zu bezahlen.

[0060] Das WLAN eines Cafés oder Kaufhauses initialisiert das Smartphone im Moment seines Anschlusses (durch eine IMSI – Nummer (International Mobile Subscriber Identity) oder IMSI (International Mobile Equipment Identity), oder MAC (Media Access Control Address)) und leitet die Daten an das Zahlungssystem weiter.

[0061] Die Daten können über den Kassenbeleg durch einen Telefonprovider übermittelt werden (der Telefonprovider erkennt in dem Fall die individuellen Merkmale des Kunden über sein Smartphone) Anmerkung: Der Telefonanbieter kann für den Kunden als einen zusätzlichen Sicherheitsfilter dienen – die tatsächliche MAC-Adresse wird ergänzend überprüft (im Falle, wenn diese Adresse missbraucht wurde).

[0062] Wenn der Telefonanbieter eine Anfrage über eine Kundenpersonifizierung durch sein Smartphone vom Café oder Kaufhaus empfängt, kann er die GPS-Koordinaten des Smartphones und der tatsächlichen geografischen Lage des Kaufhauses oder Cafés vergleichen. Wenn die Koordinaten nicht übereinstimmen kann die Transaktion blockiert werden.

[0063] Noch eine Überprüfungsvariante wäre – der Telefonprovider kann den Aufenthaltsort des Smartphone durch seine IMSI/IMEI – Nummer sicherstellen. Dieser Aufenthaltsort muss dann mit der tatsächlichen geografischen Lage des Cafés oder Kaufhauses verglichen werden.

[0064] Das Zahlungssystem leitet seine Anfrage an den Emittenten weiter (an die Bank, die eine Kredit-, bzw. EC-Karte dem Kunden ausgegeben oder das Kundenkonto eröffnet hat) und empfängt eine Zu- oder absage, abhängig von der Zahlungsfähigkeit des Kunden. Dann wird das Kaufhaus/Cafe informiert, ob die Transaktion stattfinden darf.

[0065] Der Zugriff des Kundensmartphones zum WLAN des Kaufhauses oder Cafés wird nach einer erfolgreichen Bezahlung automatisch abgeschaltet.

[0066] Zusätzlich ist Folgendes zu beachten:
Andere Vermittler zwischen Zahlungssystem und Verkäufern sind möglich. Es kann zum Beispiel eine Sozialnetzanwendung sein, die im Kundensmartphone installiert ist. Diese Anwendung kann die Funktion übernehmen, die individuellen Kundencharakteristika an das Zahlungssystem weiterzuleiten.

[0067] Es ist auch eine andere Verbindung zwischen dem Verkäufer und der Kundenbank denkbar, so wie eine direkte Verbindung über den Telefonanbieter – vorbei an dem traditionellen Zahlungssystem.

Patentansprüche

1. Verfahren zur Durchführung einer digitalen Transaktion über ein mobiles Endgerät, mit einem Kassensystem, umfassend die Schritte:
– Erzeugen eines einmaligen digitalen Codes durch das Kassensystem, der die Transaktion identifiziert, wobei der einmalige digitale Code nur einmalig als Passwort verwendet werden kann, um ein mobiles Endgerät mit einem lokalen, drahtlosen Netzwerk des Kassensystems zu verbinden;
– Eingabe des digitalen Codes in das mobile Endgerät, manuell, durch Ausdrucken des digitalen Codes auf einer Quittung vom Kassensystem, um diesen dann im mobilen Endgerät einzutippen, oder automatisch durch Übertragung über NFC, Barcode, SMS, WiFi oder Bluetooth;
– Verbinden des mobilen Endgeräts mit einem lokalen, drahtlosen Netzwerk des Kassensystems, wobei aufgrund der Verbindung eine IMSI, IMEI oder MAC-Adresse des mobilen Endgerätes erlangt wird, wobei das Netzwerk das mobile Endgerät im Moment seines Anschlusses durch eine IMSI-Nummer (International Mobile Subscriber Identity) oder IMEI (International Mobile Equipment Identity) oder MAC (Media Access Control Address) identifiziert und die Daten an das Kassensystem weiterleitet, wobei das mobile Endgerät umgekehrt die IMSI, IMEI oder MAC-Adresse des Netzwerks des Verkäufers erhält;
– Übermitteln der Transaktionsdaten mit dem einmaligen digitalen Code vom Kassensystem an eine Bank/Emittent des Besitzers des Endgerätes über einen ersten digitalen Netzwerkpfad, wobei sowohl die IMSI, IMEI oder MAC-Adresse des mobilen Endgerätes als auch die in die IMSI, IMEI oder MAC-Adresse des Netzwerks des Verkäufers in die Transaktionsdaten einfließen;
– paralleles Übermitteln des digitalen Codes, der Kontoinformationen und der IMSI, IMEI oder MAC-Adresse des Netzwerks des Verkäufers, ausgelöst durch das mobile Endgerät an die Bank/Emittent, über einen zweiten digitalen Netzwerkpfad, wobei das mobile Endgerät parallel sowohl seine IMSI, IMEI oder MAC-Adresse als auch die IMSI, IMEI oder MAC-Adresse des Netzwerks des Verkäufers an die Bank/Emittent übermittelt, und wobei das mobile Endgerät durch Anmeldung bei einem Internet-Dienst, in dem die Kontodaten abgelegt sind, eine Übermittlung der Kontodaten an die Bank/Emittent auslöst;
– Zusammenführen der Transaktionsdaten vom Kassensystem und der Kontoinformationen durch die

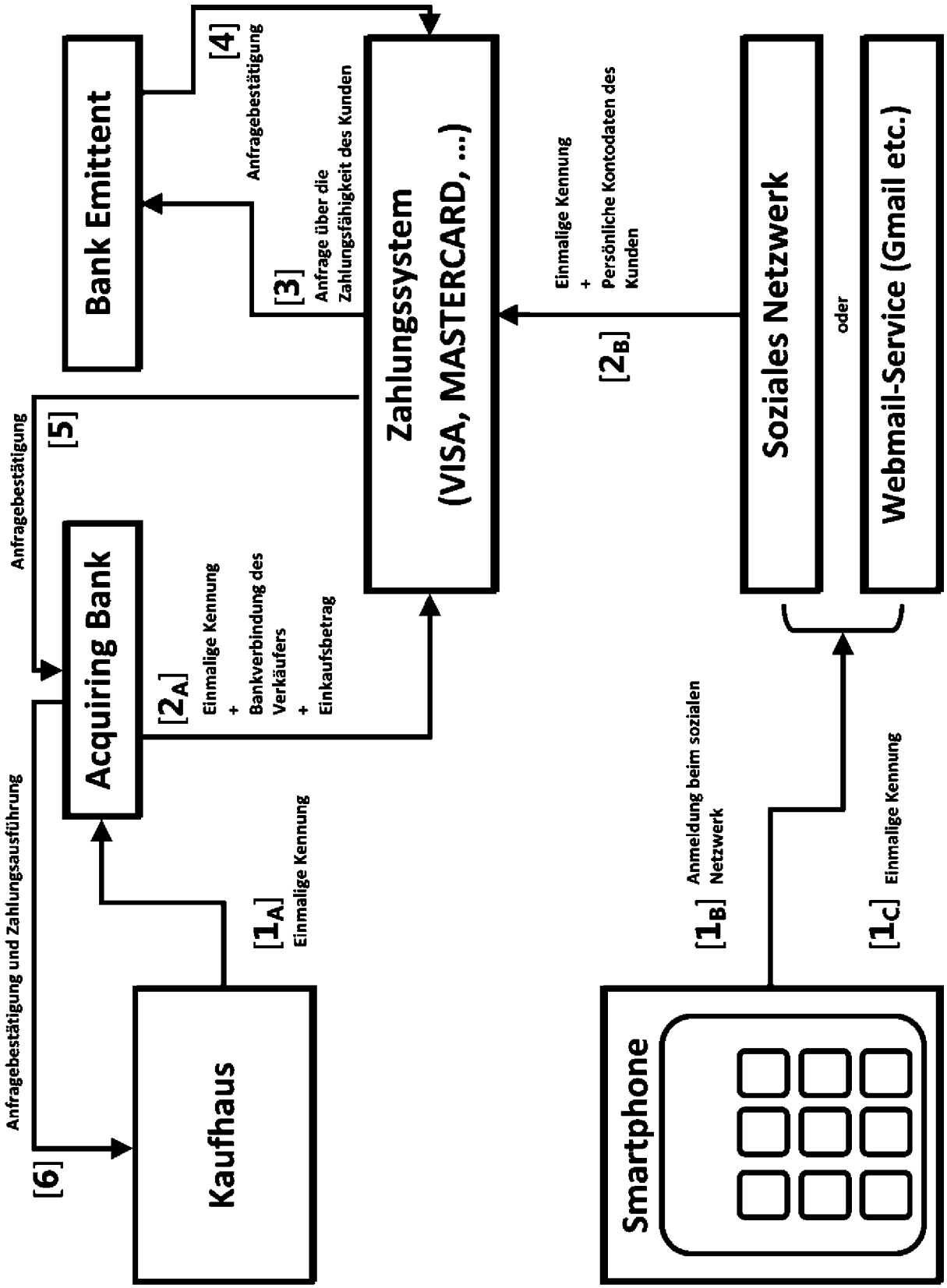
Bank/Emittent, die durch das mobile Endgerät ausgelöst wurden, und Freigabe der Transaktion bei erfolgreicher Zusammenführung, wobei die Transaktion nur freigegeben wird, wenn auch die jeweiligen IMSI, IMEI oder MAC-Adressen übereinstimmen, wobei der Telefonprovider die Standortkoordinaten des mobilen Endgerätes und die tatsächliche geografische Lage des Kassensystems vergleicht, und wenn die Koordinaten übereinstimmen, die Transaktion ausführt;
– Automatisches Abschalten des Zugangs zu dem lokalen Netzwerk auf der Basis des Codes nach einem erfolgreichen Abschluss der Transaktion.

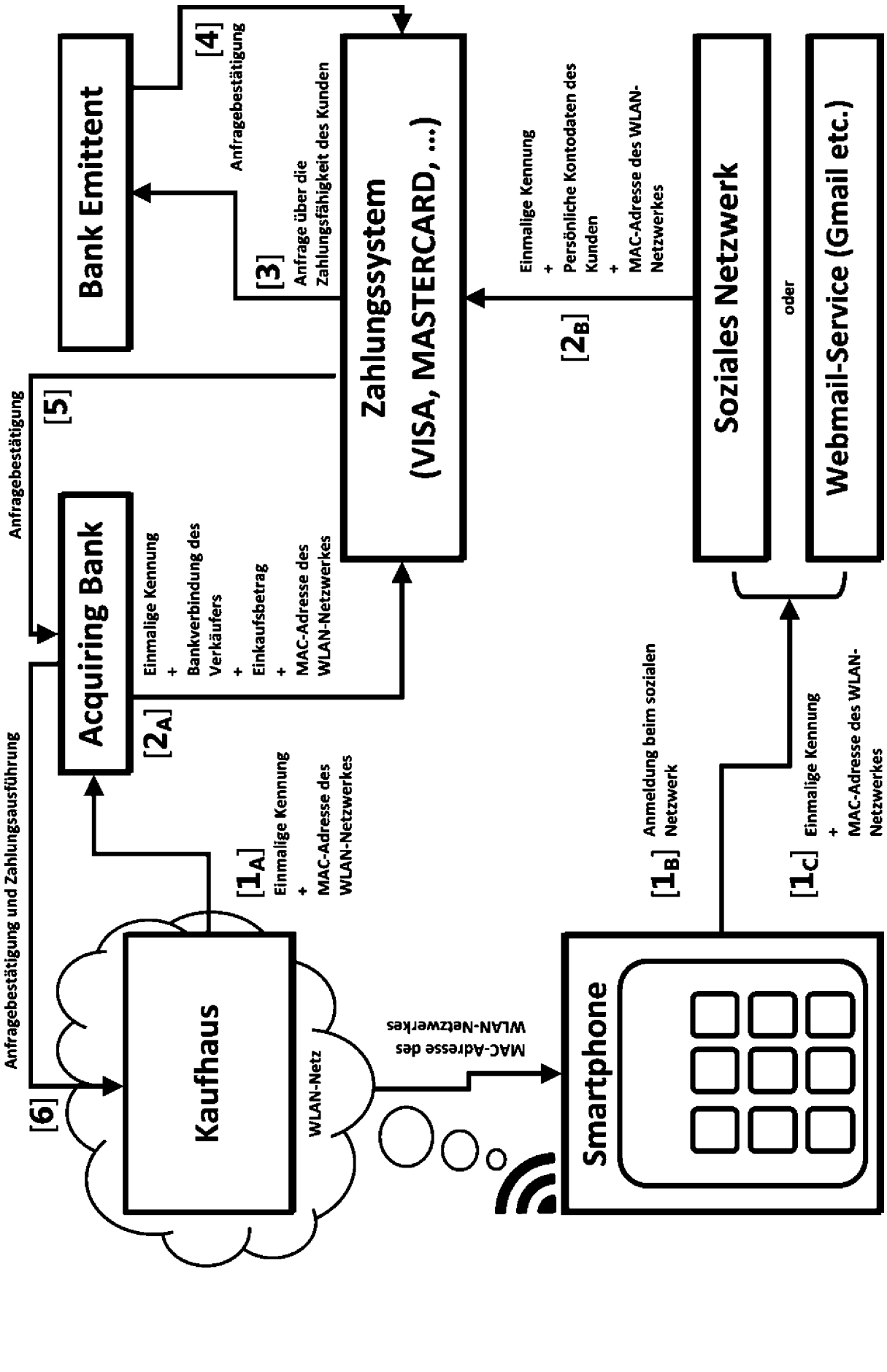
2. System umfassend ein mobiles Endgerät, ein Kassensystem und ein Banksystem, gekennzeichnet durch eine Einrichtung, die das Verfahren nach Anspruch 1 implementiert.

Es folgen 4 Seiten Zeichnungen

Anhängende Zeichnungen

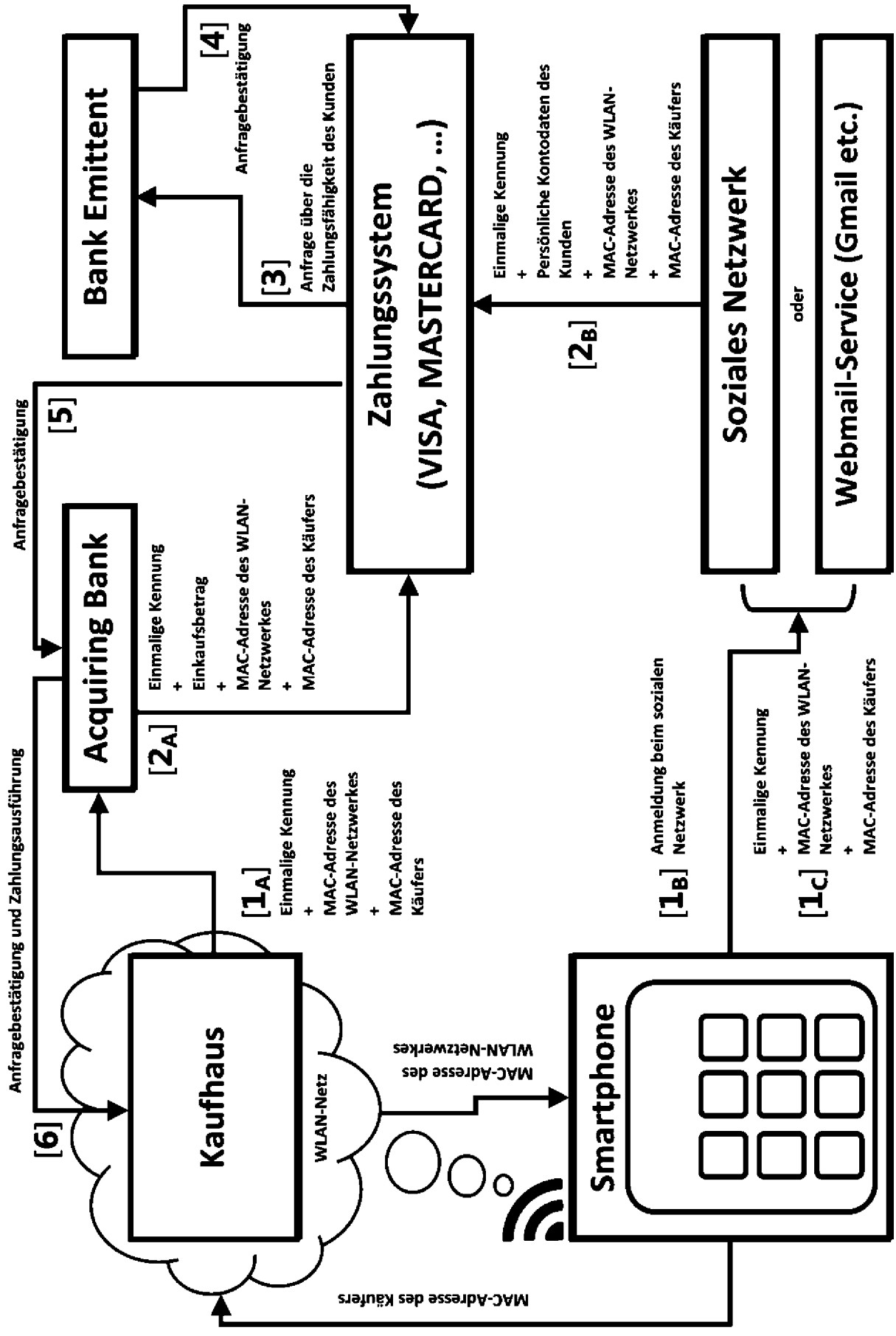
FIGUR 1



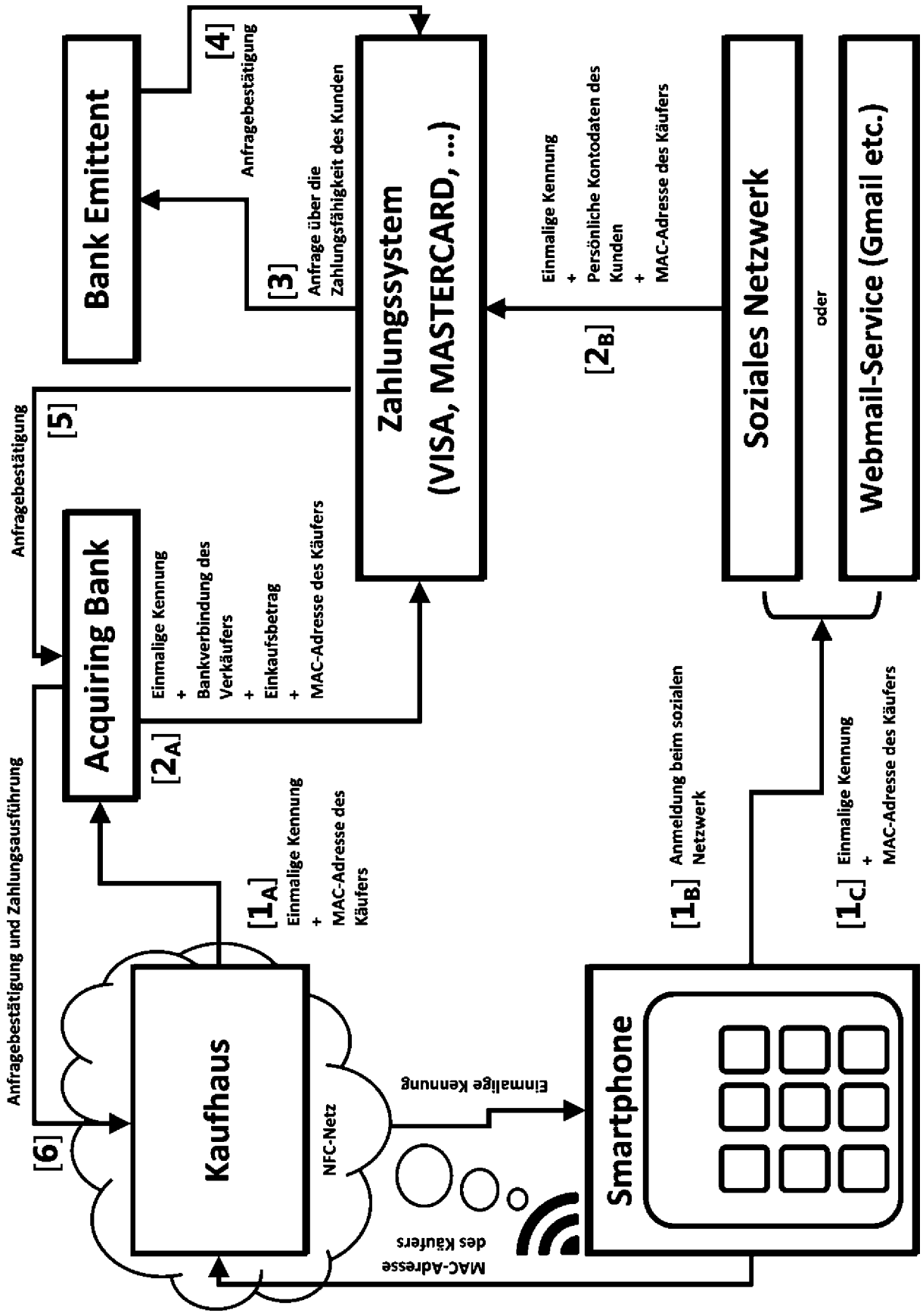

Bank Emittent
[4]
Anfragebestätigung
[3]
Anfrage über die Zahlungsfähigkeit des Kunden
Zahlungssystem (VISA, MASTERCARD, ...)
Einmalige Kennung + Persönliche Kontodaten des Kunden + MAC-Adresse des WLAN-Netzwerkes
[2B]
Soziales Netzwerk
oder
Webmail-Service (Gmail etc.)
Anfragebestätigung
[5]
Acquiring Bank
Einmalige Kennung + Bankverbindung des Verkäufers + Einkaufsbetrag + MAC-Adresse des WLAN-Netzwerkes
[2A]
Anfragebestätigung und Zahlungsausführung
[6]
[1A] Einmalige Kennung + MAC-Adresse des WLAN-Netzwerkes
[1B] Anmeldung beim sozialen Netzwerk
[1C] Einmalige Kennung + MAC-Adresse des WLAN-Netzwerkes
Kaufhaus
WLAN-Netz
MAC-Adresse des WLAN-Netzwerkes
Smartphone

FIGUR 2

FIGUR 3


Bank Emittent
[4]
Anfragebestätigung
[3]
Anfrage über die Zahlungsfähigkeit des Kunden
Zahlungssystem (VISA, MASTERCARD, ...)
Einmalige Kennung + Persönliche Kontodaten des Kunden + MAC-Adresse des WLAN-Netzwerkes + MAC-Adresse des Käufers
[2B]
Soziales Netzwerk
oder
Webmail-Service (Gmail etc.)
Anfragebestätigung
[5]
Acquiring Bank
[2A]
Einmalige Kennung + Einkaufsbetrag + MAC-Adresse des WLAN-Netzwerkes + MAC-Adresse des Käufers
Anfragebestätigung und Zahlungsausführung
[6]
Kaufhaus
WLAN-Netz
[1A]
Einmalige Kennung + MAC-Adresse des WLAN-Netzwerkes + MAC-Adresse des Käufers
MAC-Adresse des WLAN-Netzwerkes
Smartphone
[1B]
Anmeldung beim sozialen Netzwerk
[1C]
Einmalige Kennung + MAC-Adresse des WLAN-Netzwerkes + MAC-Adresse des Käufers
MAC-Adresse des Käufers

FIGUR 4


Bank Emittent
[4]
Anfragebestätigung
[3]
Anfrage über die Zahlungsfähigkeit des Kunden
Zahlungssystem (VISA, MASTERCARD, ...)
Einmalige Kennung + Persönliche Kontodaten des Kunden + MAC-Adresse des Käufers
[2B]
Soziales Netzwerk
oder
Webmail-Service (Gmail etc.)
Anfragebestätigung
[5]
Acquiring Bank
Einmalige Kennung + Bankverbindung des Verkäufers + Einkaufsbetrag + MAC-Adresse des Käufers
[2A]
Anfragebestätigung und Zahlungsausführung
[1A] Einmalige Kennung + MAC-Adresse des Käufers
[1B] Anmeldung beim sozialen Netzwerk
[1C] Einmalige Kennung + MAC-Adresse des Käufers
[6]
Kaufhaus
NFC-Netz
Einmalige Kennung
MAC-Adresse des Käufers
Smartphone