(12) NACH DEM VERTRAG ÜBER DIE INTERNATIONALE ZUSAMMENARBEIT AUF DEM GEBIET DES PATENTWESENS (PCT) VERÖFFENTLICHTE INTERNATIONALE ANMELDUNG

(19) Weltorganisation für geistiges Eigentum
Internationales Büro

(43) Internationales Veröffentlichungsdatum
19. Dezember 2013 (19.12.2013)

WIPO | PCT

(10) Internationale Veröffentlichungsnummer
WO 2013/185918 A2

(51) Internationale Patentklassifikation:
G06Q 20/32 (2012.01)

(21) Internationales Aktenzeichen: PCT/EP2013/001746

(22) Internationales Anmeldedatum:
13. Juni 2013 (13.06.2013)

(25) Einreichungssprache: Deutsch

(26) Veröffentlichungssprache: Deutsch

(30) Angaben zur Priorität:
10 2012 011 562.8 13. Juni 2012 (13.06.2012) DE

(71) Anmelder: **WEWEWE GMBH** [DE/DE]; Großeislinger Straße 78, 73033 Göppingen (DE).

(72) Erfinder: **BURGBACHER, Axel**; Großeislinger Straße 78, 73033 Göppingen (DE).

(74) Anwalt: **PATENTANWÄLTE RUFF, WILHELM, BEIER, DAUSTER & PARTNER**; Kronenstraße 30, 70174 Stuttgart (DE).

(81) Bestimmungsstaaten *(soweit nicht anders angegeben, für jede verfügbare nationale Schutzrechtsart)*: AE, AG, AL, AM, AO, AT, AU, AZ, BA, BB, BG, BH, BN, BR, BW, BY, BZ, CA, CH, CL, CN, CO, CR, CU, CZ, DE, DK, DM, DO, DZ, EC, EE, EG, ES, FI, GB, GD, GE, GH, GM, GT, HN, HR, HU, ID, IL, IN, IS, JP, KE, KG, KN, KP, KR, KZ, LA, LC, LK, LR, LS, LT, LU, LY, MA, MD, ME, MG, MK, MN, MW, MX, MY, MZ, NA, NG, NI, NO, NZ, OM, PA, PE, PG, PH, PL, PT, QA, RO, RS, RU, RW, SC, SD, SE, SG, SK, SL, SM, ST, SV, SY, TH, TJ, TM, TN, TR, TT, TZ, UA, UG, US, UZ, VC, VN, ZA, ZM, ZW.

(84) Bestimmungsstaaten *(soweit nicht anders angegeben, für jede verfügbare regionale Schutzrechtsart)*: ARIPO (BW, GH, GM, KE, LR, LS, MW, MZ, NA, RW, SD, SL, SZ, TZ, UG, ZM, ZW), eurasisches (AM, AZ, BY, KG, KZ, RU, TJ, TM), europäisches (AL, AT, BE, BG, CH, CY, CZ, DE, DK, EE, ES, FI, FR, GB, GR, HR, HU, IE, IS, IT, LT, LU, LV, MC, MK, MT, NL, NO, PL, PT, RO, RS, SE, SI, SK, SM, TR), OAPI (BF, BJ, CF, CG, CI, CM, GA, GN, GQ, GW, KM, ML, MR, NE, SN, TD, TG).

Veröffentlicht:

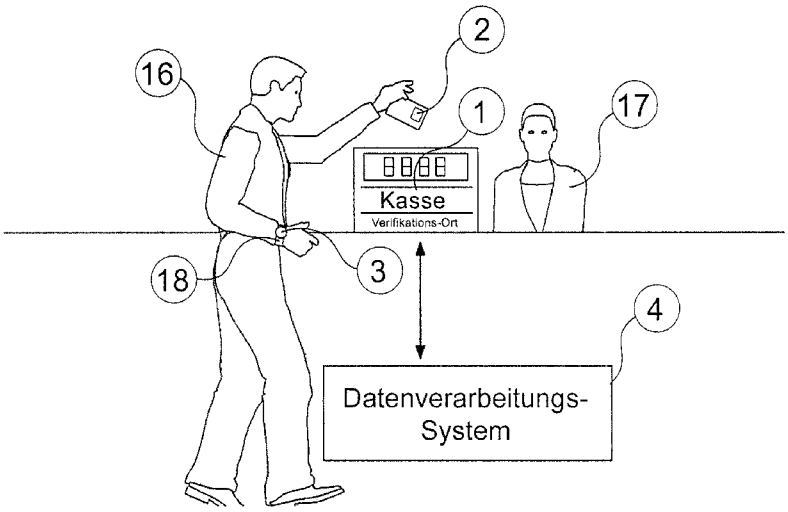
— *ohne internationalen Recherchenbericht und erneut zu veröffentlichen nach Erhalt des Berichts (Regel 48 Absatz 2 Buchstabe g)*

WO 2013/185918 A2

(54) **Title**: METHOD AND DEVICE FOR RECOGNISING AND VERIFYING ACCESS AUTHORISATIONS

(54) **Bezeichnung** : VERFAHREN UND VORRICHTUNG ZUR IDENTIFIKATION UND VERIFIKATION VON ZUGRIFFSBERECHTIGUNGEN

Abbildung 1



1 Cash desk
Verification point
4 Data processing system

(57) **Abstract**: The invention relates to a method for protected bi-directional data communication between a person (16) to be authorised and a verification device (1). In said method, authorisation is given by the reciprocal recognition of at least two communication elements (2,3). The authorisation of a first communication element (2) requires the recognised and authorised presence of a second communication element (3). A secure payment transaction or similar can thus be carried out.

(57) **Zusammenfassung**: Bei einem Verfahren zur geschützten bidirektionalen Datenkommunikation zwischen einer zu autorisierenden Person (16) und einer Verifikations-Einrichtung (1) erfolgt eine Autorisierung durch wechselseitige Identifikation mindestens zweier Kommunikationselemente (2,3). Die Autorisierung eines ersten Kommunikationselementes (2) erfordert die identifizierte und autorisierte Anwesenheit eines zweiten Kommunikationselementes (3). So kann ein gesicherter Bezahlvorgang odgl. durchgeführt werden.

Beschreibung

Verfahren und Vorrichtung zur Identifikation und Verifikation von Zugriffsberechtigungen

Anwendungsgebiet und Stand der Technik

Die Erfindung betrifft ein Verfahren zur geschützten bidirektionalen Datenkommunikation zwischen einer zu autorisierenden Person oder einem zu autorisierenden Objekt und einer Verifikations-Einrichtung sowie eine Vorrichtung zur geschützten bidirektionalen Datenkommunikation.

Geschützte bidirektionale Datenkommunikation wird heutzutage immer wichtiger und ist vor allem beim bargeldlosen Bezahlen von großer Bedeutung. Dieses bargeldlose Bezahlen soll in Zukunft noch berührungsfreier und möglichst komfortabel als Mobile Payment für eine Bedienperson ablaufen.

Die gezielte Zuweisung von Zugangsberechtigungen stellt sowohl in der realen als auch der digitalen Welt die Grundlage zur Sicherung von geistigem, virtuellem und realem Eigentum dar. Während für viele Elemente des realen Lebens ein einfacher Schlüssel immer noch gute Dienste leistet, kommen in der Welt der virtuellen und geistigen Güter immer ausgefeiltere Sicherungssysteme zum Einsatz, die im ständigen Wettlauf mit kriminellen Kräften wie beispielsweise Computer-Hackern stehen.

Der einzelnen Person werden dabei nicht selten Sorgfaltspflichten auferlegt, die er im täglichen Einsatz nur schwer erfüllen kann. Dass eine Person ihr Bargeld unter Verschluss oder Aufsicht hält, ist dabei noch die einfachste und selbstverständlichste Pflicht. Doch Bargeld ist heute nicht mehr das einzige Zahlungsmittel: von der EC-Karte über Kreditkarten bis zur E-Mail steht eine Vielzahl von Instrumenten zur Verfügung, die beim

täglichen Einkauf in Einkaufszentren ebenso zur Anwendung kommt wie beim Besuch eines Onlineshops.

Der Besitzer einer entsprechenden Plastikkarte kann diese meist nur in Verbindung mit Sicherheitsmerkmalen wie einem Lichtbild, seiner Unterschrift oder einer mehrstelligen PIN einsetzen, um sich als rechtmäßiger Eigentümer zu legitimieren.

Über den Sinn oder Unsinn der auf der Karte aufgebrachten Unterschrift lässt sich zudem streiten, da ein potenzieller Kreditkartenbetrüger damit eine einfach zu nutzende Vorlage zum Üben in der Hand hält. Das Lichtbild im Miniaturformat ähnelt nicht selten sogar weiteren Menschen, die an derselben Kasse anstehen.

Eine mehrstellige PIN wäre somit das einzige Sicherheitsmerkmal, das eine gewisse Zuverlässigkeit bietet und wird daher auch systemübergreifend von nahezu jedem Anbieter eingesetzt. Das Problem hierbei ist jedoch: merken können sich die meisten Menschen nur äußerst unsichere PINs mit 4 bis 5 Stellen. Und auch das ist in Frage gestellt, wenn man über mehrere Karten mit demzufolge mehreren PINs verfügt.

Heutzutage gehören unzählige PINs, Usernamen und Passwörter zum Alltag wie der Hausschlüssel. Die Grenzen der Merkfähigkeit sind damit bei den meisten Menschen bereits überschritten. Und ein selbst 5-stelliger PIN-Code stellt keine Hürde für einen einigermaßen versierten Kriminellen dar. Ausgefeilte sog. Skimming-Methoden dienen dazu, die PIN-Codes direkt bei der Eingabe, beispielsweise am Geldautomaten, durch versteckte Kameras abzugreifen.

Es besteht ein umfassender und dringender Bedarf an einem verbesserten bzw. neuen Verfahren und einer Vorrichtung zur Sicherung persönlicher Zugriffsberechtigungen, sei es im Bereich Kreditkarten, elektronischer Schlösser für Gebäude oder Fahrzeuge oder im weiten Feld be-

zahlter Online-Anwendungen wie Shops, Services, etc. Dies umfasst den Schutz vor Missbrauch, Betrug, Entwendung und Verlust sowie vor Vergessen von gemerkten PIN-Codes.

Aufgabe und Lösung

Der Erfindung liegt die Aufgabe zugrunde, ein eingangs genanntes Verfahren sowie eine entsprechende Vorrichtung zu schaffen, mit denen Probleme des Standes der Technik gelöst werden können und es insbesondere möglich ist, Bezahlungsvorgänge noch berührungsfreier und komfortabler abzuwickeln.

Gelöst wird diese Aufgabe durch ein Verfahren mit den Merkmalen des Anspruchs 1 sowie eine Vorrichtung mit den Merkmalen des Anspruchs 15. Vorteilhafte sowie bevorzugte Ausgestaltungen der Erfindung sind Gegenstand der weiteren Ansprüche und werden im Folgenden näher erläutert. Dabei werden manche der Merkmale nur für das Verfahren oder nur für die Vorrichtung beschrieben. Sie sollen jedoch unabhängig davon sowohl für das Verfahren als auch für die Vorrichtung selbstständig gelten können. Der Wortlaut der Ansprüche wird durch ausdrückliche Bezugnahme zum Inhalt der Beschreibung gemacht.

Es ist für das Verfahren vorgesehen, dass die geschützte bidirektionale Datenkommunikation zwischen einer zu autorisierenden Person oder einem zu autorisierenden Objekt und einem Verifikations-Ort bzw. einer Verifikations-Einrichtung erfolgt. Diese Verifikations-Einrichtung kann eine Kasse bzw. eine Art Kassenstation in einem Geschäft oder eine automatische Zahlstelle bzw. ein Automat sein. Ebenso kann es eine elektronische Schließeinrichtung odgl. sein.

Erfindungsgemäß ist vorgesehen, dass die Autorisierung durch wechselseitige Identifikation mindestens zweier Kommunikationselemente bzw. Kommunikationsmittel erfolgt. Dabei erfordert die Autorisierung ei-

nes ersten Kommunikationselementes die identifizierte und autorisierte Anwesenheit mindestens eines zweiten Kommunikationselementes, evtl. sogar mehrerer weiterer Kommunikationselemente, also unter Umständen auch drei oder vier Kommunikationselemente. Dies bedeutet also, dass die Autorisierung des ersten Kommunikationselementes nur dann erfolgt, wenn mindestens ein zweites Kommunikationselement anwesend ist. Anwesenheit bedeutet im Rahmen der Erfindung eine gewisse Nähe zum ersten Kommunikationselement bzw. zur Verifikations-Einrichtung, vorzugsweise eine Entfernung von maximal 10m, vorteilhaft weniger als 2m bzw. weniger als 1m oder sogar weniger als 0,3m bzw. 0,2m. Durch eine verringerte Reichweite wird die Sicherheit stark erhöht, da die Überwachung eines kleinen Raums viel einfacher ist für eine Person.

Durch dieses weitere Kommunikationselement bzw. Kommunikationsmittel, welches die nutzende Person mit dem ersten Kommunikationselement bzw. Kommunikationsmittel bei sich trägt, kann sichergestellt werden, dass kein Missbrauch betrieben wird durch Entwenden des ersten Kommunikationselements bzw. Kommunikationsmittels oder wenn es die nutzende Person zum Zahlen aus der Hand gibt. Dann müsste ein Dieb beide Kommunikationselemente bzw. Kommunikationsmittel stehlen bzw. in seine Gewalt bringen.

Unter Umständen kann das weitere Kommunikationselement auch versteckt getragen werden, da es zum Zahlvorgang bzw. zum Autorisieren eines geschützten Vorgangs gar nicht hervorgeholt werden muss. Dies wird nachfolgend noch im Detail ausgeführt.

In Ausgestaltung der Erfindung kann eines der beiden oder insgesamt mehreren Kommunikationselemente nach der Identifikation durch die Verifikations-Einrichtung Daten zur Weiterverarbeitung an sie übermitteln, die durch sie selbst oder durch damit verbundene Datenverarbeitungs-Systeme weiter verarbeitet werden können. Diese verarbeite-

ten Daten können dann auch an das weitere oder jeweils andere Kommunikationselement übermittelt werden, beispielsweise als Information über den gerade autorisierten Vorgang oder als hinzugefügte Information.

Bevorzugt kann die Verifikations-Einrichtung nach Verifikation mindestens zweier zusammen gehörender autorisierter Kommunikationselemente weitere Datenverarbeitungsroutinen und Funktionen auslösen. Diese können neben der Abwicklung des autorisierten Vorgangs, also beispielsweise einem Zahlvorgang, dazu dienen, diesen abzuspeichern, auszuwerten oder auch für weitere Sicherheitsabfragen bzw. Plausibiltätsabfragen zu verwenden.

Vorteilhaft erfolgt eine Datenübertragung bzw. Kommunikation zwischen Kommunikationselementen und der Verifikations-Einrichtung drahtlos bzw. per Funk, unter Umständen mit Standards wie Bluetooth. Ebenso ist die Verwendung von NFC möglich, dann aber eben nur auf sehr geringe Entfernung. Die Funktechnik kann der gewünschten Reichweite angepasst sein und sollte aus Sicherheitsgründen vorteilhaft nicht zu weit reichen.

Es ist auch möglich, dass die Kommunikationselemente Transponder aufweisen. Diese können unter Umständen auch beschreibbar bzw. änderbar sein. So können sie auch sehr dünn ausgebildet werden und benötigen keine Energieversorgung.

Vorteilhaft kann ein Kommunikationselement an mobilen Objekten fixiert oder ausgebildet werden. Es kann unter Umständen auch vorgesehen sein, dass ein Kommunikationselement selbsthaftend ist. So kann es eine Person beliebig oder nach Bedarf anordnen bzw. verwenden.

In Ausgestaltung der Erfindung kann ein Kommunikationselement als Bezahlungs-Transaktionskarte ausgelegt sein, also sehr dünn. Dies ist

vorteilhaft das erste Kommunikationselement, das aus der Hand gegeben werden kann entsprechend einer Kreditkarte. Weitere Möglichkeiten, insbesondere für das oder die weiteren Kommunikationselemente sind als Schlüsselkarte oder -anhänger, als Schmuck bzw. Ring, Armband oder Halskette oder in Kleidungsstücke eingearbeitet.

In anderer Ausgestaltung der Erfindung kann vorgesehen sein, dass ein Kommunikationselement in digitaler Form auf mobilen oder stationären Endgeräten ausgebildet ist. Dies sind vorteilhaft Mobiltelefone oder Tablet-Computer.

Zur Erhöhung der Sicherheit kann ein bidirektionaler Identifikations-, Autorisierungs-, und Verifikationsvorgang innerhalb eines limitierten Zeitfensters und/oder Entfernungsfensters erfolgen. So ist ein Betrugsversuch stark erschwert, insbesondere wenn versucht wird, verschlüsselte Funksignale zu entschlüsseln. Ein Zeitfenster kann im Bereich kleiner als Stunde oder sogar eine Minute liegen, vorteilhaft kleiner 20 oder 30 sec. Ein Entfernungsfenster kann im vorgenannten Bereich von maximal 10m, vorteilhaft weniger als 2m bzw. weniger als 1m oder sogar weniger als 0,3m bzw. 0,2m liegen.

Es kann vorgesehen sein, dass bei jedem Identifikations-, Autorisierungs-, und/oder Verifikationsvorgang, insbesondere Bezahlvorgang, von einem zentralen Server ein Transaktions-Code mit geringer Lebensdauer, vorzugsweise weniger als eine Stunde oder weniger als 5 Minuten, erzeugt wird zur Autorisierung der aktuellen Transaktion. Er kann also nur relativ kurz benutzt werden.

Die vom Kommunikationselement übertragenen Daten können aus statischen, an das Kommunikationselement gebundenen, Daten und dynamischen, während des Autorisierungsvorgangs erzeugten, Daten bestehen. Dieses Datenpaket kann an der Verifikations-Einrichtung modifiziert und anschließend wahlweise in eines oder mehrere der Kommunikati-

onselemente zurückgeschrieben werden. So kann ein neuer Sicherheitscode erzeugt und im Kommunikationselement abgespeichert werden. Ebenso ist eine Anpassung an neue Systeme zur Verwendung damit möglich.

Vorteilhaft können nach erfolgter Autorisierung und Verifikation vom Autorisierungsvorgang und Verifikationsvorgang unabhängige Daten in einem oder mehreren Kommunikationselementen gespeichert werden. Diese Daten können aus externen Quellen über verbundene Datenverarbeitungs-Systeme gelesen werden und können umgekehrt auch wieder von dort gelesen werden. So ist eine Einbindung in große DV- und Zahlungssysteme möglich.

Es kann vorgesehen sein, dass im Falle einer nicht erfolgreichen Autorisierung, also ohne Autorisierung, eine entsprechende Information mindestens eines, vorteilhaft in alle Kommunikationselemente, zurückgeschrieben bzw. dort gespeichert wird. Dann kann beispielsweise eine weitere Autorisierung oder ein Vorgang nur auf spezielle abgesicherte Weise durchgeführt werden oder nur an bestimmten Verifikations-Einrichtung. Dies dient quasi zur Sicherheitsüberprüfung.

Eine erfindungsgemäße Vorrichtung zur geschützten bidirektionalen Datenkommunikation kann mindestens zwei Kommunikationselemente aufweisen, die mit Übertragern, beispielsweise Funkmodulen oder Transpondern, ausgestattet sind. Es kann mindestens eine Verifikations-Einrichtung vorgesehen sein, die drahtlos oder drahtgebunden, zum Zwecke des Datenaustauschs zur Identifikation, Verifikation und Autorisierung von Transaktionen oder anderen Datenbewegungen damit in Verbindung steht.

Diese und weitere Merkmale gehen außer aus den Ansprüchen auch aus der Beschreibung und den Zeichnungen hervor, wobei die einzelnen Merkmale jeweils für sich allein oder zu mehreren in Form von Unter-

kombination bei einer Ausführungsform der Erfindung und auf anderen Gebieten verwirklicht sein und vorteilhafte sowie für sich schutzfähige Ausführungen darstellen können, für die hier Schutz beansprucht wird. Die Unterteilung der Anmeldung in einzelne Abschnitte sowie Zwischenüberschriften beschränken die unter diesen gemachten Aussagen nicht in ihrer Allgemeingültigkeit.

Kurzbeschreibung der Zeichnungen

Ausführungsbeispiele der Erfindung sind in den Zeichnungen schematisch dargestellt und werden im Folgenden näher erläutert. In den Zeichnungen zeigen:

Abb. 1 Eine schematische Darstellung eines Zahlungsvorgangs gemäß der Erfindung an einer Kasse und

Abb. 2 eine schematische Darstellung von Datenströmen zwischen Verifikations-Einrichtung und Komunikationselementen

Detaillierte Beschreibung der Ausführungsbeispiele

In Abbildung 1 sind ein Verfahren und eine Vorrichtung dargestellt zur geschützten Datenkommunikation zwischen einem Daten-Sender und einem Bezahl-Terminal (1) als Daten-Rezipienten, beispielsweise einer Kasse oder einem Zahlautomat, unter Verwendung mindestens zweier sich gegenseitig autorisierender Kommunikationselemente als Daten-Sender, die vorteilhaft RFID-Transponder (2,3) sein können. Sie können beispielsweise als Kredit- oder Schlüsselkarten (19,20) ausgelegt sein bzw. darauf ausgebildet sein. Der Kunde (16) eines mit auf Transponder-Technologie basierendem Bezahl-Terminal (1) ausgestatteten Geschäfts legt zur Bezahlung seine ebenfalls mit einem Transponder ausgestattete Kreditkarte (19) vor, während er an anderer Stelle, beispielsweise an seiner Uhr (18), seinem Handy oder an seiner Brille, einen zugehörigen Transponder mit sich führt. Das Bezahl-Terminal (1) erkennt

den Transponder seiner Kreditkarte (19,20) und sucht nun den zugehörigen zweiten Transponder (3). Nach innerhalb eines engen Zeitfensters erfolgreichem Datenaustausch und Rückschreiben neu erzeugter, verschlüsselter Datenblöcke in den zweiten Transponder (3) gibt das Bezahl-Terminal (1) den Zahlungsvorgang frei. Ein PIN-Code, eine Unterschrift oder ein Lichtbild sind somit überflüssig. Alle bekannten Skimming- bzw. Betrugs-Methoden greifen dann nicht mehr.

Findet dennoch ein Diebstahl der Karte statt oder geht diese verloren, ist ein Einsatz als Zahlungsmittel ohne die Anwesenheit des zweiten Transponders unmöglich, die Karte alleine ist ohne mindestens einen Partner-Transponder wertlos.

Ein Abhören des Datenverkehrs zwischen Transpondern (2,3) und Bezahl-Terminal (1), um mit Hilfe der gestohlenen Daten ein Duplikat zu erzeugen (sogenannter Man in the Middle) ist sinnlos, da bei jedem Bezahlvorgang von einem zentralen Server ein Transaktions-Code (ähnlich einer mobilen TAN beim mobilen Online-Banking) mit geringer Lebensdauer, beispielsweise eine Stunde oder weniger, erzeugt wird, der die aktuelle Transaktion autorisiert.

Erkennt das Bezahl-Terminal (1) eine Abweichung der Daten-Blöcke in Bezug auf Transponder-Kennung, ID oder den verwendeten Time-Stamp, wird diese Information zurück in die Transponder geschrieben, so dass direkt am Bezahl-Terminal (1) der Diebstahl mit allen Konsequenzen direkt angezeigt werden kann.

Die vorliegende Erfindung verhindert nahezu alle bekannten Betrugs- und Verlustproblematiken bei EC- oder Kreditkarten, ermöglicht sichere Tür- und Autoschlösser sowie das sichere Bezahlen per Karte über das Internet durch z.B. RFID-Tastaturen oder -Mäuse oder RFID-fähige Handys oder durch Versand bankunabhängiger mobiler TANs.

Durch die Beschreibbarkeit der Transponder sind Zusatzfunktionen wie das Tracking von Fahrtzeiten bei Fahrzeugen oder die Nutzungszeiten von Geräten und Systemen einschließlich Nutzungsdaten möglich.

In Abbildung 1 ist ein Kunde (16) eines Ladengeschäfts mit einer Verkäuferin (17) dargestellt. Der Kunde (16) hält das Kommunikationselement (2) vor die Verifikations-Einrichtung (1), hier als Kasse dargestellt. Der Kunde (16) trägt an seiner Armbanduhr (18) ein zweites Kommunikationselement (3), das nach gegenseitiger Identifikation, Verifikation und Autorisierung den Datentransfer von der Verifikations-Einrichtung (1) zum Datenverarbeitungs-System (4) frei gibt. Somit kann die Transaktion, hier die Bezahlung der Ware, erfolgreich abgeschlossen werden.

In Abbildung 2 sind die Datenströme zwischen der Verifikations-Einrichtung und den Kommunikationselementen (2) und (3) dargestellt. Es wird zunächst die RFIDCheck-Kennung und die zugehörige ID des Transponders von Kommunikationselement (2) ausgelesen (Schritt 5) und das Element identifiziert. Kennung und ID werden an die Verifikations-Einrichtung (1) übergeben (Schritt 6). Anschließend erfolgt anhand der Identifikations-Daten ein Abgleich mit Kommunikationselement (3) durch Auslesen und Zurückschreiben von Kennung und ID (Schritt 7,8).

Nach erfolgreichem Abgleich werden beide ID sowie die Kennungen an das Datenverarbeitungs-System (4) übertragen (13,15) und es erfolgt die Rückgabe (14) neu generierter IDs an die beiden Kommunikationselemente (2) und (3) (Schritt 9,10,11,12).

Die Übertragung läuft hierbei über die Verifikations-Einrichtung (1), die die Kommunikation zwischen allen Komponenten steuert.

- - - - - - - - - -

Patentansprüche

1. Verfahren zur geschützten bidirektionalen Datenkommunikation zwischen einer zu autorisierenden Person (16) oder einem zu autorisierenden Objekt und einer Verifikations-Einrichtung (1), dadurch gekennzeichnet, dass eine Autorisierung durch wechselseitige Identifikation mindestens zweier Kommunikationselemente (2,3) erfolgt und dass die Autorisierung eines ersten Kommunikationselementes (2) die identifizierte und autorisierte Anwesenheit eines zweiten Kommunikationselementes (3) erfordert.

2. Verfahren nach Anspruch 1, dadurch gekennzeichnet, dass eines der beiden Kommunikationselemente (2,3) nach der Identifikation durch die Verifikations-Einrichtung (1) Daten an diesen zur Weiterverarbeitung durch den Verifikations-Ort (1) selbst oder damit verbundene Datenverarbeitungs-Systeme (4) übermittelt, wobei dass diese verarbeiteten Daten an das andere oder weitere Kommunikationselemente (3) übermittelt werden.

3. Verfahren nach Anspruch 1 oder 2, dadurch gekennzeichnet, dass die Verifikations-Einrichtung (1) nach Verifikation mindestens zweier autorisierter Kommunikationselemente (2,3) weitere Datenverarbeitungsroutinen und Funktionen auslöst.

4. Verfahren nach einem der vorangegangenen Ansprüche, dadurch gekennzeichnet, dass die Kommunikationselemente (2,3) Transponder aufweisen.

5. Verfahren nach einem der vorangegangenen Ansprüche, dadurch gekennzeichnet, dass ein Kommunikationselement (3) an mobilen Objekten (18) fixierbar ist, insbesondere selbsthaftend ist.

6. Verfahren nach einem der vorangegangenen Ansprüche, dadurch gekennzeichnet, dass die Kommunikation zwischen Kommunikationselementen (2,3) und der Verifikations-Einrichtung (1) drahtlos erfolgt.

7. Verfahren nach einem der vorangegangenen Ansprüche, dadurch gekennzeichnet, dass ein Kommunikationselement (2) als Bezahlungs-Transaktionskarte (19) ausgebildet ist.

8. Verfahren nach einem der Ansprüche 1 bis 6, dadurch gekennzeichnet, dass ein Kommunikationselement (2) als Schlüsselkarte (20) ausgebildet ist.

9. Verfahren nach einem der Ansprüche 1 bis 6, dadurch gekennzeichnet, dass ein Kommunikationselement in digitaler Form auf mobilen oder stationären Endgeräten ausgebildet ist oder von diesen gebildet ist.

10. Verfahren nach einem der vorangegangenen Ansprüche, dadurch gekennzeichnet, dass ein bidirektionale Identifikations-, Autorisierungs-, und/oder Verifikationsvorgang innerhalb eines limitierten Zeitfensters und/oder Entfernungsfensters erfolgt.

11. Verfahren nach einem der vorangegangenen Ansprüche, dadurch gekennzeichnet, dass bei jedem Identifikations-, Autorisierungs-, und/oder Verifikationsvorgang, insbesondere Bezahlvorgang, von einem zentralen Server ein Transaktions-Code mit geringer Lebensdauer, vorzugsweise weniger als eine Stunde oder weniger als 5 Minuten, erzeugt wird zur Autorisierung der aktuellen Transaktion.

12. Verfahren nach einem der vorangegangenen Ansprüche, dadurch gekennzeichnet, dass die vom Kommunikationselement übertragenen Daten aus statischen, an das Kommunikationselement gebundenen Daten, und dynamischen, während des Autorisierungsvorgangs erzeugten Daten bestehen, wobei vorzugsweise diese Daten als Datenpaket an der Verifikations-Einrichtung (1) modifiziert und anschließend wahlweise in eines oder mehrere der Kommunikationselemente zurückgeschrieben werden.

13. Verfahren nach einem der vorangegangenen Ansprüche, dadurch gekennzeichnet, dass nach erfolgter Autorisierung und Verifikation vom Autorisierungsvorgang und Verifikationsvorgang unabhängige Daten in einem oder mehreren Kommunikationselementen (2,3) gespeichert werden, die aus externen Quellen über verbundene Datenverarbeitungs-Systeme (4) gelesen werden und die umgekehrt auch wieder von dort gelesen werden.

14. Verfahren nach einem der vorangegangenen Ansprüche, dadurch gekennzeichnet, dass im Falle nicht erfolgreicher Autorisierung diese Information in mindestens ein Kommunikationselement (2,3) zurückgeschrieben wird, vorzugsweise in alle Kommunikationselemente (2,3).

15. Vorrichtung zur geschützten bidirektionalen Datenkommunikation mit einem Verfahren nach einem der vorangegangenen Ansprüche, dadurch gekennzeichnet, dass die Vorrichtung mindestens zwei Kommunikationselemente (2,3) aufweist, die mit Transpondern ausgestattet sind und mit mindestens einer Verifikations-Einrichtung (1) drahtlos oder drahtgebunden in Verbindung stehen zum Zwecke des Datenaustauschs zur Identifikation, Verifikation und Autorisierung von Transaktionen oder anderen Datenbewegungen.

- - - - - - - - - -

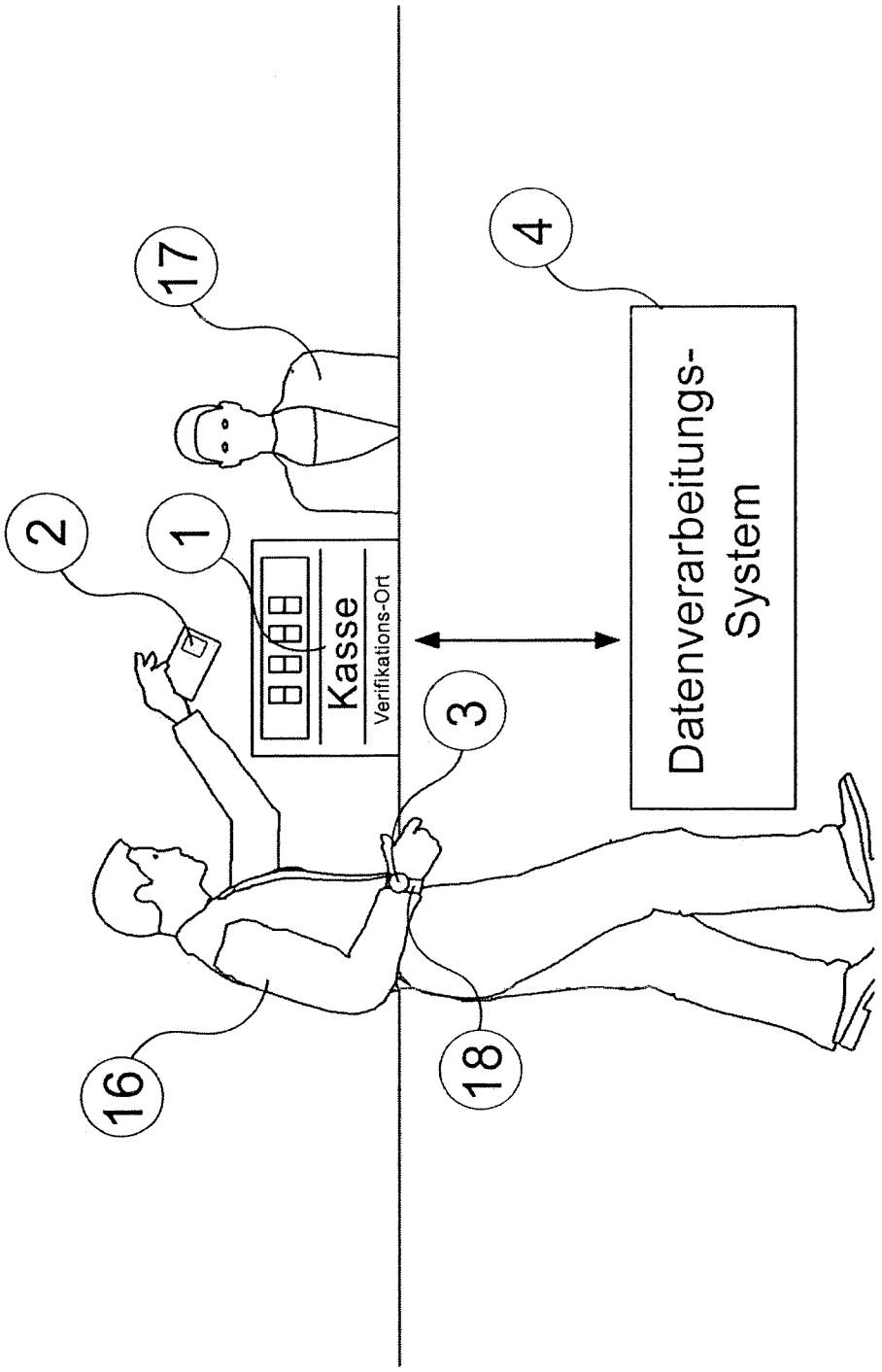

17
4
2
1
Kasse
Verifikations-Ort
Datenverarbeitungs-
System
3
16
18

Abbildung 1

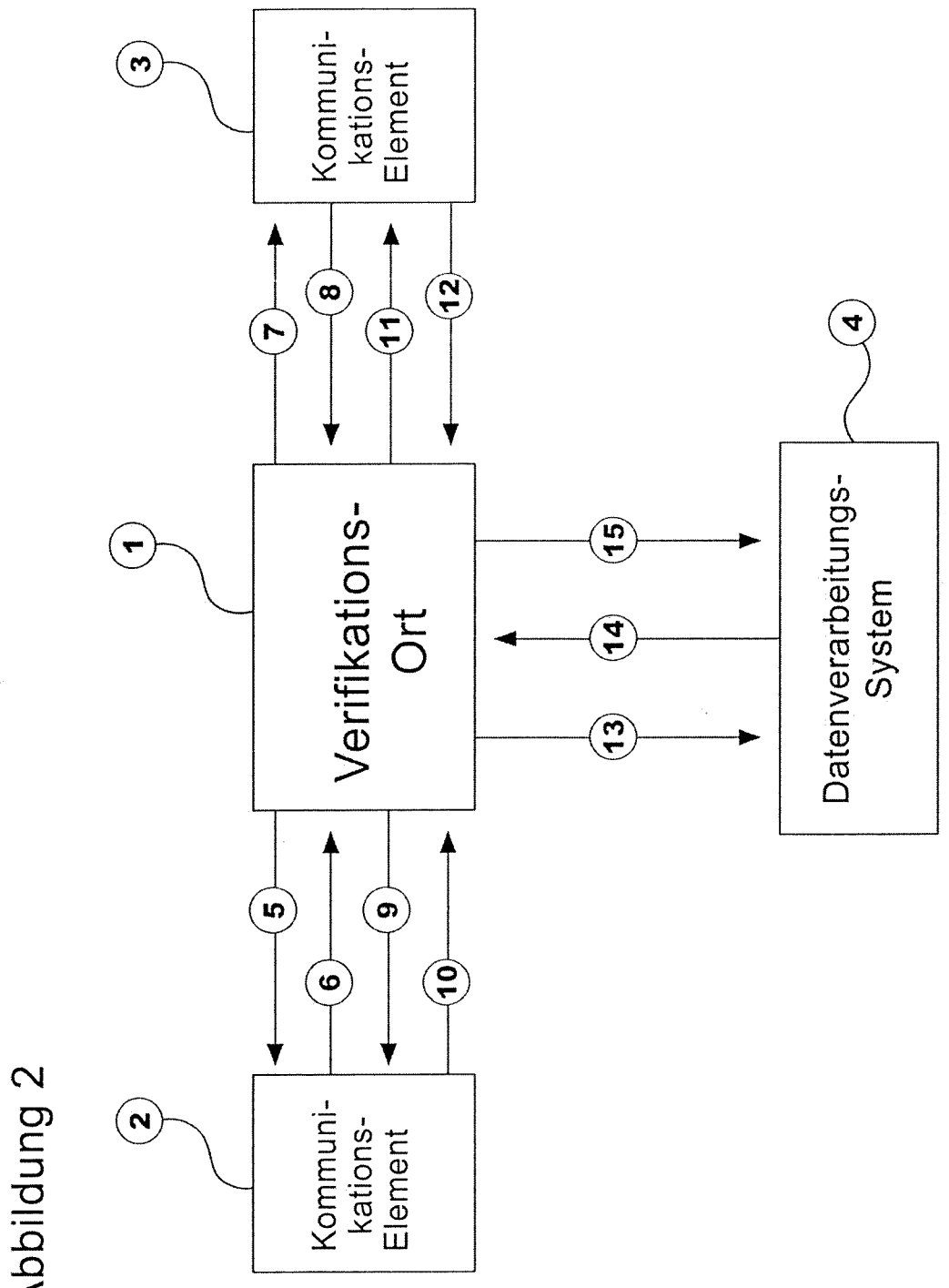

Kommuni-
kations-
Element
3
7
8
11
12
1
Verifikations-
Ort
15
14
13
4
Datenverarbeitungs-
System
5
6
9
10
Kommuni-
kations-
Element
2

Abbildung 2