(19) SCHWEIZERISCHE EIDGENOSSENSCHAFT
EIDGENÖSSISCHES INSTITUT FÜR GEISTIGES EIGENTUM

(11) CH 698 211 B1

(51) Int. Cl.: H04W 4/00 (2009.01)
G06Q 90/00 (2006.01)

Erfindungspatent für die Schweiz und Liechtenstein
Schweizerisch-liechtensteinischer Patentschutzvertrag vom 22. Dezember 1978

(12) PATENTSCHRIFT

(21) Anmeldenummer: 02072/03

(22) Anmeldedatum: 19.03.2004

(24) Patent erteilt: 15.06.2009

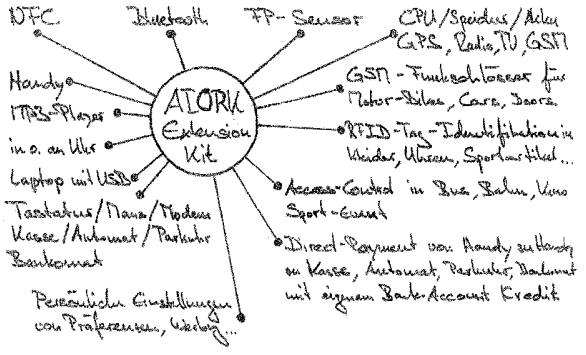
(45) Patentschrift veröffentlicht: 15.06.2009

(73) Inhaber:
Roger Humbel, St. Niklausstiege 2
5400 Baden (CH)

(72) Erfinder:
Roger Marcel Humbel, 5405 Baden-Dättwil (CH)

(54) Handy (Pass-Partout) für Funk-Schlösser, RFID-Tags und Zahlungsverkehr etc. «All In One Remote Key» (AIORK).

(57) Der «All In One Remote Key» (AIORK) für (GSM, UMTS, W-LAN, Bluetooth, RFID-transceiver) Handys und/oder Extension Kits ist ein universeller Schlüssel für alle Arten von Schlössern, Schleusen oder Zutritte und hat eine direkte Zahlungs- und Abrechnungs-Funktion für elektronische (NFC, RFID- oder auch Bluetooth) Cash Zahlungen, alle konsumierten Zutritte oder sonstigen Services, Applikationen oder Informationen. Die Transaktions-Eingabe/Bestätigung kann mit Fingern oder oral mit direkter biometrischer Sensor Bestätigung gemacht werden. Diese Handy NFC-Transceiver-Verwendung ist für: Info-Download, Direct-Cash-Payment, Access-Control, Funktionskontrollen, Autentifizierung von Internet-Auktionen, -Wett und -Börsen Transaktionen und deren Informationen oder zur RFID-Tag Identifikation von Wert-Gegenständen, elektronischen Geräten und Bauteilen etc. mit GSM basierter Internet Web-Siten bzw. Account Abbuchung und Ortung.



Beschreibung

Bezeichnung der Erfindung

Technisches Gebiet/Einleitung/Zusammenfassung

[0001] Der über ein Gerät mit mehreren Sendern (GSM, Bluetooth, NFC, W-LAN) und mit einem Fingerprint-Sensor laufende «All In One Remote Key» (AIORK) (Zugriff, Code, Nummer, Passwort, ID, Authentifizierung, Autorisation, Kauf, Verkauf, Bezahlung, Funktionskontrolle Gerät mit Fingerprintsensor für eine direkte Bewertung und für den Zugriff auf ein Interaktives Internet bzw. Mobile-Phone-Portal mit Video Hit-List, Hit-Chart bzw. Hit-Parade, Content, Fernseh-Kanal, Spiel, Service, Dienste, Produkten, Software-Implementierung, Autorisationen, Abstimmungen, Rechten und Pflichten, Spielen, Partnervermittlungen, Börsen-, Wett-, Wirtschafts- u. Zahlungs-Verkehr Einstell-Möglichkeiten) ist in einem Handy- oder Extension Kit Gerät, einer Software und einer Liste für das Öffnen, den Zugriff, die Verwendung (zwischen Schlüssel, d.h. für eine Teil-Funktion (z.B. nur Vibra-Alarm in Kino, nur SMS, Filter-Funktionen, Werbung etc.)), zusätzliche Info, die Autorisation und das Orten für ein oder mehrere Funk (Fahrrad, Auto, Haus) Schlösser oder Schlüssel gleichzeitig oder ungleichzeitig (z.B. für ganze Garage oder nur Auto etc.) und für M-Payment wie auch RFID-Tag- und weitere Applikationen.

Erfindung und Neuheit

[0002] Bis Dato gibt es unseres Erachtens keine Kamera-Handy und Abhör-Sender gesicherte Lösung für M-Payment, Access-Control und Funk-Schloss Applikationen. Insbesondere für die verschiedenen neuen GSM und Bluetooth Funk-Schlösser an Fahrrädern, Motorrädern und PKWs bzw. LKWs oder gar Garagetoren gab es noch nicht einen einzigen Schlüssel, der insbesondere mit einem Fingerprintsensor über NFC auch M-Payment Applikationen führen liess mit direkter oder indirekter GSM-Netz Abbuchung auf ein Bank-Konto. Eine über Handys auch mit NFC ausgestattete laufende RFID-Tag Applikation zur Registrierung von Eigentum mit solchen RFID-Tags gibt es auch noch nicht. Insbesondere gibt es noch nicht, dass diese neue Applikation zusammen mit den anderen neuen über Fingerprintsensoren authentifizierbaren auch auf NFC basierenden M-Payment und in Funk-Schlössern integrierten Bluetooth-Modulen basierenden Applikationen auf einer Software über eine Liste in einem Gerät gemanaged werden können.

Stand der Technik

[0003] Stand der Technik sind Handy-Schlüssel über GSM oder Bluetooth Transceivers wie in folgender Liste. D.h. folgende Schlüssel-Funktionen existieren schon bei Handys und können nicht als neue technische AIORK Entwicklung bzw. Lösung einzeln beansprucht werden, aber natürlich alle weiter unten aufgelisteten neuen «Schlüssel» etc. in Kombination mit diesen hier eben folgenden schon existierenden Handy Schlüssel, Programmen etc.:
– Telephone calls
– Any other Software download
– Games, Lotteries, Stock-Exchange
– Video and Music download
– Money, Payment and Cash Transactions
– 911, 211 Emergency Calls
– Cars, Garages and Motor-Bikes

[0004] Die «All In One Remote Key» (AIORK) technische Entwicklung bzw. Lösung ist für Handy oder solche -Software Firmen wie Symbian, Openwave, Nokia oder Siemens. Die Eingabe kann mit Fingern oder oral mit direkter biometrischer Bestätigung (Autorisation) gemacht werden.

[0005] Da mindestens RFID-Tag Erkennung und Direct-Payment, Parcel-Delivery bzw. Access-Control Funktionen mit biometrischem (Fingerprint-) Sensor und doppeltem zweitem Account-Code (wie Direct-Net) über NFC als auch alle (GPS, GSM, Bluetooth) Funk (Fahrrad) Schlösser sicher neu sind, ist dieses Merkmal des AIORK für alle Fahrzeuge etc. in einem einzigen Handy neu als auch erfinderisch und macht äussest viel Sinn, denn damit gibt es die Exklusivität, dass nur mit einem Handy alle diese verschiedenen Schlösser geöffnet werden dürfen oder die NFC-Direct-Payment, -Access-Control und -RFID-Applikationen mit einem Gerät, einer Software oder einer Liste geführt werden können. Wer möchte denn schon mehrere Handys mit sich herumtragen für jede einzelne dieser neuen Applikationen?

[0006] Solche WAP-Handys oder Zusatz-Extension-Kits mit ständiger Web-Übermittlung, welche Funk-Schlösser oder sich selber öffnen und verriegeln/abschalten können und mit Bluetooth, geschweige dann NFC und einem biometrischem Fingerprint- oder Kamera-Sensor oder Spracherkennungs-Software ausgestattet sind, gab es bisher noch nicht. Und es gab noch keine Funk-Schlösser mit GSM-, Bluetooth, NFC und Infrarot Transceiver oder Handys mit NFC-RFID-Tag Reader für Zahlungs-Applikationen. Zwar gab es Bluetooth Garagen-Türen, aber ohne Internet-, geschweige dann GSM-Anschluss und Alarm-Übermittlung oder direktem Management (öffnen, verriegeln, autorisieren, selektionieren).

[0007] Auch Handys oder -Zusatz-Kits, welche RFID-Tags oder andere NFC Transceiver mit NFC Transceiver auslesen, gab es noch nicht, insbesondere nicht mit biometrischem Authentifizierungs Fingerprint-Sensor und direkt über ein Kabel daran befestigte bzw. angeschlossene Schlüssel(Bunde) oder Zentralverriegelungen für Auto!

[0008] NFC ist Near Field Communication auf 13.56 MHz Frequenz und kann per Definition nur ca. 10 cm weit senden. Eine Kombination von Handy oder -Extension Kit mit NFC oder gar Bluetooth und biometrischem (Finger-Print) Sensor gab es bisher noch nicht. Eine Kombination von Handy oder Extension Kit mit NFC oder gar Bluetooth und biometrischem (Fingerprint-) Sensor gab es bisher auch noch nicht und bringt ultimative Direct- bzw. M-Payment etc. -Vorteile, weil keine Spionage-Sender wie bei Bluetooth die sensitiven Daten erfassen können.

Darstellung der Erfindung

[0009] Folgende Merkmalskombinationen für all diese neuen (Lock-Loop, RFID etc.) Merkmale in Handys oder Extension Kit werden in dieser AIORK technischen Entwicklung bzw. Lösung beschrieben: -NFC/Bluetooth/W-LAN Haus-, Garagen- und Zimmer-Türen oder Kino-, Sportanlass-, öffentlicher Verkehr, Parkplatz- und Parkhaus- etc. Schleusen mit direkter GSM oder Internet Zahlungsverkehrs-Abrechnung wie über Visa-/Master-Card etc. Bankomat.
– Für die Übertragung und Autorisation von einem Handy-Schlüssel-Set auf ein AIORK Handy oder Extension Kits von einer anderen Person.
– for Downloads von letzter neuester AIORK Schlüssel-Software (falls diese Bluetooth Übertragung entschlüsselt (gehackt) werden könnte) -Fahrräder mit GPS, GSM und Bluetooth-Modul
– Erkennung von Bluetooth, W-LAN, GSM, UMTS RFID-Tags Sendern in Bindungen, Boards, Boots, mobilen GSM-Schlössern, Barryvox, Handys, PDAs, Laptops, Beamers und allen anderen verriegelbaren, offnungsbaren und einstellbaren elektronischen Geräten (für Küche, Garten, Garagen)
– Wegbeschreibungs-Software und LBS Benachrichtigung für Freunde etc.
– Nachrichten, Informationen, Berichte, Handbücher, Werbung von RFID-Tags oder anderen (bluetooth) Sendern und v.a. in Kombinationen von Sendern einstellbar nach gewünschten Filtern (Thema, Geschmack)
– Filter-Funktionen z.B. bei RFID/Bluetooth/W-LAN Werbung etc. (auf das Head-Set etc.) -Schnell Registrierung und Blockierung von RFID-, Bluetooth- etc. Tags und von allen Lock-Loop Internet-WAP-Site registrierten Produkte mit Tags.
– Schüler, Feunde, Familien, Arzt Notfall-Rufe mit Schlüssel-Einstell-Funktion für welche Art von Anrufoder Aktions -Aufnahme oder -Registrierung.
– Fussfesseln oder für Handys von Schüler, Studenten oder Straffälligen, die von Lehrer- oder Behörden-, Club-Chef, oder Familien-Oberhaupt Handys gesteuert, d.h. blockiert etc. werden. -Fahrzeug Nachfolgungs- oder Fahrradfahrer-, Stau-, Unfall-Voraus Alarm-Meldungs System Ein- und Abstellung (bei Kriminellen) für Fahrräder oder PKWs oder LKWs oder sonstige Lock-Loop Produkte. -Clubs zur Information (Mitteilung von Radarfallen oder anderen Dienstleistungen) -Empfangen von allen möglichen (Werbe-) Signalen und automatische Einstellung von Fernsehern oder anderen elektronischen Sendern, Medien und Geräte auf die eingestellten Präferenzen d. Users. -Wenn in einem Raum mehrere Handys auf eine bestimmte Präferenz eingestellt sind, dann wird die mehrheitlich gewünschte bzw. besser bezahlte Info ausgestrahlt.

Erklärung zur erfinderischen Tätigkeit und Neuheit des AIORK

[0010] Unsere beiden AIORK (aktuelle) und Lock-Loop (frühere bzw. vorgängige) technischen Entwicklungen bzw. Lösungen beinhalten folgende hier neu beschriebenen Funktionen bzw. Applikationen (Payment, Ticketing, RFID-Tag Übermittlungen etc.), die man neu über ein mobiles Gerät mit NFC-Sendern betreiben (identifizieren) und über GSM/Internet etc. auf Konten/Server transferieren kann:

[0011] Sowohl mit Handys und bei Schleusen kann man nun diese neuen NFC Identifikationen machen. D.h. nur wir bestimmen bzw. betreiben die Transaktionen und verkaufen damit die (Nummern der) NFC RFID-Tags, welche an Handys und Schleusen identifiziert werden (können) und über GSM/Internet etc. auf Konten/Server transferiert werden.

[0012] Unsere identifizierbare und registrierbaren NFC RFID-Tag Nummern werden exklusiv jeder interessierten Kleidungs- oder Sportartikel-Hersteller- oder anderen insbesondere Elektronik-Hersteller Firma mit dem einzigen weltweit bekannt werdenden Lock-Loop Standard und v.ä. auch Lock-Loop Logo zum Kauf angeboten. D.h. ein Lock-Loop Merkmal ist, dass die NFC RFI D-Tags direkt in den Marken-Logos oder den Kleider-Zettel integriert sind. Das Lock-Loop Logo wird ein «Must» für alle Nobel-, High-Quality- und -Standard Labels (z.B. Nike, Adidas, Esprit, CK oder Sony, Philips, Nokia, Siemens, Mercedes, RR, Samsonite, etc.)...

[0013] Nur wir betreiben eine einzige Web-Plattform für die mind. fünf verschiedenen neuen Applikationen (Handy und Schleusen Identifikation, Registrierung, Alarm, Ortung, Weiterverkauf).

[0014] Das Hauptmerkmal der AIORK Entwicklung ist, dass mit einem einzigen Handy die exklusive Zahlungs-Funktion, Öffnung, Verriegelung, Identifikation, Ortung etc. von RFID-Tags oder Readern über Near Field Communication als auch über Bluetooth, W-LAN und GSM von allen unseren anderen neuen Produkten wie bei Laptops, Video-Cameras und v.a. Funk-(Fahrrad)-Schlösser als auch anderen Fahrzeugen oder Garagen und Türen geführt werden kann... (D.h. es beinhaltet diese technische Entwicklung/Lehre gleich mehrere neue Gegenstände/Ausführungen/Merkmale bzw. Applikationen, wo jede einzelne an sich noch mit je einer der anderen gemeinsam beansprucht wird. D.h. jede der einzelnen Applikationen ist an sich und sowieso zusammen mit den anderen neuen Applikationen in Kombination dargelegt/vorgestellt. Anders ausgedrückt: Jedermann will alle unsere dargelegten Applikationen gleichzeitig nutzen können. D.h. niemand will aber mehr als ein Handy mit sich herumtragen, wenn nicht alle Applikationen auf einem Gerät betrieben werden. Wir werden den Dienst/Service (NFC Transferierungen über GSM/Internet etc. auf Server/Konten) auf für alle diese neuen Applikatio-

nen betreiben und nur wir werden auf einem Handy alle diese NFC-Applikationen anbieten/betreiben. Also werden nur wir alle diese verschiedenen Applikationen gleichzeitig koordiniert kundenfreundlich auf einer Plattform (sowohl Server als auch Handy-Client) anbieten.

[0015] Neben der zentralen Merkmals-Kombination von «NFC-Transceiver, biometrischem (Fingerprint)-Sensor-Identifikation, GSM-Modul und Transaktion auf eine Server/Konto Web-Plattform» in einem Handy oder über ein Extension Kit werden wir wie gesagt bzw. beschrieben die Dienste/Service für die besten Access-Control und Direct-Payment Applikationen haben als auch mit dieser All-In-One-Remote-Key technischen Entwicklung/Lösung noch andere wichtige oder interessante NFC-Applikationen betreiben, weil einfach die Vermarktung solcher marginalen Applikation auch noch für/bei uns notwendig aber auch günstiger werden, wie zum Beispiel die GSM- oder NFC-Ortung von gestohlenen NFC-Produkten, wie z.B. insbesondere gestohlenen oder gar abgestellten Handys.

Beschreibung der Figuren und Abbildungen

[0016] Die Erfindung und die vorteilhaften Ausführungen sind hier folgend beschrieben mit Referenzen zu den schematischen Figuren und Abbildungen. Diese zeigen:

Fig. 1	Eine generelle Darstellung der Funktionen und Applikationen der AIORK-Software auf einer Liste, so wie sie auf einem Display bzw. einem Gerät aussieht
Fig. 2	Auflistung der wichtigsten Sender, Module, Funktionen und Applikationen der AIORK-Software- und Hardware-Lösung
Fig. 3	Darstellung der Funktion der AIORK-Diebstahlsicherheitslösung mit den Bluetooth-Modulen in den Funk-Schlössern von Fahrzeugen

[0017] Der (GSM, Bluetooth) «All In One Remote Key» (AIORK) (Access, Number, Password, ID, Authentication, Autorisation) ist in einem Gerät, einer Software und einer Liste für das Öffnen, den Zugriff, die Verwendung (zwischen Schlüssel, d.h. für eine Teil-Funktion (nur Vibra-Alarm in Kino, nur SMS, Filter-Funktionen z.B. Werbung etc.)), zusätzliche Info, die Autorisation und das Orten für ein oder mehrere Schlösser oder Schlüssel gleichzeitig oder ungleichzeitig (z.B. für ganze Garage oder nur Auto etc.) und die Eingabe kann mit Fingern oder oral mit direkter Bestätigung gemacht werden und umfasst folgende Schlüssel Funktionen:
– NFC/Bluetooth/W-LAN Haus-, Garagen- und Zimmer-Türen oder Kino-, Sportanlass-, öffentlicher Verkehr, Parkplatz- und Parkhaus- etc. Schleusen mit direkter GSM oder Internet Zahlungsverkehrs-Abrechnung wie über Visa-/Master-Card etc. Bankomat.
– Direkt M-Payment von Handy zu Handy oder MP3-Player, Kassen, Automaten, Schleusen,
– für die Übertragung und Autorisation von einem Handy-Schlüssel-Set auf ein Handy von einer anderen Person!
– für Downloads von letzter neuester AIORK Schlüssel-Software (falls diese Bluetooth, NFC, W-LAN, IR etc. Übertragung entschlüsselt (gehackt) werden könnte)
– Funk-Schlösser für (Motor-) Fahrräder, Fahrzeuge
– Funk-Haus-, Garagen- und Zimmer-Türen oder Kino-, Sportanlass-, öffentlicher Verkehr etc.
– Funk-Schleusen mit direkter Zahlungsverkehrs-Abrechnung über Visa-/Master-Card etc.
– (NFC, Bluetooth, W-LAN, GSM, UMTS) RFID-Tags bei Bindungen, Boards, Boots, mobilen GSM-Schlössern, Barryvox, Handys, PDAs, Laptops, Beamers und allen anderen verriegelbaren, offnungsbaren und einstellbaren elektronischen Geräten (für Küche, Garten, Garagen)
– Wegbeschreibungs-Software, um von Punkt A nach B gelotst zu werden.
– Nachrichten, Informationen, Berichte, Handbücher, Werbung von RFID-Tags oder anderen (bluetooth) Sendern und v.a. in Kombinationen von Sendern einstellbar nach gewünschten Filtern (Thema, Geschmack)
– Filter-Funktionen z.B. bei Werbung etc.
– Schnell Registrierung und Blockierung von RFID-Tags und von allen Lock-Loop Internet-WAP-Site registrierten Produkten mit RFID-Tags.
– Schüler, Freunde, Familien, Arzt Notfall-Rufe mit Schlüssel-Einstell-Funktion für welche Art von Anruf- oder Aktions-Aufnahme oder -Registrierung.
– Fussfesseln oder für Handys von Schülern, Studenten oder Straffälligen, die von Lehrer- oder Behörden-, Club-Chef, oder Familien-Oberhaupt Handys gesteuert, d.h. blockiert etc. werden.
– Fahrzeug Nachfolgungs- oder Fahrradfahrer-, Stau-, Unfall-Voraus Alarm-Meldungs System Ein- und Abstellung (bei Kriminellen) für Fahrräder oder PKWs oder LKWs oder sonstige Lock-Loop Produkte.
– Clubs zur Information (Mitteilung von Radarfallen oder anderen Dienstleistungen) oder bei Kumulus-Karten
– Automatische Einstellung von Fernsehern oder anderen elektronischen Geräten
– An Kassen oder bei Verkäufen von registrierten Produkten, kann mit einer einfachen Funktion der Eigentums-Wechsel gegenseitig bestätigt werden, weil der Besitzer ja nur die Autorisation hat, die Namen zur registrierten Nummer zu veröffentlichen.

[0018] Der «All In One Remote Key» (AIORK) ist dadurch gekennzeichnet, dass über ein mit einem Finger-Print-Sensor oder mit einem anderen biometrischen Identifikations Medium ausgestattetes Gerät (Handy, MP3-Player, Uhr) oder ein dazu passendes Zusatzgerät (Extention Kit) mit allen Schnittstellen für deren Schnittstellen (als Hardware wie auch Software) (für Access, Number, Password, ID, Authentication, Autorisation) (mit Speicher, Display, Tastatur, Mikrophon, Lautsprecher, CPU, Akku, Solarpanel, Kamera etc.) und/oder ein damit über Software- und Software-Schnittstellen mechanisch und/oder elektronisch über Funk verbindbares Extention Kit und/oder über eine Software und/oder eine Liste mit einem GSM-, Bluetooth-, NFC-, W-LAN-, UWB-, IrDa-, 125 kHz- oder anderem 10 cm -100 cm kurz-Distanz-Sender-, Radio- und TV- Transceiver verschiedenste elektronische und mechanische Schlüssel in Form von Softwaren und Applikationen laufen für:

[0019] A) M-Payment Applikationen, wo mit NFC, W-LAN, UWB, Bluetooth-, oder sonstigen z.B. 125 kHz Transceivern in einem Gerät wie Handy, Uhr, MP3-Player oder einem damit verbundenen Extention Kit oder mit biometrischer Personen-Identifikation wie z.B. mit einem Fingerprint-Sensor mit diesen bei v.a. direkter Berührung von Gerät zu Gerät oder zu Kasse, Vending Machine, Ticket Machine, Juke Boxe oder Gates etc. eine Zahlung mit Mikropayment getätigt wird, welche direkt oder indirekt mit einer sofortigen oder späteren GSM und iMEI-Nummer als auch Personalien, Biometrie und Konto-Nummer-Daten Übermittlung vom Gerät oder dem damit kommunizierenden Zahlungs-Terminal auf ein Bankkonto abgebucht wird und -Orts-, Zeit-, Raum-, Rechts-Konsumationen wie z.B. Park-Gebühren, Steuererklärungen oder Eintrittspreise direkt über die Transceiver abgebucht werden
– Spielgeld mit direkter Devisenumrechnung laufen
– Miet-, Kauf-, Verkauf-, Spiel-, Wett-, Börsen-Transaktionen und Versicherungs-Policen und Vertrags-Abschlüsse über das Internet und eine Web-Plattform oder direkt autorisiert werden
– Internet Direct-Payment Autorisation mit AIORK- und persönlichem Finger-Print-Sicherheitscode, um Einzahlungsscheine, Checks etc. zur Verbuchung freizugeben und E-Commerce mit Micro- und Macro-Payment über das ans Internet angeschlossene Computer, Handys und Terminals abbuchen zu können.
– akustische und tastbare biometrische Fingerprint-Sensor Regeln mit ein-, zwei-, dreimaliges Berühren oder Streichen laufen oder dass auf dem Handydisplay Preise, Produkte, Listen, Gruppen für schnelles M-Payment vorinstalliert angezeigt sind
– Homebanking auf Handy, Smartphone und PDA als auch Computer werden mit NFC-Transceiver getätigten und mit FP-Sensoren bestätigten Transaktionen gemanaged

[0020] B) das Managen, das Öffnen/Schliessen/Starten, den Zugriff, die Verwendung (zwischen Schlüssel, d.h. für eine Teil-Funktion, zusätzliche Info, die Autorisation und das Orten von einem oder mehrerer Funk-Motor-Fahrrad-, Auto, Heim, Garagen oder sonstiger mobiler oder fixer fester Funk-Schlösser, -Starter oder -Zündungen, wo die Unit-Codes der kommunizierenden Tranceiver sich die Codes, d.h. der Schlüssel gleichzeitig oder ungleichzeitig pairen und wo mit Richtfunk-Antennen -insbesondere über Bluetooth, NFC oder W-LAN, die Richtung zu den nächsten Sendern oder Tags angezeigt werden, wo zusätzlich insbesondere über eine Richt-Funk-Antenne die kürzeste Distanz bzw. die wenigsten Slaves zum Erreichen des gewünschten Senders oder Tags berechnet und angezeigt werden und über eine weitere Intelligenz die Zeit, der Ort und die anderen Slaves registriert werden und direkt mit Bewegungssensoren über das Bluetooth Scatternet und GSM auf eine Mobiltelefon-Plattform oder dem Handy vom Besitzer ein Alarm übermittelt wird und Ortungen oder Notrufalarme mit Ortungsanzeige durch GSM-Mastentracking von der GSM-Modul Software aus laufen.

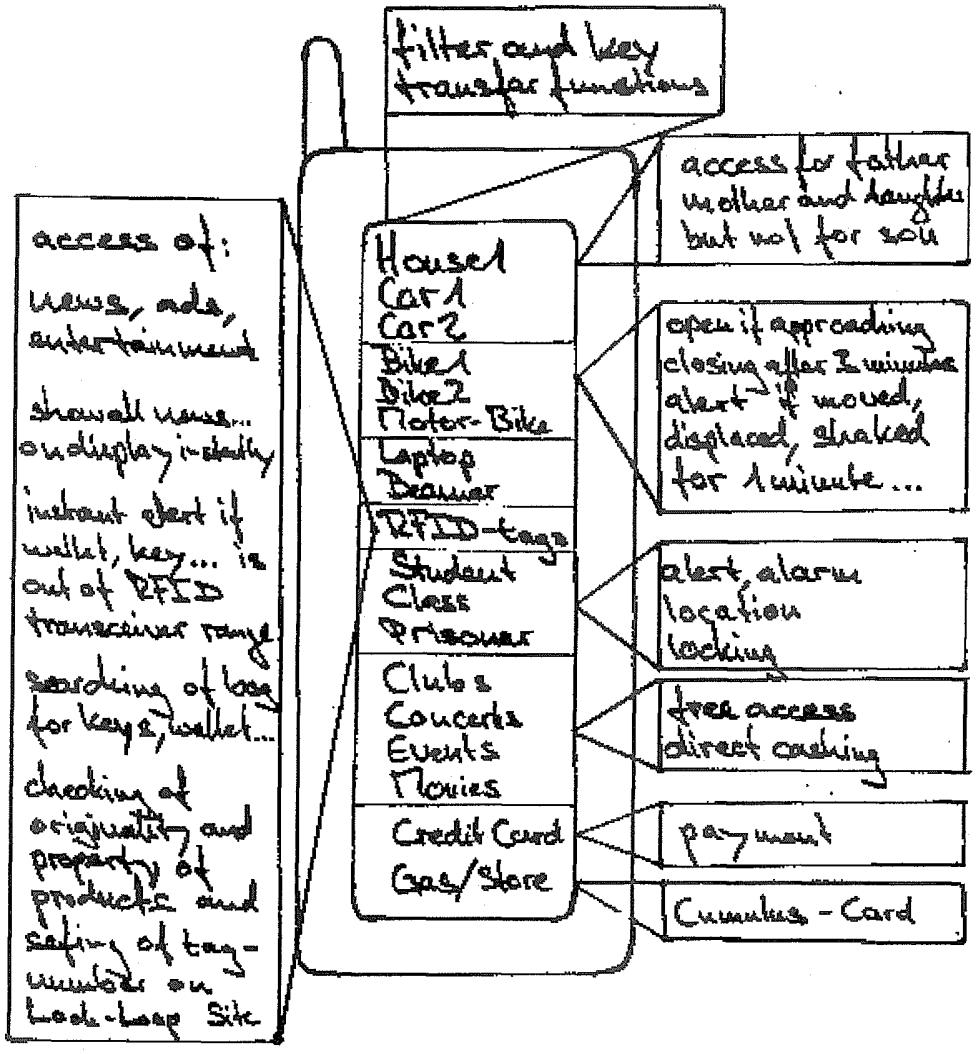
[0021] C) Access-Control Applikationen mit gegenseitiger direkter zeitgleicher Photo- und Personalien Darstellung für Personen-Kontrollen, Eintritte oder Transaktionen für Geld, Postpaketübergaben, wo mit biometrischen Fingerprint-Sensoren über NFC, Bluetooth etc. die Autorisation und Abbuchung abgewickelt wird oder wo bei Fahrzeugen (Zentraler Motoreinheit oder Hard- und Software bzw. für die Kontrolle von Motoren- oder sonstigen Betriebs-Einstellungen etc.), Geräten (Laptops, Fernseher, Waschmaschinen etc.) oder Installationen (Strom-, Telefon-, Funk-Netze, Betriebs-Zentralen, Terminals) nach einer Autorisation die geschützten Betriebsdaten ausgelesen werden oder gar neu konfiguriert werden und wo dabei vom Gerät mit FP-Sensor über Bluetooth ein Sicherheitscode CO zu einer versteckten Zündung mit Bestätigung des Sicherheitscode CO läuft und dann bei Autorisation CO über NFC ein zweiter Sicherheitscode C1 zur zentralen Motoreinheit mit einem FP-Sensor im Gerät ausgelöst wird, sodass dann bei Autorisation C01 ein weiterer Zündcode C2 vom Gerät mit FP-Sensor zur Zündung, zentralen Motoreinheit und z.B. dem Motor zum Start übermittelt wird, wobei auch noch ein Lock-Loop Funk-Schloss mit GSM-Modul und z.B. Bluetooth mit einbezogen werden kann in einen Sicherheitscode C.

[0022] D) über das Gerät ein RFID-Tag mit Geld bzw. einem Kredit beladen werden, wobei die EEOPROM Cache Speicherplätze des RFID-Tags ausgelesen wie auch gesichert beschriftet werden, indem nur Automaten oder die selben Handys mit denen die Tags aufgeladen wurden (oder mit biometrischer Identifikation über einen Fingerprint-Sensor) die Tags mit den Krediten entladen werden (können) oder die RFID-Kredit-Tags immer gleich wie im Lock-Loop Patent mit einer (Bank-Konto-) Nummer gesichert über eine Website (über GSM-MP) gemanaged werden.
– über das Gerät die RFID-Tag Nummern in Produkten, Anzeigen, Logos oder Verpackungen direkt mit einer GSM-Netz Verbindung auf einer Web-Site registriert und gemanaged werden, wobei die persönliche Registrierung der RFID-Tags auf einer Web-Site mit über Geräte mit Fingerprint-Sensor bestätigt werden
– Abklärungen über Besitztum, Eigentum, Eigenschaft des Produktes mit dem RFID-Tag gemacht werden über eine GSM-Netz Verbindung auf eine registrierte Web-Site.

Patentansprüche

1. Mobiles Gerät mit einem optionalen Zusatzgerät für Transaktions-Applikationen dadurch gekennzeichnet, dass mit NFC-Sender Zahlungs-, Zulassungs-, RFID-Tag- oder Funkschloss- Identifikationen und Applikationen führbar, transferierbar und sendbar sind, die vom Gerät mit direkter sofortiger oder dem damit kommunizierenden Transferierungs-Terminal mit indirekter späterer GSM- und Internet-Übertragung auf ein Konto, d.h. einen Server abbuchbar sind.
2. Verfahren für Transaktions-Applikationen dadurch gekennzeichnet, dass mit einem mobilen Gerät mit einem optionalen Zusatzgerät mit NFC-Sender Zahlungs-, Zulassungs-, RFID-Tag- oder Funkschloss- Identifikationen und Applikationen geführt, transferiert und gesendet werden, die vom Gerät mit direkter sofortiger oder dem damit kommunizierenden Transferierungs-Terminal mit indirekter späterer GSM- und Internet-Übertragung auf ein Konto, d.h. einen Server abgebucht werden.
3. Mobiles Gerät mit einem optionalen Zusatzgerät für Transaktions-Applikationen nach dem Anspruch 1, dadurch gekennzeichnet, dass eine biometrische Identifikation, Autorisation und Sicherung integriert ist, womit die Transaktions-Applikations Übermittlung so daraus verbunden verschlüsselbar ist.
4. Verfahren für Transaktions-Applikationen nach dem Anspruch 2, dadurch gekennzeichnet, dass eine biometrische Identifikation, Autorisation und Sicherung integriert ist, womit die Transaktions-Applikations Übermittlung so daraus verbunden verschlüsselt wird.

Fig. 1



All-In-One-Key (mobile phone)

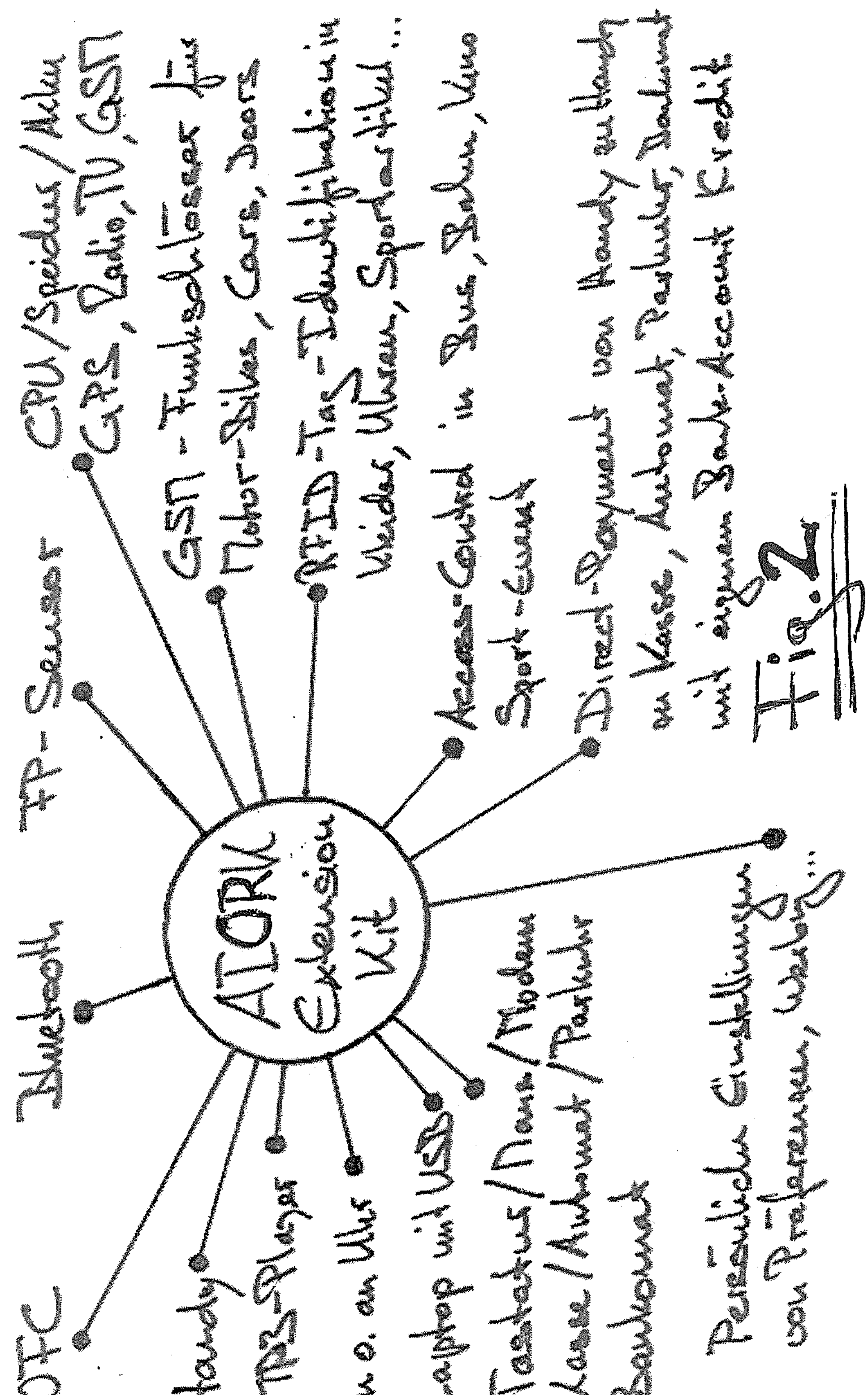

ATOM Extension Kit
NFC
Bluetooth
FP-Sensor
CPU/Speicher/Akku
GPS, Radio, TV, GSM
GSM-Funkschlüssel für Motor-Bikes, Cars, Doors
RFID-Tag-Identifikation in Kleider, Uhren, Sportartikel ...
Access-Control in Bus, Bahn, Kino
Sport-Event
Direct-Payment von Handy zu Handy an Kasse, Automat, Parkuhr, Bankomat
mit eigenem Bank-Account Kredit
Handy
MP3-Player
in o. an Uhr
Laptop mit USB
Tastatur/Maus/Modem
Kasse/Automat/Parkuhr
Bankomat
Persönliche Einstellungen von Präferenzen, Werbung...

Fig. 2