(19) SCHWEIZERISCHE EIDGENOSSENSCHAFT
EIDGENÖSSISCHES INSTITUT FÜR GEISTIGES EIGENTUM

(11) CH 714 569 A2

(51) Int. Cl.: H04B 5/00 (2006.01)

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

(12) PATENTANMELDUNG

(21) Anmeldenummer: 00050/18

(22) Anmeldedatum: 17.01.2018

(43) Anmeldung veröffentlicht: 31.07.2019

(71) Anmelder:
PBV Kaufmann Systeme GmbH, Kreuzmatte 1c
6260 Reiden (CH)

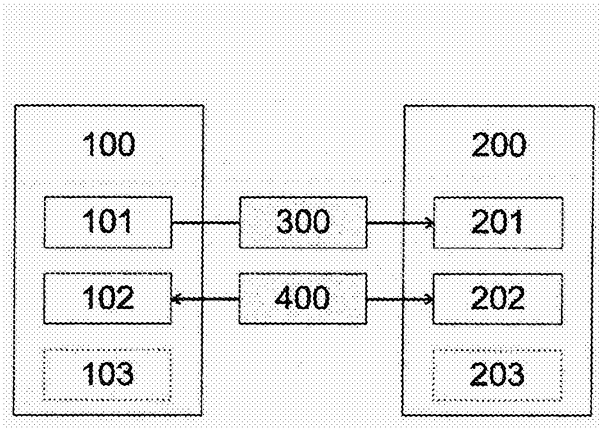
(72) Erfinder:
Stephan Wullschleger, 4600 Olten (CH)

(74) Vertreter:
Patentanwalt Koelliker GmbH Dr. Robert Koelliker,
Seehäusernstr. 15
6208 Oberkirch (CH)

(54) Sichere bidirektionale Nahfeld-Datenübertragung zwischen einem Terminal und einem mobilen Gerät ohne bidirektionale Nahfeld-Schnittstelle.

(57) Beansprucht werden ein System und ein Verfahren zur Näherungserkennung eines mobilen Geräts (200) durch ein Datenempfangsterminal (100) über NFC, zum Aufbau einer sicheren Verbindung zwischen dem Datenempfangsterminal (100) und dem mobilen Gerät (200) und zur sicheren bidirektionalen Übermittlung von Nutzdaten zwischen dem Datenempfangsterminal (100) und dem mobilen Gerät (200), selbst dann, wenn die NFC-Schnittstelle des mobilen Geräts (200) nur Nutzdaten empfangen, aber nicht versenden kann.

Das Verfahren ist dadurch gekennzeichnet, dass eine Sitzung vorzugsweise die folgenden Schritte durchläuft: a) Näherungserkennung eines Datenempfangsterminals (100) durch ein mobiles Gerät (200) mittels eines NFC-Lesers (201), b) Übermittlung der Paarungsinformationen über den NFC-Kanal (300) für den Verbindungsaufbau eines alternativen Übertragungskanals, wie beispielsweise eines BLE-Kanals (400) vom Datenempfangsterminal (100) zum mobilen Gerät (200), c) Verbindungsaufbau des mobilen Geräts (200) mit dem Datenempfangsterminal (100) über den alternativen Übertragungskanal gemäss den Paarungsinformationen, d) Nutzdatenübertragung zwischen dem mobilen Gerät (200) und dem Datenempfangsterminal (100) über den alternativen Übertragungskanal und oder den NFC-Kanal (300), und e) Trennung des alternativen Übertragungskanals, wenn das mobile Gerät (200) und das Datenempfangsterminal (100) nicht mehr in Näherungsreichweite des NFC-Kanals (300) sind, oder wenn der alternative Übertragungskanal nicht mehr gebraucht wird.



Beschreibung

[0001] Die vorliegende Erfindung bezieht sich auf ein System und ein Verfahren zum schnellen und zuverlässigen Aufbau einer drahtlosen bidirektionalen Datenverbindung zwischen zwei Geräten infolge einer Näherungserkennung zwischen den zwei Geräten, auch wenn der Sensor zur Näherungserkennung selbst nicht als Schnittstelle für die bidirektionale Datenverbindung verwendet werden kann.

[0002] Viele Geräte, insbesondere mobile Geräte wie Smartphones und Tablets, unterstützen heute eine Vielzahl verschiedener Schnittstellen zur drahtlosen bidirektionalen Datenübertragung. Die Liste der in modernen Geräten möglichen unterstützten drahtlosen Datenübertragungsschnittstellen ist lang, und sollen hier deshalb nicht einzeln genannt werden. Zu den beliebtesten und verbreitetesten drahtlosen Datenübertragungsschnittstellen gehören Mobilfunk, Wi-Fi, Bluetooth und NFC.

[0003] Naturgemäss hat jede drahtlose Datenübertragungsschnittstelle ihre physikalischen und ergonomischen Eigenschaften mit differenzierten Vor- und Nachteilen bezüglich ihren Einsatzbereichen und Anwendungen. Entsprechend werden diese Schnittstellen bestmöglich nach ihren Eigenschaften den Zielanwendungen ausgewählt und implementiert. Einige wichtige Vergleichseigenschaften von drahtlosen Datenübertragungsschnittstellen sind u.a. Übertragungsrate, Kanalrichtung, Reaktionszeit und Echtzeittauglichkeit, Aufwand und Dauer für den Verbindungsaufbau sowie die Reichweite. Die Reichweite sowie der Aufwand und die Dauer für den Verbindungsaufbau sind im Zusammenhang mit der Erfindung von besonderem Interesse.

[0004] Die Reichweite einer drahtlosen Daten-übertragungsschnittstelle beschreibt den grössten noch zuverlässig zur Datenübertragung funktionierenden Abstand zwischen Übertragungseinheit und Empfangseinheit. Die Reichweite kann von einigen Millimetern bis einige Kilometer erlangen, wobei viele drahtlose Datenübertragungsschnittstellen nach möglichst hoher Reichweite tendieren. Eine Ausnahme ist die NFC-Schnittstelle (Near Field Communication) mit maximal 10 Zentimetern Reichweite. Diese gewollt kurze Reichweite hat den überaus nützlichen Vorteil, dass die Datenübertragungsschnittstellen damit ohne einen zusätzlichen Näherungssensor zur Näherungserkennung verwendet werden kann. In einer entsprechenden Mensch-Maschine-Anwendung kann diese Eigenschaft direkt als Absichtserkennung und diese zu einer bestimmten Reaktion der Maschine heran gezogen werden. Diese Eigenschaft ist besonders für den erfindungsgemässen Anwendungszweck von grossem Vorteil.

[0005] Die Dauer für den Verbindungsaufbau einer drahtlosen Datenübertragungsschnittstelle beschreibt den zeitlichen Aufwand von der Absicht innerhalb der Reichweite bis zum Zeitpunkt der Bereitschaft zur Übertragung der ersten Nutzdaten. Dieser Verbindungsaufbau kann sehr einfach und unmittelbar sein, wenn das Protokoll auf beiden Seiten vorkonfiguriert ist oder keine besonderen Sicherungs- oder Sicherheitsanforderungen bestehen. Der Aufbau kann aber auch aufwändig und kompliziert sein, insbesondere wenn ein Benutzereingriff notwendig ist, beispielsweise zur Zielauswahl oder zur Passworteingabe. Das Optimum dieser Eigenschaft ist direkt vom Anwendungszweck abhängig. Der erfindungsgemässe Anwendungszweck erfordert eine drahtlose Datenübertragungsschnittstelle mit möglichst kurzer Dauer für den Verbindungsaufbau ohne Benutzereingriff, mit einer bidirektionalen Datenübermittlung und der Option für eine gegenseitige Authentifizierung und einen sicheren Datenkanal. Diese Anforderungen werden unter Anderem, aber in besonderem Mass, von der NFC- und der BLE-Schnittstelle erfüllt.

[0006] In der Praxis kann nicht für jeden Anwendungszweck immer die am besten geeignete drahtlose Datenübertragungsschnittstelle implementiert werden. Viel mehr werden Geräte mit jenen Schnittstellen ausgestatten, die für die Erfüllung aller Anwendungszwecke den besten Kompromiss zwischen Komplexität, Kosten, Performance und nicht zuletzt Politik aufweisen. Dies stellt in der Regel kein Problem dar, da die Schnittstellen ausreichend gut gewählt werden, sodass sich die Geräte auf dem Markt auch durchsetzen können.

[0007] Der Erfindungsgemässe Anwendungszweck könnte beispielsweise, aber nicht ausschliesslich, eine Ticketing-, eine Payment- und/oder eine Access-Control-Lösung für mobile Geräte sein. Dieser Anwendungszweck erfordert eine bidirektionale drahtlose Datenübertragungsschnittstelle mit einer Näherungserkennung, vorzugsweise unter zehn Zentimeter Reichweite, sowie der Fähigkeit auf dem Datenkanal schnellst möglich eine Information kryptographisch sicher vom mobilen Gerät zum Datenempfangsterminal oder in umgekehrter Richtung zu übermitteln. Die unter den am meisten verbreiteten drahtlosen Datenübertragungsschnittstellen für obigen Anwendungszweck am besten geeignete Schnittstelle ist NFC, denn diese vereint alle Anforderungen in einer Schnittstelle.

[0008] Leider hat sich die NFC-Schnittstelle wirtschaftlich zu einer derart wichtigen Schnittstelle entwickelt, dass einige Hersteller deren vollumfängliche Nutzung nur für interne Anwendungen zulassen und für Fremdanwendungen einschränken oder gar sperren. Der Gerätehersteller Apple zum Beispiel erlaubt die volle Nutzung von NFC nur für ihre hauseigene Zahlungs-App «ApplePay». Für Apps von anderen Herstellern ist NFC verwehrt, resp. auf einen unidirektionalen NDEF-Tag-Leser limitiert. Aus diesem Grund kann der erfindungsgemässe Anwendungszweck auf beispielsweise einem mobilen Gerät der Firma Apple von einer andern Firma als Apple nicht umgesetzt werden.

[0009] Überraschenderweise konnte mit dem erfindungsgemässen Verfahren eine Lösung gefunden werden, wie der erfindungsgemässe Anwendungszweck gelöst werden kann, auch wenn nur eine unidirektionale NFC-Schnittstelle wie bei einem mobilen Gerät der Firma Apple zur Verfügung steht.

Das System und das Verfahren

[0010] Das erfindungsgemässe System und Verfahren ist ein Verfahren zur Näherungserkennung eines mobilen Geräts (200), welches nur mit einer eingeschränkten unidirektionalen NFC-Leser-Schnittstelle (201) ausgerüstet ist, durch ein Datenempfangsterminal (100), zum Aufbau einer kryptographisch sicheren Verbindung zwischen Datenempfangsterminal (100) und mobilem Gerät (200) und zur kryptographisch sicheren Übermittlung von Daten wie beispielsweise einer Identifikationsnummer vom mobilen Gerät (200) zum Datenempfangsterminal (100).

[0011] Die für das erfindungsgemässe System und Verfahren gestellten technischen Mindestvoraussetzungen an das mobile Gerät (200) sind

- eine NFC-Schnittstelle, welche mindestens in der Lage ist, einen beliebigen NFC- oder RFID-Tag (PICC – Proximity Integrated Circuit Card, oder VICC – Vicinity Integrated Circuit Card) nach einem beliebigen Protokoll auszulesen (fortan NFC-Leser (201) genannt),
- eine BLE-Schnittstelle, welche mindestens in der Lage ist, eins oder mehrere Datenpakete vom mobilen Gerät (200) an ein Datenempfangsterminal (100) zu versenden (fortan BLE-Transmitter (202) genannt) und
- für den Fall, dass eine hohe kryptographische Sicherheit gefordert ist ein Sicherheitselement (SE, TEE, TPM, OMTP, etc.) in der erforderlichen Form zur sicheren Aufbewahrung von Schlüsseln oder vertraulichen Daten (fortan Geräte-SE (203) genannt).

[0012] Die für das erfindungsgemässe System und Verfahren gestellten technischen Mindestvoraussetzungen an das Datenempfangsterminal (100) sind

- eine NFC-Schnittstelle, welche mindestens in der Lage ist, sich als PICC oder VICC gegenüber dem mobilen Gerät (200) auszugeben (fortan NFC-Transponder (101) genannt), wobei die an das mobile Gerät (200) zu übertragenden Nutzdaten im NFC-Transponder (101) durch das Datenempfangsterminal (100) veränderbar sind,
- eine BLE-Schnittstelle, welche mindestens in der Lage ist, eins oder mehrere Datenpakete von einem mobilen Gerät (200) am Datenempfangsterminal (100) zu empfangen (fortan BLE-Empfänger (102) genannt) und
- für den Fall, dass eine hohe kryptographische Sicherheit gefordert ist ein Sicherheitselement (SE, TEE, TPM, OMTP, etc.) in der erforderlichen Form zur sicheren Aufbewahrung von Schlüsseln oder vertraulichen Daten (fortan Terminal-SE (103) genannt).

[0013] Beim NFC-Leser (201) im mobilen Gerät (200) handelt es sich wie oben erwähnt um eine Schnittstelle, welche nur zum Auslesen von NFC-Transpondern verwendet werden kann. Schreiben in die NFC-Transponder ist nicht möglich. Der NFC-Leser (201) kann somit nur in eine Richtung, nämlich zum Verschieben von Daten vom NFC-Transponder zum mobilen Gerät (200), verwendet werden. Die Anforderung der bidirektionalen Datenübertragung ist somit nicht erfüllt. Erfüllt sind jedoch die Anforderungen:

- Näherungserkennung,
- der geringe protokollarische Aufwand,
- die kurze Dauer für den Verbindungsaufbau und
- die ausreichend hohe Übertragungsrate.

[0014] Die auf den ersten Blick unbrauchbare Schnittstelle muss nun mit einem zusätzlichen Kanal zur Datenübertragung vom mobilen Gerät (200) zum Datenempfangsterminal (100) ergänzt werden. Im erfindungsgemässen Verfahren wird exemplarisch BLE (Bluetooth Low Energy) als Kanal verwendet. Dies stellt keine Einschränkung dar. Der Kanal könnte über eine beliebige andere drahtlose Datenübertragungsschnittstelle gelöst werden, welche die für den Anwendungszweck erforderlichen Eigenschaften aufweist. Die exemplarische, aber nicht einschränkende Wahl auf BLE erfolgt aus folgenden Gründen. BLE hat:

- eine sehr weite Verbreitung und ist auf fast allen modernen mobilen Geräten, insbesondere den mobilen Geräten der Firma Apple, implementiert,
- einen relativ geringen protokollarischen Aufwand,
- eine kurze Dauer für den Verbindungsaufbau,
- eine ausreichend hohe Übertragungsrate und
- eine sehr hohe Zuverlässigkeit.

[0015] Leider kennt BLE keine Näherungserkennung und sollte deshalb keine spontane Verbindung mit dem nächsten innerhalb der Reichweite liegenden Datenempfangsterminal (100) aufbauen. Der Benutzer des mobilen Geräts (200) hätte nie die Gewissheit, dass das vermeintlich vor ihm befindliche Datenempfangsterminal (100) auch wirklich das Datenempfangsterminal (100) ist, mit dem er eine Verbindung aufgebaut hat. Das mobile Gerät (200) muss die Adresse, die Identifikation, den Namen oder eine beliebige andere eindeutige Paarungsinformation des Datenempfangsterminals (100) im Voraus kennen, um sicher zu stellen, dass sich nicht ein falsches Datenempfangsterminal (100´) «vordrängt».

[0016] In der Kombination erfüllen BLE und die unidirektionale NFC-Schnittstelle zusammen alle erforderlichen Eigenschaften, denn für die Paarung des mobilen Geräts (200) mit dem Datenempfangsterminal (100) kann der NFC-Transponder die nötigen Paarungsinformationen als einzige oder ergänzende Daten mit übermitteln. Dadurch kann das mobile Gerät (200) spontan und auf Anhieb eine Funkverbindung zum korrekten Datenempfangsterminal (100) einleiten.

[0017] Nach erfolgtem Verbindungsaufbau über den BLE-Kanal (400) sind alle Voraussetzungen erfüllt um die Eigenschaften einer bidirektionalen NFC-Verbindung zu imitieren. Für die Datenübermittlung vom Datenempfangsterminal (100) zum mobilen Gerät (200) stehen fortan zwei Kanäle zur Auswahl, der NFC-Kanal (300) und der BLE-Kanal (400). In umgekehrter Richtung erfolgt alle Datenübermittlung über den BLE-Kanal (400). Das Datenempfangsterminal (100) und das mobile Gerät (200) befinden sich in einer gemeinsamen Sitzung.

[0018] Abhängig vom Anwendungszweck wird eine Sitzung nach erfolgter Übermittlung der erwarteten Nutzdaten vom Datenempfangsterminal (100) und/oder vom mobilen Gerät (200) wieder geschlossen, die Verbindungen getrennt und die Schnittstellen für eine neue Paarung freigegeben oder die Sitzung bleibt so lange offen, bis das Datenempfangsterminal (100) und das mobile Gerät (200) nicht mehr innerhalb der Reichweite des NFC-Kanals ist. Für den zweiten Fall nutzt das Datenempfangsterminal (100) den NFC-Transponder (101) und das mobile Gerät (200) den NFC-Leser (201) in regelmässigen Abständen für eine Näherungserkennung, um zu überprüfen, ob sich das mobile Gerät (200), resp. das Datenempfangsterminal (100) noch in Reichweite befindet. Stellt einer der Teilnehmer fest, dass die Näherungserkennung nicht mehr erfüllt ist, dann schliesst er die Sitzung umgehend, trennt alle Verbindungen und gibt die Schnittstellen für eine neue Paarung wieder frei.

[0019] Eine mögliche Methode zur gegenseitigen Authentifizierung der Teilnehmer und somit zur Erhöhung der Sicherheit der Verbindung ist der einseitige oder beidseitige Austausch einer kryptographischen Aufgabe (Challenge), welche nur von autorisierten Teilnehmern korrekt gelöst werden kann. Abhängig vom Anwendungszweck sind unterschiedliche Methoden zu bevorzugen.

[0020] Im Folgenden werden nicht limitierende, bevorzugte Ausführungsformen des erfindungsgemässen Verfahrens zum schnellen und zuverlässigen Aufbau einer drahtlosen bidirektionalen Datenverbindung zwischen zwei Geräten infolge einer Näherungserkennung zwischen den zwei Geräten, auch wenn der Sensor zur Näherungserkennung selbst nicht als Schnittstelle für die bidirektionale Datenverbindung verwendet werden kann, anhand der nachfolgenden Zeichnungen beschrieben. Diese sind nicht einschränkend auszulegen und werden als Bestandteil der Beschreibung verstanden:

Fig. 1 zeigt beispielhaft ein Datenempfangsterminal (100) mit einem NFC-Transponder (101), einem BLE-Empfänger (102) und einem optionalen Sicherheitselement SE (103), ein mobiles Gerät (200) mit einem NFC-Leser (201), einem BLE-Transmitter (202) und einem optionalen Sicherheitselement SE (203). Im NFC-Transponder (101) des Datenempfangsterminals (100) stehen mindestens die BLE-Paarungsinformation des BLE-Empfängers (102) sowie gegebenenfalls eine Challenge und gegebenenfalls weitere Daten für das mobile Gerät (200) zum Auslesen bereit. Die Challenge kann gegebenenfalls in gewissen zeitlichen Abständen verändert werden. Erscheint ein mobiles Gerät (200) in der Näherungsreichweite des Datenempfangsterminals (100), verbindet sich das mobile Gerät (200) mit dem NFC-Leser (201) über den NFC-Kanal (300) umgehend mit dem NFC-Transponder (101) und liest die BLE-Paarungsinformation des BLE-Empfängers (102) sowie gegebenenfalls die Challenge und gegebenenfalls weitere Daten aus. Anhand der Paarungsinformation verbindet sich der BLE-Transmitter (202) des mobilen Geräts (200) über den BLE-Kanal (400) mit dem BLE-Empfänger (102) und übermittelt die ID und/oder die Antwort-Challenge und/oder andere Daten vom mobilen Gerät (200) an das Datenempfangsterminal (100). Anhand der Challenge kann gegebenenfalls die Validität des BLE-Kanals (400) geprüft werden, um sicherzustellen, dass wirklich das mobile Gerät (200) und nicht ein anderes mobiles Gerät (200´) mit dem Datenempfangsterminal (100) verbunden ist. Die optionalen Sicherheitselemente SE (103, 203) können zur Erhöhung der Sicherheit und gegebenenfalls zur Lösung der Challenge dienen.

Fig. 2 zeigt beispielhaft die Übermittlung der Identifikationsnummer ID des mobilen Geräts (200) zum Datenempfangsterminal (100), wobei das Datenempfangsterminal (100) die Authentizität des mobilen Geräts (200) und die Integrität der ID anhand einer Challenge validieren kann, und nach erfolgter Übermittlung den BLE-Kanal (400) wieder trennt.

(500) Das Datenempfangsterminal (100) wird in einer sicheren Umgebung mit einem geheimen Hauptschlüssel K, der für den BLE-Kanal (400) notwendigen Paarungsinformationen PID und ggf. einem Intervall T initialisiert. Das mobile Gerät (200) wird in einer sicheren Umgebung mit einer ID und einem geheimen, mit der ID diversifizierten Schlüssel KDID initialisiert. Der geheime diversifizierte Schlüssel KDID auf dem mobilen Gerät (200) und der geheime Hauptschlüssel K auf dem Datenempfangsterminal (100) sollten vor unbefugtem Zugriff, beispielsweise im Geräte-SE (203), resp. im Terminal-SE (103) geschützt, aufbewahrt werden.
Datenempfangsterminal (100): PID, K, T
Mobiles Gerät (200): ID, KDID

(501) Das Datenempfangsterminal (100) stellt im NFC-Transponder (101) ein Datenpaket S1 mit einer neuen Zufallszahl RND und der Paarungsinformation PID bereit. S1 = PID | RND

(502) Kann für eine Intervall-Zeit T kein mobiles Gerät (200) über den BLE-Kanal (400) eine Verbindung aufbauen, dann springt die Methode zu Schritt 501. Erscheint ein mobiles Gerät (200) in Näherungsreichweite liest dessen NFC-Leser (201) S1 aus dem NFC-Transponder (101) aus.

(503) Das mobile Gerät (200) verschlüsselt RND mit dem Schlüssel KDID zu ERND. ERND = E(KDID, RND)

(504) Das mobile Gerät (200) versucht über den BLE-Kanal (400) eine Verbindung mit dem BLE-Empfänger (102) anhand der Paarungsinformationen PID herzustellen. Kann keine Verbindung hergestellt werden springt die Methode zu Schritt 502.

(505) Nach erfolgreichem Verbindungsaufbau wird das Datenpaket S2, bestehend aus der ID und der verschlüsselten Zufallszahl ERND, über den BLE-Kanal (400) an das Datenempfangsterminal (100) übermittelt. S2 = ID I ERND

(506) Das Datenempfangsterminal (100) und/oder das mobile Gerät (200) trennen den BLE-Kanal (400) nach erfolgter Übermittlung umgehend.

(507) Das Datenempfangsterminal (100) interpretiert S2 und generiert aus der ID und dem Hauptschlüssel K den diversifizierten Schlüssel KDID, mit welchem es die verschlüsselte Zufallszahl ERND entschlüsselt und mit RND vergleicht. Sind RND gleich dem Dechiffrat von ERND, dann ist die ID integer und das mobile Gerät (200) authentisch.
KDID = DIVERSIFY(K, ID)
OK wenn: RND == D(KDID, ERND)

(508) Ist die ID integer und das mobile Gerät (200) authentisch wird die ID gegebenenfalls vom Datenempfangsterminal (100) an einen Host zur Verarbeitung weiter gereicht. Die Methode springt weiter zu Schritt 501.

Fig. 3 zeigt beispielhaft den Verbindungsaufbau des mobilen Geräts (200) zum Datenempfangsterminal (100) für eine stehende Verbindung über den BLE-Kanal (400), wobei das Datenempfangsterminal (100) die Authentizität des mobilen Geräts (200) anhand einer Challenge validiert und den BLE-Kanal (400) infolge einer fehlgeschlagenen Validierung oder eines Ausfalls der Näherungserkennung durch das Datenempfangsterminal (100) oder durch das mobile Gerät (200) trennt.

(600) Das Datenempfangsterminal (100) wird in einer sicheren Umgebung mit einem geheimen Hauptschlüssel K, der für den BLE-Kanal (400) notwendigen Paarungsinformationen PID und einem Intervall T initialisiert. Das mobile Gerät (200) wird in einer sicheren Umgebung mit einer ID und einem geheimen, mit der ID diversifizierten Schlüssel KDID initialisiert. Der geheime diversifizierte Schlüssel KDID auf dem mobilen Gerät (200) und der geheime Hauptschlüssel K auf dem Datenempfangsterminal (100) sollten vor unbefugtem Zugriff, beispielsweise in einem Geräte-SE, resp. Terminal-SE geschützt, aufbewahrt werden.
Datenempfangsterminal (100): PID, K, T
Mobiles Gerät (200): ID, KDID

(601) Das Datenempfangsterminal (100) stellt im NFC-Transponder ein Datenpaket S1 mit einer neuen Zufallszahl RND und der Paarungsinformation PID bereit. S1 = PID I RND

(602) Ist für die Dauer eines Intervalls T kein mobiles Gerät (200) in Näherungsreichweite und/oder ist über den BLE-Kanal (400) keine Verbindung aufgebaut, dann werden alle offenen Verbindungen getrennt und die Methode springt zu Schritt 601. Befindet sich ein mobiles Gerät (200) in Näherungsreichweite liest dessen NFC-Leser (201) S1 aus dem NFC-Transponder (102) aus.

(603) Das mobile Gerät (200) generiert eine eigene Zufallszahl RND2 und verschlüsselt RND zusammen mit RND2 mit dem Schlüssel KDID zu ERND. RND2 kann als Basis für einen Sitzungsschlüssel für eine Kanalverschlüsselung auf dem BLE-Kanal (400) verwendet werden. ERND = E(KDID, RND I RND2)

(604) Das mobile Gerät (200) versucht über den BLE-Kanal (400) eine Verbindung mit dem BLE-Empfänger (102) anhand der Paarungsinformationen PID herzustellen, falls diese Verbindung nicht bereits besteht. Kann keine Verbindung hergestellt werden springt die Methode zu Schritt 602.

(605) Nach erfolgreichem Verbindungsaufbau wird das Datenpaket S2, bestehend aus der ID und den verschlüsselten Zufallszahlen ERND, über den BLE-Kanal (400) an das Datenempfangsterminal (100) übermittelt. S2 = IDI ERND

(606) Das Datenempfangsterminal (100) interpretiert S2 und generiert aus der ID und dem Hauptschlüssel K den diversifizierten Schlüssel KDID, mit welchem es die verschlüsselten Zufallszahlen ERND entschlüsselt und mit RND vergleicht. Sind RND gleich dem Dechiffrat von ERND, dann ist die ID integer und das mobile Gerät (200) authentisch. KDID = DIVERSIFY(K, ID) RNDIRND2 = D(KDID, ERND)

(607) Ist die ID nicht integer und/oder das mobile Gerät (200) nicht authentisch und/oder das mobile Gerät (200) ist ausserhalb der Näherungsreichweite zum Datenempfangsterminal (100), dann werden alle Verbindungen geschlossen und die Methode springt zu Schritt 601.

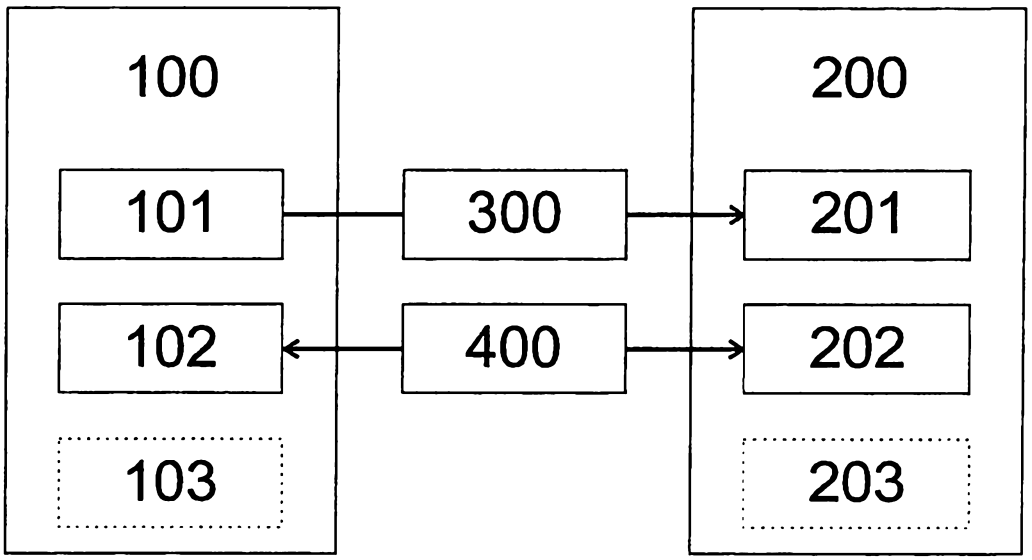
(608) Ist die ID integer und das mobile Gerät (200) authentisch und in Näherungsreichweite, dann kann der BLE-Kanal (400) fortan für den gegenseitigen Nutzdatenaustausch genutzt werden. Nach Ablauf des Intervalls T springt die Methode zu Schritt 601.

Patentansprüche

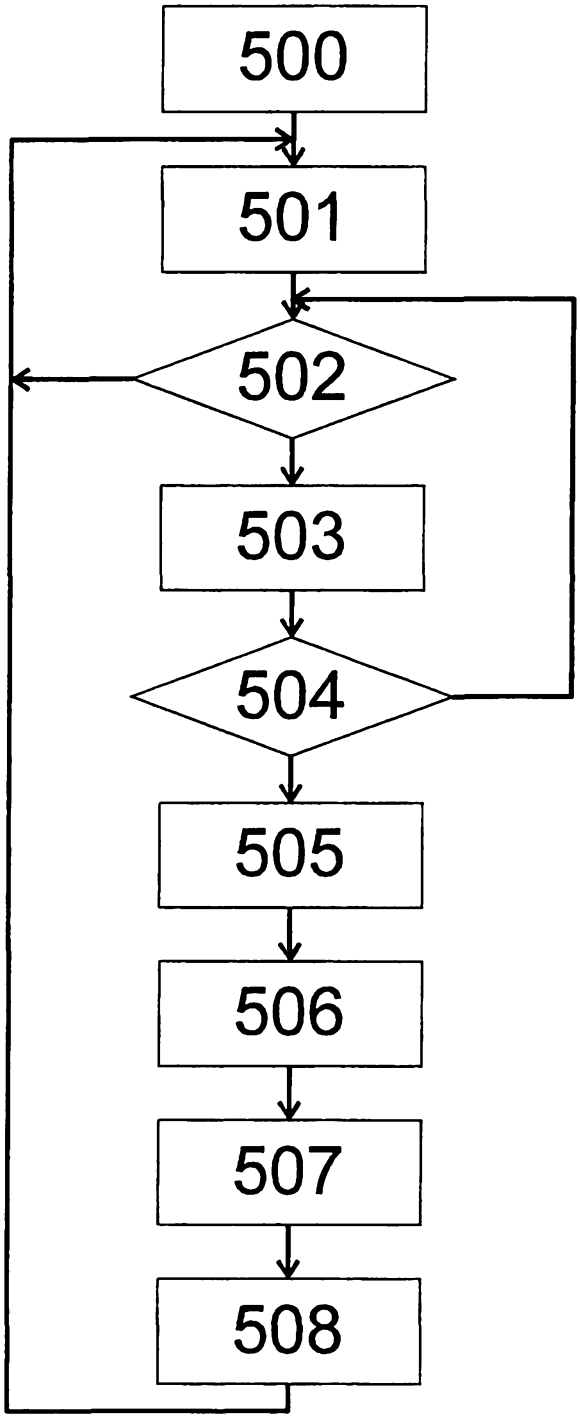
1. System und Verfahren
– zur Näherungserkennung eines mobilen Geräts (200) durch ein Datenempfangsterminal (100) über NFC,
– zum Aufbau einer sicheren Verbindung zwischen dem Datenempfangsterminal (100) und dem mobilem Gerät (200) und/oder
– zur sicheren bidirektionalen Übermittlung von Nutzdaten zwischen dem Datenempfangsterminal (100) und dem mobilen Gerät (200), auch wenn die NFC-Schnittstelle des mobilen Geräts (200) nur Nutzdaten empfängt, aber nicht versendet,
dadurch gekennzeichnet, dass das Verfahren folgende Schritte umfasst:
a) Näherungserkennung eines Datenempfangsterminals (100) durch ein mobiles Gerät (200) mittels eines NFC-Lesers (201),
b) gegebenenfalls Übermittlung der Paarungsinformationen über den NFC-Kanal (300) für den Verbindungsaufbau eines alternativen drahtlosen Übertragungskanals vom Datenempfangsterminal (100) zum mobilen Gerät (200),
c) Verbindungsaufbau des mobilen Geräts (200) mit dem Datenempfangsterminal (100) über den alternativen drahtlosen Übertragungskanal gemäss den Paarungsinformationen,
d) gegebenenfalls Nutzdatenübertragung zwischen dem mobilen Gerät (200) und dem Datenempfangsterminal (100) über den alternativen drahtlosen Übertragungskanal und oder den NFC-Kanal (300), und
e) gegebenenfalls Trennung des alternativen drahtlosen Übertragungskanals, wenn das mobile Gerät (200) und das Datenempfangsterminal (100) nicht mehr in Näherungsreichweite des NFC-Kanals (300) sind, oder wenn der alternative drahtlose Übertragungskanal nicht mehr gebraucht wird.
2. System und Verfahren nach Anspruch 1, dadurch gekennzeichnet, dass der alternative drahtlose Übertragungskanal zur Nutzdatenübertragung vom mobilen Gerät (200) zum Datenempfangsterminal (100) über den BLE-Kanal (400) erfolgt.
3. System und Verfahren nach Anspruch 1 oder 2, dadurch gekennzeichnet, dass die Nutzdatenübertragung vom Datenempfangsterminal (100) zum mobilen Gerät (200) über den NFC-Kanal (300) und/oder den alternativen drahtlosen Übertragungskanal über den BLE-Kanal (400) erfolgt.
4. System und Verfahren nach mindesten einem der Anspruch 1 bis 3, dadurch gekennzeichnet, dass die Näherungserkennung und die Übertragung der Paarungsinformation nicht über den NFC-Kanal (300), sondern über eine beliebige andere Nahfeld-Kopplung wie beispielsweise RFID, induktiv, optisch, magnetisch, akustisch oder kinetisch erfolgt.
5. System und Verfahren nach mindesten einem der Anspruch 1 bis 4, dadurch gekennzeichnet, dass die Paarungsinformation nicht direkt über die Nahfeld-Kopplung erfolgt, sondern über eine beliebige lokale oder entfernte Quelle anhand einer Referenz auf das Datenempfangsterminal (100).
6. System und Verfahren nach mindesten einem der Anspruch 1 bis 5, dadurch gekennzeichnet, dass zur Erhöhung der Sicherheit und des gegenseitigen Vertrauens zwischen dem Datenempfangsterminal (100) und dem mobilen Gerät (200) vor der ersten Nutzdatenübertragung und/oder vor der Nutzdatenverarbeitung eine oder je eine kryptographische Challenge gestellt wird, welche nur von den autorisierten Teilnehmern gelöst werden kann.
7. System und Verfahren nach Anspruch 6, dadurch gekennzeichnet, dass die Challenge auf einem symmetrischen und/oder einem asymmetrischen Krypto-Algorithmus basiert.
8. System und Verfahren nach mindesten einem der Anspruch 1 bis 7, dadurch gekennzeichnet, dass die Nutzdatenübertragung im Klartext und/oder im Klartext mit Hash und/oder im Klartext mit MAC und/oder im Chiffriertext und/oder in einer anderen beliebigen kryptographischen Nachrichtenform übermittelt wird.
9. System und Verfahren nach Anspruch 6 oder 7, dadurch gekennzeichnet, dass zur weiteren Erhöhung der Sicherheit und Vertrauenswürdigkeit die Geheimnisse für die kryptographischen Aufgaben in Sicherheitselementen SE (103) und/oder SE (203) vor Fremdzugriff geschützt hinterlegt werden.
10. System und Verfahren nach Anspruch 9, dadurch gekennzeichnet, dass zur weiteren Erhöhung der Sicherheit die kryptographischen Aufgaben direkt im Sicherheitselement SE (103) und/oder SE (203) vor Fremdeinwirkung geschützt ausgeführt werden.

11. System und Verfahren nach mindesten einem der Anspruch 1 bis 10, dadurch gekennzeichnet, dass die Trennung und Freigabe des alternativen drahtlosen Übertragungskanals, vorzugsweise des BLE-Kanals (400) zwischen dem Datenempfangsterminal (100) und dem mobilen Gerät (200) jederzeit einseitig oder beidseitig erfolgen kann.

Figur 1:



Figur 2:



Figur 3: