



(10) **DE 10 2014 209 046 A1** 2015.11.19

(12)

Offenlegungsschrift

(21) Aktenzeichen: **10 2014 209 046.6**

(22) Anmeldetag: **13.05.2014**

(43) Offenlegungstag: **19.11.2015**

(51) Int Cl.: **H04L 9/08 (2014.01)**

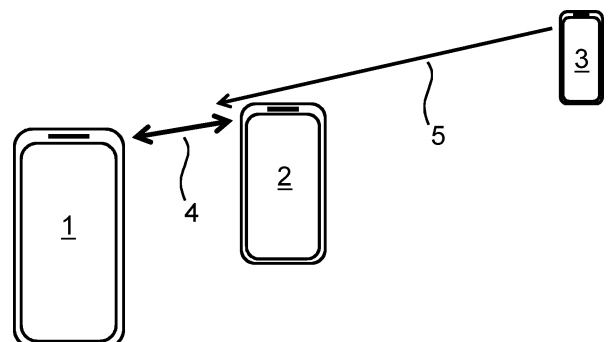
(71) Anmelder:
Robert Bosch GmbH, 70469 Stuttgart, DE

(72) Erfinder:
**Duplys, Paulius, 71706 Markgröningen, DE;
Seudie, Herve, 71297 Mönsheim, DE**

Die folgenden Angaben sind den vom Anmelder eingereichten Unterlagen entnommen

(54) Bezeichnung: **Verfahren zur Generierung eines geheimen, kryptographischen Schlüssels in einem mobilen Endgerät**

(57) Zusammenfassung: Die Erfindung geht aus von einem Verfahren zur Generierung eines geheimen, kryptographischen Schlüssels in einem mobilen Endgerät. Dabei kommuniziert das mobile Endgerät mit einem zweiten Gerät über einen kurzreichweitigen Funk-Übertragungskanal, insbesondere nach einem Bluetooth-Standard, einem Near-Field-Communication-Standard oder einem RFID-Standard. Das mobile Endgerät leitet einen geheimen, kryptographischen Schlüssel aus physikalischen Eigenschaften des kurzreichweitigen Funk-Übertragungskanals ab und baut mit dem geheimen, kryptographischen Schlüssel eine sichere Kommunikationsverbindung zu dem zweiten Gerät auf.



Beschreibung

[0001] Die vorliegende Erfindung betrifft Verfahren zur Generierung eines gemeinsamen, geheimen, kryptographischen Schlüssels in einem mobilen Endgerät und einem weiteren Gerät sowie ein hierzu eingerichtetes mobiles Endgerät und ein Computerprogramm. Sie beschäftigt sich insbesondere mit dem sicheren Austausch von Daten zwischen einem mobilen Endgerät und einer Kommunikationseinheit eines Fahrzeugs, insbesondere einer Head-Unit (Hauptbedienschnittstelle), oder zwischen zwei mobilen Endgeräten. Die Kommunikation der zwei Geräte erfolgt dabei über eine drahtlose Verbindung.

[0002] In vielen Kommunikationsszenarien ist es notwendig, die Integrität der zwischen Geräten ausgetauschten Daten sicherzustellen, z.B. wenn eine Kommunikationseinheit eines Fahrzeugs durch ein mobiles Endgerät konfiguriert werden soll. In anderen Szenarien müssen die zwischen Geräten ausgetauschten Daten aufgrund von Vertraulichkeit oder Datenschutz geheim gehalten werden, zum Beispiel wenn aufgezeichnete Ortsinformationen von der Head-Unit eines Fahrzeugs zu einem mobilen Endgerät übermittelt werden oder wenn über das mobile Endgerät ein Firmware-Update für eine Fahrzeugkomponente durchgeführt werden soll.

[0003] Neben den Sicherheitsaspekten ist allerdings auch die Nutzerfreundlichkeit von Sicherheitsmechanismen von großer Bedeutung.

Stand der Technik

[0004] Eine sichere Kommunikation zwischen verschiedenen Geräten wird in einer zunehmend vernetzten Welt immer wichtiger und stellt in vielen Anwendungsbereichen eine wesentliche Voraussetzung für die Akzeptanz und somit auch den wirtschaftlichen Erfolg der entsprechenden Anwendungen dar.

[0005] Dies umfasst – je nach Anwendung – verschiedene Schutzziele, wie beispielsweise die Wahrung der Vertraulichkeit der zu übertragenden Daten, die gegenseitige Authentifizierung der beteiligten Knoten oder die Sicherstellung der Datenintegrität.

[0006] Zur Erreichung dieser Schutzziele kommen üblicherweise geeignete kryptographische Verfahren zum Einsatz, die man generell in zwei verschiedene Kategorien unterteilen kann: Symmetrische Verfahren, bei denen Sender und Empfänger über denselben kryptographischen Schlüssel verfügen, sowie asymmetrische Verfahren, bei denen der Sender die zu übertragenden Daten mit dem öffentlichen (d.h. auch einem potenziellen Angreifer möglicherweise bekannten) Schlüssel des Empfängers verschlüsselt, die Entschlüsselung aber nur mit dem zugehörigen

privaten Schlüssel erfolgen kann, der idealerweise nur dem Empfänger bekannt ist.

[0007] Asymmetrische Verfahren haben unter anderem den Nachteil, dass Sie in der Regel eine sehr hohe Rechenkomplexität aufweisen. Damit sind sie nur bedingt für ressourcenbeschränkte Knoten, wie z.B. Sensoren, Aktuatoren, o.ä., geeignet, die üblicherweise nur über eine relativ geringe Rechenleistung sowie geringen Speicher verfügen und energieeffizient arbeiten sollen, beispielsweise aufgrund von Batteriebetrieb oder dem Einsatz von Energy Harvesting. Darüber hinaus steht oftmals nur eine begrenzte Bandbreite zur Datenübertragung zur Verfügung, was den Austausch von asymmetrischen Schlüsseln mit Längen von 2048 Bit oder noch mehr unattraktiv macht.

[0008] Bei symmetrischen Verfahren hingegen muss gewährleistet sein, dass sowohl Empfänger als auch Sender über den gleichen Schlüssel verfügen. Das zugehörige Schlüsselmanagement stellt dabei generell eine sehr anspruchsvolle Aufgabe dar. Im Bereich des Mobilfunks werden Schlüssel beispielsweise mit Hilfe von SIM-Karten in ein Mobiltelefon eingebracht und das zugehörige Netz kann dann der eindeutigen Kennung einer SIM-Karte den entsprechenden Schlüssel zuordnen. Im Fall von Wireless LANs hingegen erfolgt üblicherweise eine manuelle Eingabe der zu verwendenden Schlüssel (in der Regel durch die Eingabe eines Passwortes) bei der Einrichtung eines Netzwerkes. Ein solches Schlüsselmanagement wird allerdings schnell sehr aufwändig und impraktikabel, wenn man eine sehr große Anzahl von Knoten hat, beispielsweise in einem Sensornetzwerk oder anderen Maschine-zu-Maschine-Kommunikationssystemen. Darüber hinaus ist eine Änderung der zu verwendenden Schlüssel oftmals überhaupt nicht bzw. nur mit sehr großem Aufwand möglich.

[0009] Gängige kurzreichweitige Funkstandards setzen derzeit auf relativ schwache Sicherheitsmechanismen (z.B. die bereits erfolgreich gehackte Stromchiffrierung E0 für Bluetooth) oder gar keine Sicherheitsmechanismen (z.B. bei der Near Field Communication NFC).

[0010] Seit einiger Zeit werden unter dem Schlagwort „Physical Layer Security“ neuartige Ansätze untersucht und entwickelt, mit Hilfe derer Schlüssel für symmetrische Verfahren automatisch auf der Grundlage der Übertragungskanäle zwischen den involvierten Knoten erzeugt werden können. Die Ermittlung von Zufallszahlen oder Pseudozufallszahlen aus Kanalparametern ist z.B. der WO 1996023376 A2 zu entnehmen, die Erzeugung geheimer Schlüssel aus Kanalparametern ist in der WO 2006081122 A2 offenbart.

Offenbarung der Erfindung

[0011] Die Erfindung betrifft Verfahren gemäß den unabhängigen Verfahrensansprüchen sowie ein mobiles Endgerät und ein Computerprogramm, die dazu eingerichtet sind, eines der Verfahren durchzuführen.

[0012] Ausgegangen wird dabei von zwei Geräten, einem mobilen Endgerät und einem weiteren Gerät, die mit Kommunikationsmitteln zur drahtlosen Übertragung von Daten ausgestattet sind und über eine kurzreichweitige Funkverbindung, insbesondere nach dem Bluetooth-, NFC- oder RFID-Standard, kommunizieren. Sie einigen sich derart auf einen gemeinsamen, geheimen Schlüssel, dass dieser Schlüssel nicht oder nur sehr schwer von potentiellen Angreifern ausgespäht werden kann. Das Verfahren ermöglicht eine perfect forward secrecy (PFS; auf Deutsch etwa: perfekte vorwärts gerichtete Geheimhaltung), wenn der Schlüssel als Sitzungsschlüssel (session key) für die nachfolgende Datenverschlüsselung eingesetzt wird.

[0013] Die vorgestellten Verfahren ermöglichen einen sicheren und nutzerfreundlichen Informationsaustausch zwischen zwei mobilen Endgeräten oder zwischen einem mobilen Endgerät und einer Kommunikationseinheit eines Fahrzeugs über drahtlose Funkverbindungen. Sie können kostengünstig realisiert werden, da die Geräte hierzu lediglich über Funkschnittstellen und über übliche Verarbeitung- und Berechnungsmittel verfügen müssen.

[0014] Im Vergleich zu asymmetrischen Verfahren bringt die vorgestellte Vorgehensweise Kosteneinsparungen in der Hardware sowie einen geringeren Energieverbrauch mit sich. Im Vergleich zu herkömmlichen symmetrischen Verfahren weist es ein stark vereinfachtes Schlüsselmanagement auf. Das Verfahren ist einfach einsetzbar und bedienbar und durch seine weitgehende Automatisierung auch von Personen ohne besondere Fachkenntnisse einfach durchführbar. Die Sicherheit ist skalierbar, d.h. es können je nach Anforderung im Prinzip Schlüssel beliebiger Länge erzeugt werden.

Zeichnungen

[0015] Nachfolgend ist die Erfindung unter Bezugnahme auf die beiliegenden Zeichnungen und anhand von Ausführungsbeispielen näher beschrieben. Dabei zeigen

[0016] Fig. 1 schematisch ein mobiles Endgerät in Kommunikation mit einem weiteren mobilen Endgerät und

[0017] Fig. 2 schematisch ein mobiles Endgerät in Kommunikation mit einer Kommunikationseinheit eines Fahrzeugs.

Beschreibung der Ausführungsbeispiele

[0018] Die vorliegende Erfindung bezieht sich auf ein Verfahren zur automatischen Generierung von symmetrischen, kryptographischen Schlüsseln basierend auf physikalischen Kanälen zwischen einem mobilen Endgerät und einem weiteren Gerät mit Funkkommunikationsmitteln.

[0019] Damit können ohne hohen Aufwand symmetrische Verschlüsselungsverfahren zur Realisierung verschiedener Sicherheitsziele eingesetzt werden. Es wird hierbei die Reziprozität und die inhärente Zufälligkeit der Übertragungskanäle zwischen den Geräten ausgenutzt. Ein solches Verfahren kann beispielsweise ablaufen, wie im Folgenden beschrieben. Die zwei Geräte schätzen eine bestimmte Anzahl von Kanalparametern, evtl. auch über die Zeit. Diese Kanalparameter werden von beiden Geräten geeignet quantisiert. Vorzugsweise folgen dann Maßnahmen zur Rausch- bzw. Fehlerreduktion, z.B. durch entsprechende Fehlerdecodierung. Mit Hilfe geeigneter Mechanismen erfolgt dann ein Abgleich der quantisierten Kanalparameter zwischen den Geräten, vorzugsweise unter Verwendung eines öffentlichen Protokolls. Dies ist notwendig, da aufgrund von Messungenauigkeiten, Rauschen, Interferenzen, etc. beide Geräte im Allgemeinen zunächst keine identischen Parametersätze ermittelt haben. Der Abgleich sollte dabei derart gestaltet sein, dass ein potenzieller Angreifer, der die ausgetauschten Daten mithören kann, davon nicht ohne Weiteres auf die quantisierten Kanalparameter schließen kann. Hierzu können beispielsweise Paritätsbits zwischen den Geräten ausgetauscht werden. Optional können noch eine Schlüsselvalidierung (z.B. eine Entropieabschätzung) und eine Schlüsselverbesserung (z.B. durch Schlüsselverdichtung über Hashwert-Bildung) durchgeführt werden. Schließlich werden auf Grundlage der abgeglichenen, quantisierten Kanalparameter entsprechende symmetrische Schlüssel erzeugt.

[0020] Dabei wird angenommen, dass ein potenzieller Angreifer einen genügend großen Abstand zu den beiden Geräten hat, in denen der symmetrische Schlüssel erzeugt werden soll. Der Abstand sollte dabei mindestens in der Größenordnung der so genannten Kohärenzlänge liegen, die bei den gängigen drahtlosen Kommunikationssystemen im Bereich von wenigen Zentimetern liegt. Damit sieht der Angreifer jeweils andere (unabhängige) Übertragungskanäle zu diesen beiden Geräten und kann nicht ohne Weiteres denselben Schlüssel rekonstruieren. Zudem kann mit Hilfe dieses Ansatzes auch ohne großen Aufwand regelmäßig ein Re-Keying durchgeführt werden, d.h. eine Neuberechnung der zu verwendenden Schlüssel, und es muss nicht auf komplexe, rechenintensive asymmetrische Verfahren zurückgegriffen werden.

[0021] Als Kanalparameter kommen z.B. Phase oder Amplitude des Kanalkoeffizienten in Frage. Der Receive Signal Strength Indicator (RSSI) stellt z.B. einen gängigen Indikator für die Empfangsfeldstärke kabelloser Kommunikationsanwendungen dar und kann für diese Zwecke herangezogen werden. Zur Ermittlung der Kanalparameter können beiden Seiten bekannte Pilotsignalfolgen zwischen den Geräten übertragen werden, welche die nötigen Kanalschätzungen erleichtern.

[0022] Bei den beschriebenen Verfahren wird davon ausgegangen, dass die Übertragungskanäle zwischen den Geräten ausreichende Schwankungen ihrer Kanaleigenschaften aufweisen, um daraus geeignete Kanalparameter ableiten zu können, die sich als Grundlage für eine Schlüsselgenerierung in den Teilnehmer eignen (insbesondere ausreichende Zufallseigenschaften aufweise). Es wird aber auch angenommen, dass die Kanaleigenschaften über kurze Zeitspannen ausreichend konstant sind, dass Datenübertragungen in beide Richtungen erfolgen können, aus denen die jeweiligen Geräte trotz zeitlichen Versatzes ausreichend gleiche Kanaleigenschaften abschätzen können, um ausreichend ähnliche Kanalparameter zu erhalten, aus denen gleiche Schlüssel erhalten werden können.

[0023] In **Fig. 1** sind ein erstes mobiles Endgerät **1**, ein zweites mobiles Endgerät **2** und ein drittes mobiles Endgerät **3** gezeigt. Die Endgeräte verfügen jeweils über Mittel zur Funkübertragung von Daten. Das mobile Endgerät **1** und das mobile Endgerät **2** sind zueinander so nahe positioniert, dass über die kurze Entfernung **4** zwischen ihnen eine Kommunikation mittels eines kurzreichweitigen Drahtlosstandards wie Bluetooth, NFC oder RFID aufgebaut werden kann. Die Geräte erzeugen nun einen gemeinsamen, geheimen Schlüssel aus zeitinvarianten Eigenschaften des kurzreichweitigen Kommunikationskanals (fading channel) zwischen ihnen mit den Methoden der oben beschriebenen Physical Layer Security.

[0024] Befindet sich ein potentieller Angreifer, hier das mobile Endgerät **3**, in ausreichender Entfernung **5** von den beiden anderen Geräten (typischerweise mehrere Wellenlängen), so kann er den geheimen Schlüssel nicht ausspähen, da die für ihn beobachtbaren Werte der Eigenschaften des Kommunikationskanals sich aufgrund intrinsischer physikalischer Eigenschaften des drahtlosen Kommunikationskanals von denen unterscheiden, welche die beiden Geräte beobachten. In **Fig. 2** sind ein mobiles Endgerät **11** und ein stationäres Gerät **12**, insbesondere ein Kommunikationsmittel eines Fahrzeugs wie z.B. eine Hauptbedienschnittstelle (Head-Unit), gezeigt. Diese kommunizieren über einen kurzreichweitigen Funkkanal **14** und leiten aus diesem geheime Schlüssel zur Absicherung ihrer weiteren Kommuni-

kation ab. Ein potentieller Angreifer, hier als mobiles Endgerät **13** gezeigt, kann diesen Schlüssel nicht ausspähen, wenn er sich in ausreichender Entfernung **15** zu den beiden anderen Geräten befindet.

[0025] Die vorgestellten Verfahren zur Erzeugung eines geheimen Schlüssels in dem mobilen Endgerät **1** bzw. **11** sind vorzugsweise davon abhängig, dass die beiden beteiligten Geräte über einen kurzreichweitigen Funkkanal kommunizieren und aus diesem der Schlüssel abgeleitet wird. Dadurch kann der Nutzer des mobilen Endgerät **1** seinen Gegenüber oder die Kommunikationseinheit im Fahrzeug aufgrund der kurzen Entfernung direkt sehen. Es ist also eine nicht-technische Authentifizierung möglich, z.B. wenn die Nutzer der mobilen Endgeräte sich gegenseitig kennen oder der Nutzer des mobilen Endgeräts auch der Besitzer des Fahrzeugs ist, mit dessen Kommunikationseinheit das mobile Endgerät verbunden werden soll. Ein sich nicht unmittelbar neben dem mobilen Endgerät aufhaltender Angreifer stellt keine Gefahr dar.

[0026] Insbesondere wird die Kommunikation über eine kurzreichweitige Kommunikation zur Bedingung dafür gemacht, dass die beiden Geräte mit der jeweiligen Schlüsselgenerierung beginnen. Z.B. kann in einem ersten Schritt eines entsprechenden Verfahrens durch das mobile Endgerät oder das weitere Gerät überprüft werden, ob die Kommunikation mit dem jeweils anderen Gerät über einem (ihm vorbekannten) kurzreichweitigen Kommunikationsstandard erfolgt, und von ihm nur, falls das erfüllt ist, eine Schlüsselgenerierung initialisiert werden.

ZITATE ENTHALTEN IN DER BESCHREIBUNG

Diese Liste der vom Anmelder aufgeführten Dokumente wurde automatisiert erzeugt und ist ausschließlich zur besseren Information des Lesers aufgenommen. Die Liste ist nicht Bestandteil der deutschen Patent- bzw. Gebrauchsmusteranmeldung. Das DPMA übernimmt keinerlei Haftung für etwaige Fehler oder Auslassungen.

Zitierte Patentliteratur

- WO 1996023376 A2 [0010]
- WO 2006081122 A2 [0010]

Patentansprüche

1. Verfahren zur Generierung eines geheimen, kryptographischen Schlüssels in einem mobilen Endgerät (1, 11), **dadurch gekennzeichnet**, dass das mobile Endgerät (1, 11) mit einem zweiten Gerät (2, 12) über einen kurzreichweitigen Funk-Übertragungskanal (4, 14), insbesondere nach einem Bluetooth-Standard, einem Near-Field-Communication-Standard oder einem RFID-Standard, kommuniziert, dass das mobile Endgerät (1, 11) einen geheimen, kryptographischen Schlüssel aus physikalischen Eigenschaften des kurzreichweitigen Funk-Übertragungskanals (4, 14) ableitet und dass das mobile Endgerät (1, 11) mit dem geheimen, kryptographischen Schlüssel eine sichere Kommunikationsverbindung zu dem zweiten Gerät (2, 12) aufbaut.

2. Verfahren nach Anspruch 1, **dadurch gekennzeichnet**, dass das zweite Gerät (2, 12) den gleichen, geheimen, kryptographischen Schlüssel aus den physikalischen Eigenschaften des kurzreichweitigen Funk-Übertragungskanals (4, 14) ableitet.

3. Verfahren nach einem der vorangegangenen Ansprüche, **dadurch gekennzeichnet**, dass das zweite Gerät (2, 12) ein zweites mobiles Endgerät (2) ist.

4. Verfahren nach einem der Ansprüche 1 oder 2, **dadurch gekennzeichnet**, dass das zweite Gerät (2, 12) eine Kommunikationseinheit (12), insbesondere eine Hauptbedienschnittstelle, eines Fahrzeugs ist.

5. Mobiles Endgerät (1, 11), insbesondere Mobiltelefon oder Tablet-Computer, das dazu eingerichtet ist, mit einem zweiten Gerät (2, 12) über einen kurzreichweitigen Funk-Übertragungskanal (4, 14), insbesondere nach einem Bluetooth-Standard, einem Near-Field-Communication-Standard oder einem RFID-Standard, zu kommunizieren, aus physikalischen Eigenschaften des kurzreichweitigen Funk-Übertragungskanals (4, 14) einen geheimen, kryptographischen Schlüssel abzuleiten und mit dem geheimen, kryptographischen Schlüssel eine sichere Kommunikation zu dem zweiten (2, 12) Gerät aufzubauen.

6. Computerprogramm, welches dazu eingerichtet ist, alle Schritte eines Verfahrens nach einem der Ansprüche 1 bis 4 durchzuführen.

7. Maschinenlesbares Speichermedium mit einem darauf gespeicherten Computerprogramm nach Anspruch 6.

Es folgen 2 Seiten Zeichnungen

Anhängende Zeichnungen

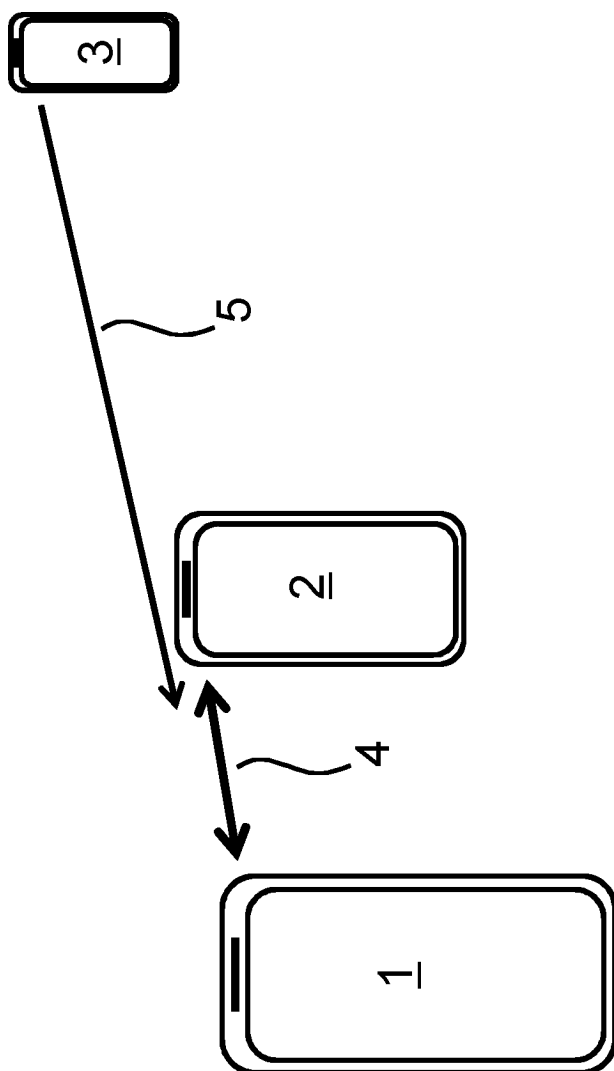


Fig. 1

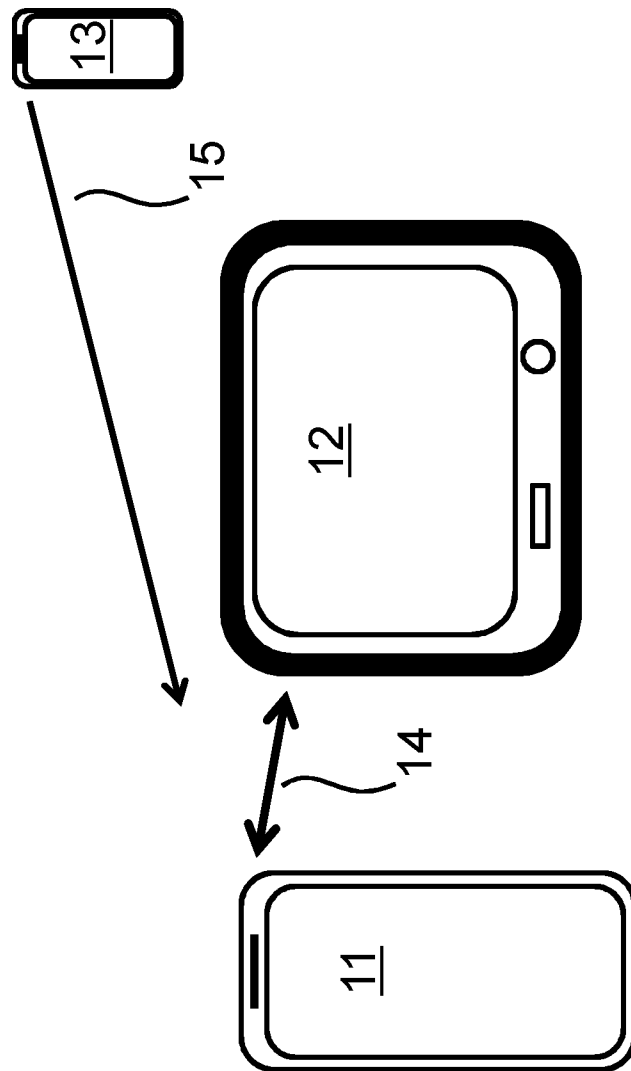


Fig. 2