(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
1. August 2013 (01.08.2013)

WIPO | PCT

(10) Internationale Veröffentlichungsnummer
WO 2013/110253 A1

(51) Internationale Patentklassifikation:
G06F 9/445 (2006.01) *H04W 12/04* (2009.01)

(21) Internationales Aktenzeichen: PCT/DE2012/100398

(22) Internationales Anmeldedatum:
21. Dezember 2012 (21.12.2012)

(25) Einreichungssprache: Deutsch

(26) Veröffentlichungssprache: Deutsch

(30) Angaben zur Priorität:
PCT/EP2011/006560
23. Dezember 2011 (23.12.2011) EP
10 2012 111 834.5
5. Dezember 2012 (05.12.2012) DE

(71) Anmelder: **APPBYYOU GMBH** [DE/DE]; Himmelberg 14, 78582 Balgheim (DE).

(72) Erfinder: **WINKLER-TEUFEL, Alexandra**; Himmelberg 14, 78582 Balgheim (DE).

(74) Anwalt: **GEITZ TRUCKENMÜLLER LUCHT**; Kriegsstraße 234, 76135 Karlsruhe (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, KM, 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, ML, MR, NE, SN, TD, TG).

Veröffentlicht:

— *mit internationalem Recherchenbericht (Artikel 21 Absatz 3)*

— *mit geänderten Ansprüchen gemäss Artikel 19 Absatz 1*

(54) **Title**: METHOD FOR SETTING UP AN ENCRYPTED CONNECTION BETWEEN TWO COMMUNICATION APPLIANCES FOLLOWING PRIOR KEY INTERCHANGE VIA A SHORTHAUL CONNECTION

(54) **Bezeichnung** : VERFAHREN ZUM AUFBAU EINER VERSCHLÜSSELTEN VERBINDUNG ZWISCHEN ZWEI KOMMUNIKATIONSGERÄTEN NACH VORHERIGEM SCHLÜSSELAUSTAUSCH ÜBER EINE KURZSTRECKENVERBINDUNG

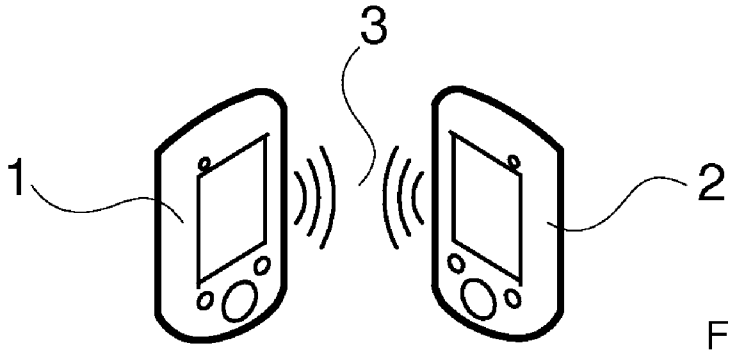

Fig. 1

(57) **Abstract**: In order to set up an encrypted communication link between two mobile appliances, it is proposed that the identification data and keys that are required therefor be interchanged in a one-off identification step and that, as part of the setup of the actual communication link, an unencrypted connection first of all be set up for reciprocal identification and then a connection encrypted with the initial interchanged keys be set up.

(57) **Zusammenfassung**: Zum Aufbau einer verschlüsselten Kommunikationsverbindung zwischen zwei Mobilgeräten wird vorgeschlagen, die hierfür erforderlichen Identifikationsdaten und Schlüssel in einem einmaligen Identifikationsschritt auszutauschen und im Zuge des Aufbaus der eigentlichen Kommunikationsverbindung zunächst eine unverschlüsselte Verbindung zur gegenseitigen Identifizierung und daraufhin eine mit den zunächst ausgetauschten Schlüsseln verschlüsselte Verbindung aufzubauen.

WO 2013/110253 A1

VERFAHREN ZUM AUFBAU EINER VERSCHLÜSSELTEN VERBINDUNG ZWISCHEN ZWEI KOMMUNIKATIONSGERÄTEN NACH VORHERIGEM SCHLÜSSELAUSTAUSCH ÜBER EINE KURZSTRECKENVERBINDUNG

Die vorliegende Erfindung betrifft ein Verfahren zum Aufbau einer verschlüsselten Kommunikationsverbindung zwischen zwei Mobilgeräten.

Grundprinzip einer jeden Verschlüsselung ist es, eine Nachricht so zu bearbeiten, dass diese im Gegensatz zu einer Klartext-Übermittlung für den Empfänger ohne geeignete Entschlüsselungsmittel unlesbar bleibt. Verschlüsselungsverfahren als solche sind hierbei bereits seit sehr langer Zeit bekannt, erste Verschlüsselungsverfahren werden bereits Julius Cäsar zugeschrieben. Dieser verschlüsselte militärische Nachrichten dadurch, dass eine Verschiebung der einzelnen Buchstaben im Alphabet durchgeführt wurde, welche der Empfänger in umgekehrter Richtung durchführte um wieder zum Klartext zu gelangen. Nachdem in diesem Falle die Frage, um wie viele Buchstaben eine Verschiebung stattgefunden hatte, nicht im Vordergrund stand, da durch eine Wiederholung des Verfahrens maximal nach dem 25. Versuch der Klartext vorlag, bestand der eigentliche Schutz der Nachricht darin, das Verfahren geheim zu halten. Lediglich aufgrund des Umstandes, dass ungewünschte Empfänger nichts über die Verschlüsselung wussten, konnte sie funktionieren.

In heutiger Zeit verhält es sich diesbezüglich anders, nachdem Informationen über verschiedene Verschlüsselungsverfahren überall frei verfügbar sind, so dass das einfache Cäsar-Verfahren mittlerweile zu den unsichersten Verfahren zählt. Vielmehr in den Vordergrund gerückt ist die Verwendung geeigneter Schlüssel, mit denen die Verschlüsselung durchgeführt wird. Die Verwendung geheimer Schlüssel sorgt dafür, dass je nach Umfang dieses Schlüssels eine Entschlüsselung nahezu unmöglich wird. Aufgrund dieses Umstandes verlagert sich die Entschlüs-

selungsproblematik für einen Abhörenden weg vom Verständnis des Verschlüsselungsverfahren hin zu der Beschaffung von Informationen über den Schlüssel selbst.

Auch hier kennt die Geschichte ein bekanntes Beispiel. Das Verschlüsselungssystem „Enigma“, das die Deutschen im Zweiten Weltkrieg einsetzen, konnte erst durch die Erbeutung von Codebüchern und einem Verschlüsselungsapparat entschlüsselt werden, da in den Codebüchern für jeden Tag separate, einzelne Codes angegeben waren. Die Verwendung und Verteilung derartiger Codebücher muss jedoch als einerseits extrem aufwändig, andererseits wie die Geschichte zeigt auch als anfällig angesehen werden.

Insbesondere in heutigen Zeiten, da Kommunikationsverbindungen im Wesentlichen über das Internet gebildet werden, stellt eine geeignete Verschlüsselung vertraulicher Daten den Anwender vor einige Herausforderungen. Es sind Verfahren bekannt, beispielsweise der sogenannte Diffie-Hellman-Schlüsselaustausch, bei denen der gemeinsame Schlüssel durch für den Abhörenden nicht umkehrbare Rechenoperationen ermittelt wird und die damit als weitgehend sichere Möglichkeiten zum Austausch von Schlüsseln über unsichere Kanäle gelten. Im speziellen genannten Fall besteht jedoch immer noch die Möglichkeit, durch einen so genannten Man-in-the-middle-Angriff die Nachrichten zu entschlüsseln, indem vorgetäuscht wird, dass eine direkte Verbindung besteht, während tatsächlich beide Kommunikationspartner mit einem zentralen, und damit abhörfähigen, Knoten kommunizieren.

Insbesondere bei einer Kommunikation im Internet, etwa bei Peer-to-Peer-Verbindungen wie beispielsweise einer Voice-over-IP-Verbindung, besteht die Gefahr, dass der dortige Server als abhörfähiger Knoten missbraucht wird.

Vor diesem Hintergrund liegt der vorliegenden Erfindung die Aufgabe zu Grunde, ein Verfahren zum Aufbau einer verschlüsselten Kommunikationsverbindung zwischen zwei Mobilgeräten zu schaffen, welches die Möglichkeit eröffnet, eine möglichst sichere Verschlüsselung einer Peer-to-Peer-Verbindung zu gewährleisten

und gleichzeitig das Problem des Schlüsselaustauschs auf ein möglichst einfach handhabbares Verfahren abzubilden.

Gelöst wird dieses Problem durch ein Verfahren zum Aufbau einer verschlüsselten Kommunikationsverbindung zwischen zwei Mobilgeräten gemäß den Merkmalen des Anspruchs 1. Weitere, sinnvolle Ausgestaltungen eines derartigen Verfahrens können den Unteransprüchen entnommen werden.

Erfindungsgemäß ist hierfür vorgesehen, dass in einem einmaligen Identifikationsschritt zunächst ein direkter Datenaustausch zwischen den beiden miteinander kommunizierenden Mobilgeräten stattfindet, was beispielsweise bei einem einmaligen Treffen der Nutzer dieser Mobilgeräte durchgeführt werden kann. Im Rahmen des Datenaustauschs bei diesem einmaligen Identifikationsschritt wird ein gemeinsamer Schlüssel ausgetauscht, so dass die Realisierung eines symmetrischen Verschlüsselungsverfahrens ermöglicht wird.

Zum Aufbau einer verschlüsselten Kommunikationsverbindung wird dann zunächst eine unverschlüsselte Kommunikationsverbindung aufgebaut, mit der die Gesprächsteilnehmer identifiziert werden können. Nachdem eine Identifizierung des jeweils auf der Gegenseite kommunizierenden Mobilgeräts stattgefunden hat und festgestellt wurde, dass mit diesem Mobilgerät ein einmaliger Identifikationsschritt stattgefunden hat, wird eine zweite Kommunikationsverbindung aufgebaut und der Datenteil der nachfolgend übersandten Nachrichten mit dem in dem einmaligen Identifikationsschritt ausgetauschten gemeinsamen Schlüssel verschlüsselt.

Nachdem aufgrund der einmaligen Identifikation der beiden Mobilgeräte der Schlüsselcode lediglich diesen beiden Mobilgeräten bekannt ist, kann nach einer gegenseitigen Identifikation somit sogleich in eine verschlüsselte Kommunikationsverbindung gewechselt werden, während dann die unverschlüsselte Kommunikationsverbindung, welche zum Aufbau der Kommunikation diente, wieder beendet werden kann. Es ist hierdurch auch möglich, bei Peer-to-Peer-Verbindungen

eine sichere Kommunikation zu ermöglichen, da eine Übertragung des Schlüsselcodes eingangs der Kommunikation weder direkt noch indirekt stattfindet.

Zur Vereinfachung des einmaligen Identifikationsschrittes zwischen den beiden Mobilgeräten und zur Erhöhung der insoweit zu wahrenden Sicherheit kann der einmalige Identifikationsschritt über eine kabelgebundene Übertragung, mittels Nahfeldkommunikation oder über eine Funkverbindung mit kurzer Reichweite erfolgen. In jedem Fall ist es hierbei erforderlich, auszuschließen, dass Dritte die Übertragung mitverfolgen können. Insbesondere kann die Nahfeldkommunikation derart ausgestaltet sein, dass ein Mobilgerät einen Schlüsselcode erstellt, beispielsweise in einem Zufallsverfahren, diesen Schlüsselcode in einen zweidimensionalen Barcode kodiert und diesen auf seinem Display wiedergibt, während anschließend das zweite Mobilgerät mit seinem optischen Sensor das Display des ersten Mobilgerätes scannt, so den zweidimensionalen Barcode erfasst und durch Entschlüsselung des zweidimensionalen Barcodes ebenfalls den Schlüsselcode erhält. Gleichzeitig können bei dieser Identifikation auch gerätegebundene Informationen, wie beispielsweise eindeutige Hardwareadressen und dergleichen, ausgetauscht werden, so dass die Kommunikationsmöglichkeiten nicht nur auf den Besitz des Schlüsselcodes, sondern auch an ein bestimmtes Mobilgerät gebunden sind. Insbesondere kann es vorgesehen sein, die beiden Hardwareadressen der Mobilgeräte in dem gemeinsamen Schlüsselcode zu verarbeiten.

Insoweit ist es notwendig, neben dem Schlüsselcode auch Identifikationsdaten wie beispielsweise einen Zugriffscode zur gegenseitigen Identifizierung mit zu übertragen, so dass bei dem Initiieren der ersten, unverschlüsselten Kommunikationsverbindung eine gegenseitige Identifikation ermöglicht wird.

Als unverschlüsselte Kommunikationsverbindung kann insbesondere eine Telefonverbindung durch einfaches Anrufen des zweiten Mobilgerätes, eine unverschlüsselte Datenverbindung durch das Internet bei bereits bekannter Internetadresse oder eine Internetverbindung unter Zwischenschaltung eines vermittelnden Servers aufgebaut werden. Im letzteren Fall kann die Anmeldung bei dem jeweiligen Server vor Aufbau der entsprechenden Verbindung erforderlich sein.

Soweit es sich bei der unverschlüsselten Kommunikationsverbindung um eine Telefonverbindung handelt, ist es erforderlich, für die anschließend aufzubauende Peer-to-Peer-Verbindung die erforderlichen Internetadressen der Mobilgeräte auszutauschen, so dass eine Adressierung der Nachrichten sinnvollerweise auch erfolgen kann. Im Falle einer direkten Kommunikation durch das Internet oder bei einer Zwischenschaltung des vermittelnden Servers sind die Adressdaten entweder den Mobilgeräten direkt bekannt oder wurden bei der Anmeldung an den Server weitergegeben und werden dann von dem Server bereitgestellt.

In konkreter Ausgestaltung kann die Sicherheit dadurch erhöht werden, dass jeweils eines der Mobilgeräte als Zentralgerät einen Zentralknoten eines sternförmigen Kommunikationsnetzes bildet, während das andere Mobilgerät als Peripheriegerät angeschlossen wird. Das Zentralgerät kann in diesem Fall ein Programmprodukt als native Applikation ausführen, welches nach einer Identifizierung in dem einmaligen Identifikationsschritt eine Internetapplikation generiert und diese für eine Ausführung auf dem Peripheriegerät auf einem Internetserver bereitstellt. In diese Internetapplikation ist in diesem Falle bereits die Zugriffsinformation und die Hardwareinformation des zweiten Mobilgerätes, welches durch die Ausführung der Internetapplikation als Peripherknoten in dem sternförmigen Kommunikationsnetz eingesetzt wird, eingeflossen, so dass die Internetapplikation lediglich von dem mit ihr verknüpften Mobilgerät ausgeführt werden kann. Insoweit ist auch vorgesehen, eine eigene, eindeutig identifizierbare Internetapplikation für jedes als Peripherknoten dem sternförmigen Kommunikationsnetz hinzuzufügende Mobilgerät einzurichten. In einem derartigen, sternförmigen Kommunikationsnetz kann dann der Zentralknoten seinerseits als Vermittlungsknoten zwischen mehreren Peripherknoten eingesetzt werden, um die Möglichkeiten der Kommunikation innerhalb des Kommunikationsnetzes zu verbessern. Im Übrigen ist jedoch vorgesehen, mehrere sternförmige Kommunikationsnetze so zu überlagern, dass praktisch jedes teilnehmende Mobilgerät als Zentralgerät in seinem eigenen sternförmigen Kommunikationsnetz fungiert.

Die vorstehend beschriebene Erfindung wird im Folgenden anhand eines Ausführungsbeispiels näher erläutert.

Es zeigen

Figur 1 zwei Mobilgeräte während eines einmaligen Identifikationsschrittes in einer schematischen Darstellung,

Figur 2 zwei Mobilgeräte während einer unverschlüsselten Kommunikationsverbindung auf drei alternativen Wegen in schematischer Darstellung,

Figur 3 zwei Mobilgeräte während der schließlich verschlüsselten Kommunikationsverbindung in einer schematischen Darstellung, sowie

Figur 4 eine schematische Darstellung einer codierten, verschlüsselten Nachricht.

Figur 1 zeigt ein erstes Mobilgerät 1 sowie ein zweites Mobilgerät 2, welche zur Durchführung eines ersten, einmaligen Identifikationsschrittes zum Aufbau einer verschlüsselten Kommunikationsverbindung eine Nahfeldkommunikation 3 aufbauen. Zielsetzung dieses Vorgehens soll letztendlich der Aufbau späterer, verschlüsselter Direktverbindungen zwischen den beiden Mobilgeräten 1 und 2, insbesondere über eine Internetverbindung, sein. Hierzu ist es erforderlich, einen Schlüsselcode 8 gemeinsam auf beiden Mobilgeräten 1 und 2 vorzuhalten, mit dem die Verschlüsselung der von dem ersten Mobilgerät 1 an das zweite Mobilgerät 2 und umgekehrt zu übersendenden Nachrichten 9 durchgeführt werden kann. Im Rahmen dieses ersten einmaligen Identifikationsschrittes werden zwischen den Mobilgeräten 1 und 2 Zugriffscodes zur gegenseitigen Identifizierung sowie ein gemeinsamer Schlüsselcodes zum Aufbau einer symmetrischen Verschlüsselung ausgetauscht, wobei der Austausch über eine kabelgebundene Direktverbindung stattfinden kann. Alternativ ist im Rahmen der Nahfeldkommunikation 3 die Möglichkeit gegeben, dass zunächst etwa drahtlos die Hardwareadresse des einen

Mobilgerätes 1 oder 2 an das andere Mobilgerät 2 oder 1 übertragen wird und schließlich der eigentliche Schlüsselcode in einen zweidimensionalen Barcode kodiert, am Display dargestellt und von dem jeweils anderen Mobilgerät 2, 1 von dessen optischem Sensor abgescannt und entschlüsselt wird.

Figur 2 zeigt den Aufbau der verschlüsselten Kommunikationsverbindung, wobei am Anfang einer derartigen verschlüsselten Kommunikationsverbindung zunächst der herkömmliche Aufbau einer unverschlüsselten Kommunikationsverbindung steht. Zwischen dem ersten Mobilgerät 1 und dem zweiten Mobilgerät 2 kann eine derartige Verbindung entweder als Serververbindung 4, als unverschlüsselte Direktverbindung 5 oder als Telefonverbindung 6 aufgebaut werden. Auch weitere Möglichkeiten stehen hierfür offen. Im Falle einer Serververbindung 4 wird sich sowohl das erste Mobilgerät 1 als auch das zweite Mobilgerät 2 an einen Server anmelden, woraufhin der Server jeweils die Adressdaten der Mobilgeräte 1 und 2 an den jeweils anderen Teilnehmer weitergibt, so dass anschließend die gewünschte verschlüsselte Direktverbindung 7 aufgebaut werden kann. Im Falle der unverschlüsselten Direktverbindung 5 durch das Internet ist die Adresslage bereits klar, da eine derartige Direktverbindung 5 lediglich bei bekannten Adressen aufgebaut werden kann. Die dritte Möglichkeit, welche hier in Bezug genommen werden soll, besteht in dem Aufbau einer Telefonverbindung 6, beispielsweise in Form einer GSM- oder UMTS-Verbindung, über die dann anschließend ebenfalls die Internetadressen der Mobilgeräte 1 und 2 ausgetauscht werden. Ergänzend werden in diesem erstem Handshake Zugriffsinformationen ausgetauscht, welche eine gegenseitige Identifikation der Mobilgeräte 1 und 2 zulassen.

Figur 3 zeigt die beiden Mobilgeräte 1 und 2 nach dem Aufbau der letztendlich gewünschten, verschlüsselten Direktverbindung 7, welche nach einer gegenseitigen Identifizierung mit den zuvor ausgetauschten Zugriffsdaten und unter Verwendung des initial ausgetauschten Schlüsselcodes 8 erfolgt. Eine derartige verschlüsselte Direktverbindung 7 kann als Datenverbindung zur Übertragung von Dateien verwendet werden, jedoch ist es ohne Weiteres auch möglich, eine derartige verschlüsselte Direktverbindung 7 etwa für Voice-over-IP-Verbindungen zu nutzen.

Figur 4 zeigt ein mögliches Beispiel der Kodierung einer im Rahmen der Erfindung genutzten Nachricht 9. Eine derartige Nachricht 9 besteht aus einem Header 10, aus einem Zeiger 11 und einem Datenteil mit verschlüsselten Daten 12, wobei die Daten durch Überlagerung des Schlüsselcodes 8, welcher bei dem einmaligen Identifikationsschritt ausgetauscht worden ist, verändert worden sind. Der Zeiger 11 zeigt hierbei auf eine Stelle des Schlüsselcodes 8, indem beispielsweise der Zeiger 11 eine zweistellige Zahl ist, welche auf die Stelle des Schlüsselcodes 8 hinweist. Beginnend mit dieser Stelle wird den verschlüsselten Daten 12 in jeder Position eine Zahl des Schlüsselcodes 8 sukzessive überlagert, wobei bei Erreichen des Endes des Schlüsselcodes 8 wieder von vorne begonnen wird. Auf Grund der Kenntnis des Schlüsselcodes 8 auf beiden Seiten sowie der Übermittlung des Zeigers 11 kann auf der Gegenseite die Nachricht 9 wieder entschlüsselt werden und damit auf die unverschlüsselten Nachrichten zugegriffen werden.

Vorstehend beschrieben ist somit ein Verfahren zum Aufbau einer verschlüsselten Kommunikationsverbindung zwischen zwei Mobilgeräten unter Nutzung einer Peer-to-Peer-Direktverbindung im Internet, wobei aufgrund einer ersten, einmaligen Identifikation zwischen den beteiligten Mobilgeräten eine sichere und vertrauenswürdige Übermittlung eines Schlüsselcodes erfolgt, so dass eine abhörsichere Übermittlung von Nachrichten durchgeführt werden kann.

B E Z U G S Z E I C H E N L I S T E

1 erstes Mobilgerät
2 zweites Mobilgerät
3 Nahfeldkommunikation
4 Serververbindung
5 unverschlüsselte Direktverbindung
6 Telefonverbindung
7 verschlüsselte Direktverbindung
8 Schlüsselcode
9 Nachricht
10 Header
11 Zeiger
12 verschlüsselte Daten

PATENTANSPRÜCHE

1. Verfahren zum Aufbau einer verschlüsselten Kommunikationsverbindung zwischen zwei Mobilgeräten (1, 2), bei dem in einem einmaligen Identifikationsschritt ein Datenaustausch zwischen den beiden Mobilgeräten (1, 2) stattfindet und bei jedem Aufbau einer Kommunikationsverbindung zunächst eine unverschlüsselte Kommunikationsverbindung aufgebaut wird und die Mobilgeräte (1, 2) nach gegenseitiger Identifizierung aufgrund der in dem einmaligen Identifikationsschritt ausgetauschten Daten zu einer verschlüsselten Kommunikationsverbindung zum Austausch verschlüsselter Daten wechseln, deren Verschlüsselung mithilfe eines in dem einmaligen Identifikationsschritt ausgetauschten Schlüsselcodes (8) erfolgt.

2. Verfahren gemäß Anspruch 1, dadurch gekennzeichnet, dass der Datenaustausch innerhalb des einmaligen Identifikationsschritts eine kabelgebundene Übertragung über eine Direktverbindung, eine Nahfeldkommunikation (3) oder eine Funkverbindung mit kurzer Reichweite vorsieht.

3. Verfahren gemäß einem der Ansprüche 1 oder 2, dadurch gekennzeichnet, dass im Rahmen des einmaligen Identifikationsschritts wenigstens ein Zugriffscode zur gegenseitigen Identifizierung der Mobilgeräte (1, 2) und ein Schlüsselcode (8) zur Verschlüsselung der zwischen den Mobilgeräten (1, 2) auszutauschenden Daten ausgetauscht werden.

4. Verfahren gemäß einem der vorhergehenden Ansprüche, dadurch gekennzeichnet, dass als unverschlüsselte Kommunikationsverbindung eine Telefonverbindung (6), eine unverschlüsselte Direktverbindung (5) durch das Internet oder eine Internetverbindung unter Zwischenschaltung eines vermittelnden Servers (4) aufgebaut wird.

5. Verfahren gemäß Anspruch 4, dadurch gekennzeichnet, dass es sich bei der unverschlüsselten Kommunikationsverbindung um eine Telefonverbin-

dung (6) handelt, in deren Rahmen die für den Aufbau der verschlüsselten Kommunikationsverbindung erforderlichen Adressen der Mobilgeräte (1, 2) ausgetauscht werden.

6. Verfahren gemäß einem der vorhergehenden Ansprüche, dadurch gekennzeichnet, dass eines der Mobilgeräte (1, 2) als Zentralgerät einen Zentralknoten eines sternförmigen Kommunikationsnetzes repräsentiert, während das andere Mobilgerät (2, 1) als Peripherge rät einen Peripherknoten dieses Kommunikationsnetzes darstellt, wobei das Zentralgerät ein Programmprodukt als native Applikation ausführt, welches nach dem einmaligen Identifikationsschritt unter Einbindung der im Rahmen des einmaligen Identifikationsschritts ausgetauschten Daten eine Internetapplikation zur ausschließlichen Kommunikation mit dem Zentralknoten generiert und, zur Ausführung auf dem Periphergerät, auf einem Internetserver bereitstellt.

7. Verfahren gemäß Anspruch 6, dadurch gekennzeichnet, dass das Programmprodukt für jeden hinzuzufügenden Peripherknoten eine eigene, eindeutig identifizierbare Internetapplikation generiert.

8. Verfahren gemäß einem der Ansprüche 6 oder 7, dadurch gekennzeichnet, dass die Ausführbarkeit jeder für einen Peripherknoten generierten Internetapplikation an eine eindeutige Hardwareadresse des Periphergeräts geknüpft wird.

9. Verfahren gemäß Anspruch 8, dadurch gekennzeichnet, dass die eindeutige Hardwareadresse im Rahmen des einmaligen Identifikationsschritts zwischen dem Zentralgerät und dem Periphergerät ausgetauscht wird.

10. Verfahren gemäß einem der vorhergehenden Ansprüche, dadurch gekennzeichnet, dass der Zentralknoten als Vermittlungsknoten zwischen mehreren Peripherknoten eingesetzt werden kann.

GEÄNDERTE ANSPRÜCHE
beim Internationalen Büro eingegangen am 17 Juni 2013 (17.06.2013)

1. Verfahren zum Aufbau einer verschlüsselten Kommunikationsverbindung zwischen zwei Mobilgeräten (1, 2), bei dem in einem einmaligen Identifikationsschritt ein Datenaustausch zwischen den beiden Mobilgeräten (1, 2) stattfindet und bei jedem Aufbau einer Kommunikationsverbindung zunächst eine unverschlüsselte Kommunikationsverbindung aufgebaut wird und die Mobilgeräte (1, 2) nach gegenseitiger Identifizierung aufgrund der in dem einmaligen Identifikationsschritt ausgetauschten Daten zu einer verschlüsselten Kommunikationsverbindung zum Austausch verschlüsselter Daten wechseln, deren Verschlüsselung mithilfe eines in dem einmaligen Identifikationsschritt ausgetauschten Schlüsselcodes (8) erfolgt,
dadurch gekennzeichnet, dass im Rahmen des einmaligen Identifikationsschritts wenigstens ein Zugriffscode zur gegenseitigen Identifizierung der Mobilgeräte (1, 2) und ein Schlüsselcode (8) zur Verschlüsselung der zwischen den Mobilgeräten (1, 2) auszutauschenden Daten ausgetauscht werden, indem der Zugriffscode und der Schlüsselcode (8) in einen zweidimensionalen Barcode kodiert und auf einem Display eines ersten Mobilgeräts (1) wiedergegeben wird und ein zweites Mobilgerät (2) das Display des ersten Mobilgeräts (1) mit einem optischen Sensor scannt, den zweidimensionalen Barcode erfasst und dekodiert.

2. Verfahren gemäß Anspruch 1, dadurch gekennzeichnet, dass als unverschlüsselte Kommunikationsverbindung eine Telefonverbindung (6), eine unverschlüsselte Direktverbindung (5) durch das Internet oder eine Internetverbindung unter Zwischenschaltung eines vermittelnden Servers (4) aufgebaut wird.

3. Verfahren gemäß Anspruch 2, dadurch gekennzeichnet, dass es sich bei der unverschlüsselten Kommunikationsverbindung um eine Telefonverbindung (6) handelt, in deren Rahmen die für den Aufbau der verschlüsselten Kommunikationsverbindung erforderlichen Adressen der Mobilgeräte (1, 2) ausgetauscht werden.

4. Verfahren gemäß einem der vorhergehenden Ansprüche, dadurch gekennzeichnet, dass eines der Mobilgeräte (1, 2) als Zentralgerät einen Zentralknoten eines sternförmigen Kommunikationsnetzes repräsentiert, während das andere Mobilgerät (2, 1) als Periphergerät einen Peripherknoten dieses Kommunikationsnetzes darstellt, wobei das Zentralgerät ein Programmprodukt als native Applikation ausführt, welches nach dem einmaligen Identifikationsschritt unter Einbindung der im Rahmen des einmaligen Identifikationsschritts ausgetauschten Daten eine Internetapplikation zur ausschließlichen Kommunikation mit dem Zentralknoten generiert und, zur Ausführung auf dem Periphergerät, auf einem Internetserver bereitstellt.

5. Verfahren gemäß Anspruch 4, dadurch gekennzeichnet, dass das Programmprodukt für jeden hinzuzufügenden Peripherknoten eine eigene, eindeutig identifizierbare Internetapplikation generiert.

6. Verfahren gemäß einem der Ansprüche 4 oder 5, dadurch gekennzeichnet, dass die Ausführbarkeit jeder für einen Peripherknoten generierten Internetapplikation an eine eindeutige Hardwareadresse des Periphergeräts geknüpft wird.

7. Verfahren gemäß Anspruch 6, dadurch gekennzeichnet, dass die eindeutige Hardwareadresse im Rahmen des einmaligen Identifikationsschritts zwischen dem Zentralgerät und dem Periphergerät ausgetauscht wird.

8. Verfahren gemäß einem der Ansprüche 4 bis 7, dadurch gekennzeichnet, dass der Zentralknoten als Vermittlungsknoten zwischen mehreren Peripherknoten eingesetzt werden kann.

ZEICHNUNG

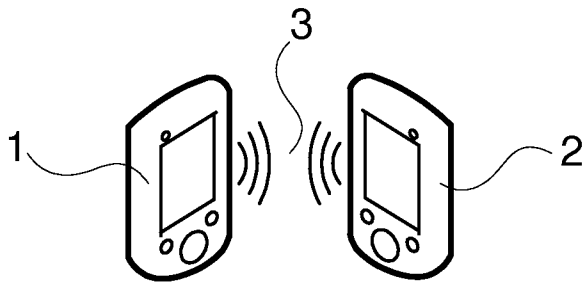

Fig. 1

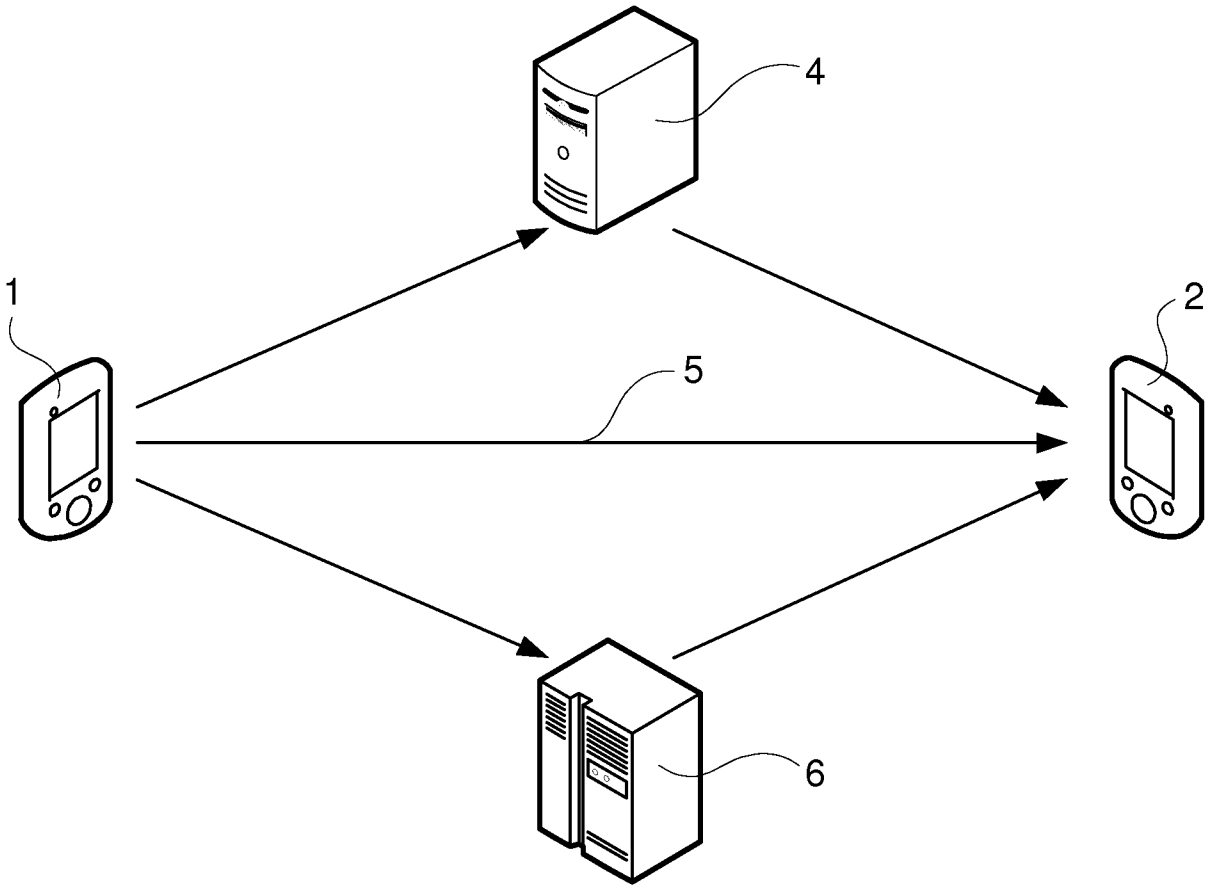

Fig. 2

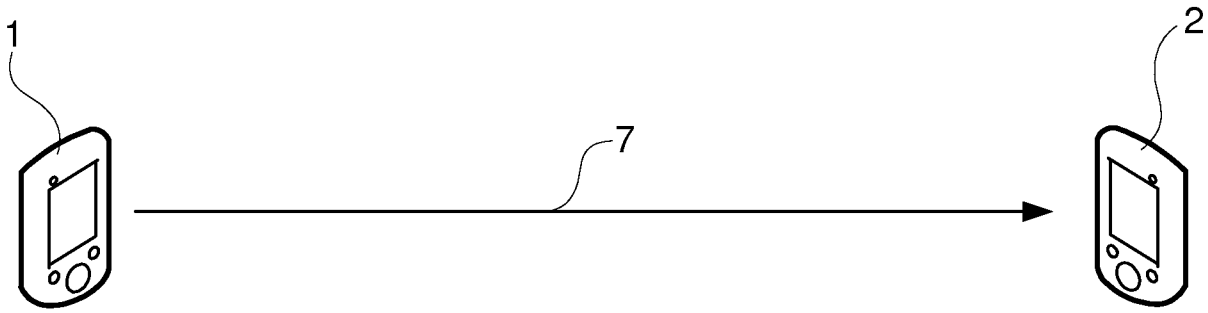

Fig. 3

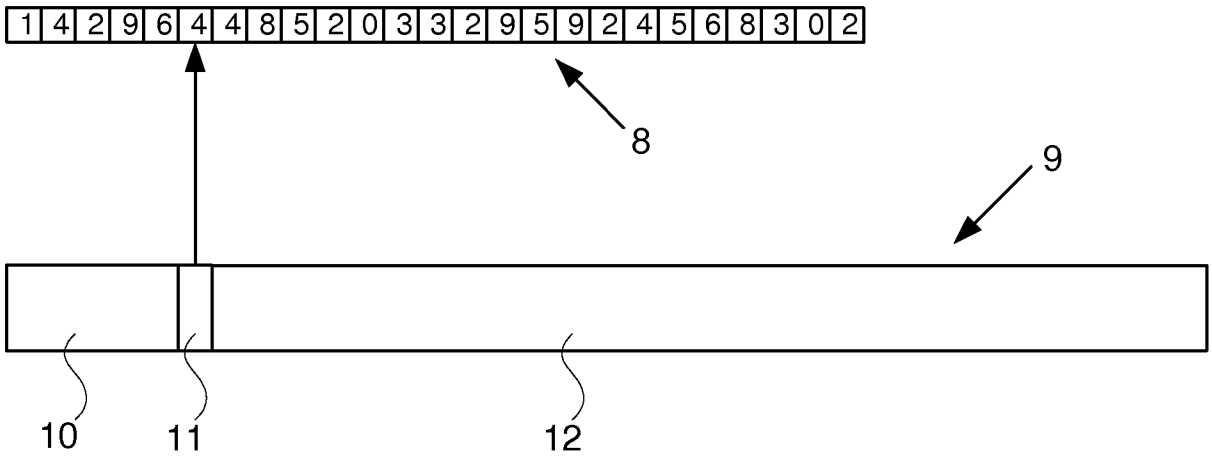

Fig. 4

INTERNATIONAL SEARCH REPORT

International application No
PCT/DE2012/100398

A. CLASSIFICATION OF SUBJECT MATTER
INV. G06F9/445 H04W12/04
ADD.

According to International Patent Classification (IPC) or to both national classification and IPC

B. FIELDS SEARCHED

Minimum documentation searched (classification system followed by classification symbols)
G06F H04W H04L

Documentation searched other than minimum documentation to the extent that such documents are included in the fields searched

Electronic data base consulted during the international search (name of data base and, where practicable, search terms used)

EPO-Internal, INSPEC, WPI Data

C. DOCUMENTS CONSIDERED TO BE RELEVANT

Category*	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
X	EP 1 940 115 A2 (INTEL CORP [US]) 2 July 2008 (2008-07-02) paragraph [0001] paragraphs [0011] - [0031] figures 1-3 claims 1-5	1-10
X	WO 2009/066212 A1 (NXP BV [NL]; RAZZELL CHARLES [US]) 28 May 2009 (2009-05-28) page 1, line 5 - page 2, line 24 page 3, line 19 - page 8, line 2 figures 1-3	1-10

-/--

[X] Further documents are listed in the continuation of Box C.

[X] See patent family annex.

* Special categories of cited documents :

"A" document defining the general state of the art which is not considered to be of particular relevance

"E" earlier application or patent but published on or after the international filing date

"L" document which may throw doubts on priority claim(s) or which is cited to establish the publication date of another citation or other special reason (as specified)

"O" document referring to an oral disclosure, use, exhibition or other means

"P" document published prior to the international filing date but later than the priority date claimed

"T" later document published after the international filing date or priority date and not in conflict with the application but cited to understand the principle or theory underlying the invention

"X" document of particular relevance; the claimed invention cannot be considered novel or cannot be considered to involve an inventive step when the document is taken alone

"Y" document of particular relevance; the claimed invention cannot be considered to involve an inventive step when the document is combined with one or more other such documents, such combination being obvious to a person skilled in the art

"&" document member of the same patent family

Date of the actual completion of the international search	Date of mailing of the international search report
8 April 2013	16/04/2013

Name and mailing address of the ISA/	Authorized officer
European Patent Office, P.B. 5818 Patentlaan 2 NL - 2280 HV Rijswijk Tel. (+31-70) 340-2040, Fax: (+31-70) 340-3016	Noll, Joachim

1

Form PCT/ISA/210 (second sheet) (April 2005)

INTERNATIONAL SEARCH REPORT

International application No
PCT/DE2012/100398

C(Continuation). DOCUMENTS CONSIDERED TO BE RELEVANT

Category*	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
X	EP 1 274 194 A1 (TOSHIBA KK [JP]) 8 January 2003 (2003-01-08) paragraphs [0001] - [0007] paragraphs [0010] - [0041] figures 1-7 claims 1-5	1-10

X	EP 2 306 692 A1 (RESEARCH IN MOTION LTD [CA]) 6 April 2011 (2011-04-06)	1-5
Y	paragraphs [0001] - [0022] paragraphs [0027] - [0100] figures 1-7	6-10

Y	US 7 065 070 B1 (CHANG IFAY F [US]) 20 June 2006 (2006-06-20) column 1, lines 50-59 column 2, line 57 - column 3, line 58 column 4, line 35 - column 10, line 33 figures 1-8 claims 1-18	6-10

1

INTERNATIONAL SEARCH REPORT

Information on patent family members

International application No
PCT/DE2012/100398

Patent document cited in search report	Publication date	Patent family member(s)	Publication date
EP 1940115 A2	02-07-2008	CN 101286839 A	15-10-2008
		EP 1940115 A2	02-07-2008
		JP 2008178092 A	31-07-2008
		KR 20080063130 A	03-07-2008
		US 2008162937 A1	03-07-2008
WO 2009066212 A1	28-05-2009	CN 101868954 A	20-10-2010
		US 2010281261 A1	04-11-2010
		WO 2009066212 A1	28-05-2009
EP 1274194 A1	08-01-2003	EP 1274194 A1	08-01-2003
		JP 2003018148 A	17-01-2003
		US 2003007641 A1	09-01-2003
EP 2306692 A1	06-04-2011	CA 2714832 A1	02-04-2011
		EP 2306692 A1	06-04-2011
US 7065070 B1	20-06-2006	US 7065070 B1	20-06-2006
		US 7643435 B1	05-01-2010

INTERNATIONALER RECHERCHENBERICHT

Internationales Aktenzeichen
PCT/DE2012/100398

A. KLASSIFIZIERUNG DES ANMELDUNGSGEGENSTANDES
INV. G06F9/445 H04W12/04
ADD.

Nach der Internationalen Patentklassifikation (IPC) oder nach der nationalen Klassifikation und der IPC

B. RECHERCHIERTE GEBIETE

Recherchierter Mindestprüfstoff (Klassifikationssystem und Klassifikationssymbole)
G06F H04W H04L

Recherchierte, aber nicht zum Mindestprüfstoff gehörende Veröffentlichungen, soweit diese unter die recherchierten Gebiete fallen

Während der internationalen Recherche konsultierte elektronische Datenbank (Name der Datenbank und evtl. verwendete Suchbegriffe)
EPO-Internal, INSPEC, WPI Data

C. ALS WESENTLICH ANGESEHENE UNTERLAGEN

Kategorie*	Bezeichnung der Veröffentlichung, soweit erforderlich unter Angabe der in Betracht kommenden Teile	Betr. Anspruch Nr.
X	EP 1 940 115 A2 (INTEL CORP [US]) 2. Juli 2008 (2008-07-02) Absatz [0001] Absätze [0011] - [0031] Abbildungen 1-3 Ansprüche 1-5 -----	1-10
X	WO 2009/066212 A1 (NXP BV [NL]; RAZZELL CHARLES [US]) 28. Mai 2009 (2009-05-28) Seite 1, Zeile 5 - Seite 2, Zeile 24 Seite 3, Zeile 19 - Seite 8, Zeile 2 Abbildungen 1-3 -----	1-10

-/--

[X] Weitere Veröffentlichungen sind der Fortsetzung von Feld C zu entnehmen [X] Siehe Anhang Patentfamilie

* Besondere Kategorien von angegebenen Veröffentlichungen :
"A" Veröffentlichung, die den allgemeinen Stand der Technik definiert, aber nicht als besonders bedeutsam anzusehen ist
"E" frühere Anmeldung oder Patent, die bzw. das jedoch erst am oder nach dem internationalen Anmeldedatum veröffentlicht worden ist
"L" Veröffentlichung, die geeignet ist, einen Prioritätsanspruch zweifelhaft erscheinen zu lassen, oder durch die das Veröffentlichungsdatum einer anderen im Recherchenbericht genannten Veröffentlichung belegt werden soll oder die aus einem anderen besonderen Grund angegeben ist (wie ausgeführt)
"O" Veröffentlichung, die sich auf eine mündliche Offenbarung, eine Benutzung, eine Ausstellung oder andere Maßnahmen bezieht
"P" Veröffentlichung, die vor dem internationalen Anmeldedatum, aber nach dem beanspruchten Prioritätsdatum veröffentlicht worden ist
"T" Spätere Veröffentlichung, die nach dem internationalen Anmeldedatum oder dem Prioritätsdatum veröffentlicht worden ist und mit der Anmeldung nicht kollidiert, sondern nur zum Verständnis des der Erfindung zugrundeliegenden Prinzips oder der ihr zugrundeliegenden Theorie angegeben ist
"X" Veröffentlichung von besonderer Bedeutung; die beanspruchte Erfindung kann allein aufgrund dieser Veröffentlichung nicht als neu oder auf erfinderischer Tätigkeit beruhend betrachtet werden
"Y" Veröffentlichung von besonderer Bedeutung; die beanspruchte Erfindung kann nicht als auf erfinderischer Tätigkeit beruhend betrachtet werden, wenn die Veröffentlichung mit einer oder mehreren Veröffentlichungen dieser Kategorie in Verbindung gebracht wird und diese Verbindung für einen Fachmann naheliegend ist
"&" Veröffentlichung, die Mitglied derselben Patentfamilie ist

Datum des Abschlusses der internationalen Recherche	Absendedatum des internationalen Recherchenberichts
8. April 2013	16/04/2013

Name und Postanschrift der Internationalen Recherchenbehörde	Bevollmächtigter Bediensteter
Europäisches Patentamt, P.B. 5818 Patentlaan 2 NL - 2280 HV Rijswijk Tel. (+31-70) 340-2040, Fax: (+31-70) 340-3016	Noll, Joachim

1

C. (Fortsetzung) ALS WESENTLICH ANGESEHENE UNTERLAGEN

Kategorie*	Bezeichnung der Veröffentlichung, soweit erforderlich unter Angabe der in Betracht kommenden Teile	Betr. Anspruch Nr.
X	EP 1 274 194 A1 (TOSHIBA KK [JP]) 8. Januar 2003 (2003-01-08) Absätze [0001] - [0007] Absätze [0010] - [0041] Abbildungen 1-7 Ansprüche 1-5 -----	1-10
X	EP 2 306 692 A1 (RESEARCH IN MOTION LTD [CA]) 6. April 2011 (2011-04-06)	1-5
Y	Absätze [0001] - [0022] Absätze [0027] - [0100] Abbildungen 1-7 -----	6-10
Y	US 7 065 070 B1 (CHANG IFAY F [US]) 20. Juni 2006 (2006-06-20) Spalte 1, Zeilen 50-59 Spalte 2, Zeile 57 - Spalte 3, Zeile 58 Spalte 4, Zeile 35 - Spalte 10, Zeile 33 Abbildungen 1-8 Ansprüche 1-18 -----	6-10

1

INTERNATIONALER RECHERCHENBERICHT

Angaben zu Veröffentlichungen, die zur selben Patentfamilie gehören

Internationales Aktenzeichen
PCT/DE2012/100398

Im Recherchenbericht angeführtes Patentdokument	Datum der Veröffentlichung	Mitglied(er) der Patentfamilie	Datum der Veröffentlichung
EP 1940115 A2	02-07-2008	CN 101286839 A	15-10-2008
		EP 1940115 A2	02-07-2008
		JP 2008178092 A	31-07-2008
		KR 20080063130 A	03-07-2008
		US 2008162937 A1	03-07-2008
WO 2009066212 A1	28-05-2009	CN 101868954 A	20-10-2010
		US 2010281261 A1	04-11-2010
		WO 2009066212 A1	28-05-2009
EP 1274194 A1	08-01-2003	EP 1274194 A1	08-01-2003
		JP 2003018148 A	17-01-2003
		US 2003007641 A1	09-01-2003
EP 2306692 A1	06-04-2011	CA 2714832 A1	02-04-2011
		EP 2306692 A1	06-04-2011
US 7065070 B1	20-06-2006	US 7065070 B1	20-06-2006
		US 7643435 B1	05-01-2010