

(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
26. November 2009 (26.11.2009)

(10) Internationale Veröffentlichungsnummer
WO 2009/141035 A1

- (51) Internationale Patentklassifikation:
H04W 8/26 (2009.01)
- (21) Internationales Aktenzeichen: PCT/EP2009/002827
- (22) Internationales Anmeldedatum:
17. April 2009 (17.04.2009)
- (25) Einreichungssprache: Deutsch
- (26) Veröffentlichungssprache: Deutsch
- (30) Angaben zur Priorität:
10 2008 024 798.7 23. Mai 2008 (23.05.2008) DE
- (71) Anmelder (für alle Bestimmungsstaaten mit Ausnahme von US): **T-MOBILE INTERNATIONAL AG** [DE/DE]; Landgrabenweg 151, 53227 Bonn (DE).
- (72) Erfinder; und
- (75) Erfinder/Anmelder (nur für US): **KALINER, Stefan** [DE/DE]; Oelbergstr. 94c, 53639 Königswinter (DE).
- (74) Anwalt: **METHLING, Frank-O.**; Cohausz Dawidowicz Hannig & Sozien, Schumannstrasse 97-99, 40237 Düsseldorf (DE).
- (81) Bestimmungsstaaten (soweit nicht anders angegeben, für jede verfügbare nationale Schutzrechtsart): AE, AG, AL, AM, AO, AT, AU, AZ, BA, BB, BG, BH, BR, BW, BY, BZ, CA, CH, CN, CO, CR, CU, CZ, 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, PG, PH, PL, PT, RO, RS, RU, SC, SD, SE, SG, SK, SL, SM, ST, SV, SY, 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, LS, MW, MZ, NA, SD, SL, SZ, TZ, UG, ZM, ZW), eurasisches (AM, AZ, BY, KG, KZ, MD, RU, TJ, TM), europäisches (AT, BE, BG, CH, CY, CZ, DE, DK, EE, ES, FI, FR, GB, GR, HR, HU, IE, IS, IT, LT,

[Fortsetzung auf der nächsten Seite]

(54) Title: METHOD FOR OVER-THE-AIR PERSONALIZING OF CHIP CARDS IN TELECOMMUNICATIONS

(54) Bezeichnung: VERFAHREN ZUR OVER-THE-AIR PERSONALISIERUNG VON CHIPKARTEN IN DER TELEKOMMUNIKATION

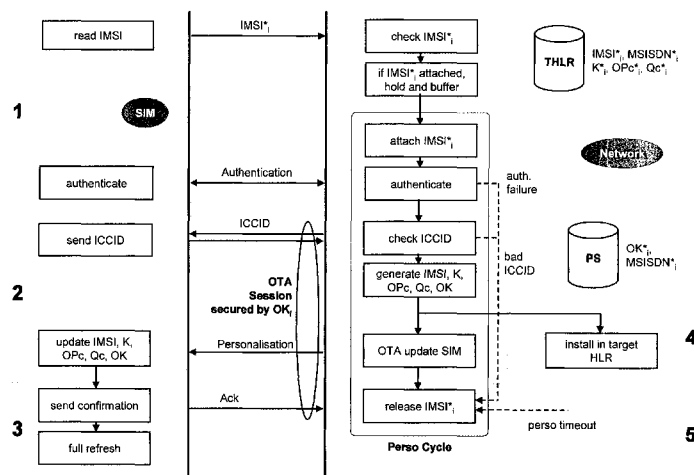


Fig. 1

(57) Abstract: The invention relates to a method for commissioning and personalizing a subscriber identification module SIM, wherein the SIM is set up with a non-individual and preliminary set (S*) of initial identifying and authenticating parameters prior to first commissioning, said set comprising at least one non-individual and preliminary subscriber identification (IMSI*) and a non-individual and preliminary secret key (K*), wherein the parameter set (S*) allows first commissioning of the SIM in a mobile telecommunications network by means of a mobile terminal device, wherein personalizing is performed after the first commissioning of the SIM, in that an individual and final subscriber data set (S) is transferred to and stored on the SIM, particularly comprising a unique final subscriber identification (IMSI) and a unique final secret key (K), particularly in that the final subscriber data set (S) is transferred by means of a regular connection of the mobile telecommunications system using the preliminary set (S*). The number of potential preliminary subscriber data sets is prescribed and is particularly much less than the total number of subscriber identification modules (SIM) equipped with said data sets. It can also be reused cyclically. The final subscriber data set is first stored after the mobile terminal device confirms that the personalization process was successful. Otherwise, the personalization request is automatically repeated, or the personalization data are sent again.

(57) Zusammenfassung:

[Fortsetzung auf der nächsten Seite]



WO 2009/141035 A1



LU, LV, MC, MK, MT, NL, NO, PL, PT, RO, SE, SI, **Veröffentlicht:**
SK, TR), OAPI (BF, BJ, CF, CG, CI, CM, GA, GN, GQ, — *mit internationalem Recherchenbericht (Artikel 21 Absatz*
GW, ML, MR, NE, SN, TD, TG). *3)*

Die Erfindung betrifft ein Verfahren zur Inbetriebnahme und Personalisierung eines Teilnehmeridentifizierungsmoduls SIM, wobei das SIM vor der ersten Inbetriebnahme mit einem nicht-individuellen und vorläufigen Satz (S*) initialer Identifizierungs- und Authentisierungsparameter ausgerüstet wird, enthaltend zumindest eine nicht-individuelle und vorläufige Teilnehmeridentifikation (IMSI*) und einen nicht-individuellen und vorläufigen Geheimschlüssel (K*), wobei der Parametersatz (S*) eine erste Inbetriebnahme des SIM in einem Mobilfunknetz mittels eines Mobilfunkendgerätes gestattet, wobei nach der ersten Inbetriebnahme des SIM eine Personalisierung durchgeführt wird, indem ein individueller und endgültiger Teilnehmerdatensatz (S) übertragen und auf dem SIM gespeichert wird, insbesondere enthaltend eine eindeutige endgültige Teilnehmeridentifikation (IMSI) und einen eindeutigen endgültigen Geheimschlüssel (K), insbesondere dass der endgültige Teilnehmerdatensatz (S) über eine reguläre Verbindung des Mobilfunksystems unter Verwendung des vorläufigen Satzes (S*) übertragen wird. Die Anzahl der möglichen vorläufigen Teilnehmerdatensätze ist festgelegt und insbesondere viel kleiner als die Anzahl der insgesamt mit diesen Datensätzen ausgerüsteten Teilnehmeridentifizierungsmodule (SIM). Sie kann auch zyklisch wiederverwendet werden. Die Speicherung des endgültigen Teilnehmerdatensatzes erfolgt erst nach Bestätigung des Mobilfunkgerätes, dass der Personalisierungsvorgang erfolgreich war. Anderenfalls wird eine automatische Wiederholung der Personalisierungsanfrage bzw. ein erneuter Versand der Personalisierungsdaten durchgeführt.

Verfahren zur Over-The-Air Personalisierung von Chipkarten in der Telekommunikation

Die Erfindung betrifft ein Verfahren zur Inbetriebnahme und Personalisierung eines Teilnehmeridentifizierungsmoduls SIM.

Chipkarten werden in der Telekommunikation, insbesondere z.B. in den mobilen GSM oder UMTS Systemen, zur eindeutigen und sicheren Identifizierung der Teilnehmer wie auch zur Bereitstellung vieler Sonderfunktionen und Mehrwertdienste eingesetzt. Die je nach Generation und Art des zugrunde liegenden Systemstandards z.B. als UICC, SIM, USIM, R-UIM oder auch ISIM bezeichneten Chipkarten oder Chipkarten-Applikationen (zusammenfassend als "SIM" oder gleichbedeutend als Teilnehmeridentifizierungsmodul bezeichnet) tragen dazu eine Vielzahl spezieller Parameter, geheime Schlüssel und weitere Elemente unterschiedlichster Art, z.B. mit Netzbetreiber-, Anbieter-, Produkt- oder Teilnehmerbezug.

Zur Inbetriebnahme eines mobilen Endgerätes und Teilnahme am Mobilfunkdienst ist ein SIM mit bestimmten individuellen Daten - mindestens Teilnehmeridentität IMSI, Geheimschlüssel K und individuelle Parameter für den Authentisierungsalgorithmus - zwingend erforderlich. Übereinstimmende Elemente müssen in den Teilnehmerdatenbanken (z.B. HLR/AC oder HSS) des Heimatnetzes vorhanden sein, andernfalls ist kein Verbindungsaufbau möglich, weder teilnehmerseitig noch netzseitig.

Das Laden der SIMs und die Ausprägung der Individualdaten erfolgt im Rahmen der Kartenherstellung bei der so genannten Personalisierung, in jedem Falle lange bevor das Teilnehmeridentifizierungsmodul SIM zum Einsatz kommt. Die Wertschöpfungskette der Kartenbereitstellung stellt sich i.d.R. wie folgt dar:

- **Chiphersteller:** Fertigt den Chip mit (Teilen der) Betriebssoftware.
- **Kartenhersteller:** Fertigt den Kartenkörper, implantiert den Chip, lädt ggf. weitere, nicht-individuelle Teile der Betriebssoftware und entsprechende Daten.
- **Personalisierer:** Lädt höher individualisierte Daten, individuelle Teilnehmerkennungen, Geheimschlüssel und ggf. weitere Teile der Software (Applikationen). Tauscht Individualdaten mit dem Netzbetreiber aus. Ist i.d.R. mit dem Kartenhersteller identisch.
- **Verpacker/Logistiker:** Verpackt und versendet die personalisierten Chipkarten an den Netzbetreiber oder andere Bestimmungsorte. Kann mit dem Kartenhersteller und/oder dem Personalisierer identisch sein.
- **Netzbetreiber:** Betreibt das Kommunikationsnetz. Definiert die Personalisierung für seine Produkte, liefert alle Vorgaben an den Personalisierer, erhält Individualdaten (mindestens IMSI, K und individuelle Parameter des Authentisierungsalgorithmus) vom Personalisierer zur Einrichtung der Teilnehmerverhältnisse in seinen Datenbanken.

Am Ende des Bereitstellungsprozesses befinden sich die SIMs in den Verkaufsstellen des Netzbetreibers. Erst beim Abschluss eines Mobilfunkvertrages erfolgt im Rahmen der so genannten Aktivierung die Zuordnung zum konkreten Kunden und die Vergabe einer Rufnummer. Die Aktivierung setzt das Vorhandensein des Teilnehmerverhältnisses in den Datenbanken des Netzbetreibers voraus.

Als Nachteile dieser Prozesskette, insbesondere der zentralisierten Personalisierung, sind anzuführen:

- Spezialisierung und Individualisierung des Produktes früh in der Bereitstellungskette, der tatsächliche Bedarf kann zu diesem Zeitpunkt nur abgeschätzt werden.
- Ressourcenbindung (Datenbank- und Nummernkapazität) beim Netzbetreiber erfolgt z.T. lange vor dem eigentlichen Bedarf.
- Sehr spezielle Dienstleistung mit technisch aufwändigen Lösungen und eingeschränkter Flexibilität. Hoher Aufwand für die Betreuung des externen Personalisierers. Änderungen werden i.d.R. nach Angebot beauftragt, dann entwickelt, getestet und abgenommen, mit entsprechendem Zeitbedarf. Notwendige Flexibilität erfordert komplexe Schnittstellen.
- Erhebliche Schwierigkeiten beim Handling neuer SIM-Bauformen, etwa nicht-entnehmbare oder "Machine-to-Machine" (M2M) Varianten. Führt zu ungünstiger Spezialisierung bereits bei Vorprodukten. Innovationsbremse.
- Alternative "Soft"-Konzepte für SIMs sind bei herkömmlicher Personalisierung vollständig unmöglich.

Die Aufgabe der Erfindung ist es daher, ein Verfahren zur Inbetriebnahme und Personalisierung eines Teilnehmeridentifizierungsmoduls SIM derart weiterzubilden, das die Nachteile des Verfahrens nach dem Stand der Technik überwindet, und es insbesondere gestattet, dass ohne eine frühzeitige Bindung von Ressourcen, wie beispielsweise die Datenbank- und Nummernkapazität, eine dem aktuellen Bedarf gerecht werdende Bereitstellung personalisierter und zum Betrieb in einem Mobilfunknetz freigegebene Teilnehmeridentifizierungsmodule SIM jederzeit möglich ist.

Diese Aufgabe wird mit einem Verfahren gemäß Anspruch 1 gelöst. Weitere vorteilhafte Ausgestaltungen des erfindungsgemäßen Verfahrens sind in den Unteransprüchen angegeben.

Besonders vorteilhaft bei dem erfindungsgemäßen Verfahren zur Inbetriebnahme und Personalisierung eines Teilnehmeridentifizierungsmoduls SIM ist es, dass das

SIM vor der ersten Inbetriebnahme mit einem nicht-individuellen und vorläufigen Satz (S*) initialer Identifizierungs- und Authentisierungsparameter ausgerüstet wird, enthaltend zumindest eine nicht-individuelle und vorläufige Teilnehmeridentifikation (IMSI*) und einen nicht-individuellen und vorläufigen Geheimschlüssel (K*), wobei der Parametersatz (S*) eine erste Inbetriebnahme des SIM in einem Mobilfunknetz mittels eines Mobilfunkendgerätes gestattet, wobei nach der ersten Inbetriebnahme des SIM eine Personalisierung durchgeführt wird, indem ein individueller und endgültiger Teilnehmerdatensatz (S) übertragen und auf dem SIM gespeichert wird, insbesondere enthaltend eine eindeutige endgültige Teilnehmeridentifikation (IMSI) und einen Geheimschlüssel (K), insbesondere dass der endgültige Teilnehmerdatensatz (S) über eine reguläre Verbindung des Mobilfunksystems unter Verwendung von (S*) übertragen wird.

Der vorläufige Satz (S*) initialer Identifizierungs- und Authentisierungsparameter enthält somit zumindest eine nicht-individuelle und vorläufige Teilnehmeridentifikation (IMSI*) und einen nicht-individuellen und vorläufigen Geheimschlüssel (K*), wobei der Parametersatz (S*) eine erste Inbetriebnahme des SIM in einem Mobilfunknetz mittels eines Mobilfunkendgerätes gestattet, d.h. dass sowohl die Teilnehmeridentifikation als auch der Geheimschlüssel als Bestandteile des vorläufigen Satzes (S*) initialer Identifizierungs- und Authentisierungsparameter nicht-individuell und nur vorläufig sind.

Hierdurch ist es zunächst möglich, eine Vielzahl von Teilnehmeridentifizierungsmodulen SIM (Subscriber Identity Module), die eine Nutzung der Dienste eines Mobilfunknetzes gestatten, mit nicht-individuellen und vorläufigen Parameterdatensätzen auszustatten, ohne dass bereits die entsprechende Anzahl von Ressourcen wie beispielsweise eindeutig zugeordnete Teilnehmeridentitäten IMSI und Mobilfunkrufnummern MSISDN zugeordnet werden müssen, da der vorläufige Parameterdatensatz eine erste Inbetriebnahme, d.h. ein Einbuchen in ein Mobilfunknetz gestattet, und sodann netzseitig die Personalisierung des SIM durchgeführt wird, indem ein endgültiger Teilnehmerdatensatz generiert, über die bestehende Funkverbindung oder über eine besonders gesicherte Funkverbindung übertragen und auf dem SIM gespeichert wird. Die endgültigen Teilnehmerdaten, die auf dem SIM gespeichert werden und der

Teilnehmeridentifikation bei der Nutzung von Diensten des Mobilfunknetzes dienen, werden somit im Rahmen eines standardgemäßen (Over The Air – OTA) Prozesses zur dem SIM übertragen. Auch hierdurch werden in vorteilhafter Weise die vorhandenen Ressourcen und Netzkapazitäten genutzt.

Die vorliegende Erfindung ermöglicht die Verlagerung der Personalisierung räumlich vom externen Personalisierer in die Domäne des Netzbetreibers und zeitlich an das Ende der Bereitstellungskette in den idealen Zeitpunkt der ersten Inbetriebnahme des mobilen Endgerätes.

Durch das vorgeschlagene Verfahren gelingt es, Teilnehmeridentifizierungsmodule (SIM) für ein mobiles Kommunikationssystem vollständig ohne individuelle Daten herzustellen (abgesehen von z.B. einer fortlaufenden Seriennummer) und zur Auslieferung zu bringen. Zu diesem Zeitpunkt tragen sie stattdessen spezielle nicht-individuelle und temporäre Identifizierungsdaten, die aber trotzdem eine standardgerechte Verbindung zum Netz des Betreibers ermöglichen. Mit OTA Mechanismen erfolgt dann die individuelle Personalisierung der endgültigen Parameter des Teilnehmerverhältnisses und die weitere dedizierte Ausrüstung der SIM mit Daten und Applikationen. Die kartenseitige Gestaltung der Technik ermöglicht ferner die unbegrenzte Wiederholung des Prozesses (Repersonalisierung, auch im Rahmen eines Netzbetreiberwechsels) und jederzeitige Änderbarkeit aller relevanten Daten auf gleichem Wege. Die Vorteile sind im einzelnen:

- Die individuelle Konfiguration der SIM erfolgt zum spätestens möglichen Zeitpunkt, bis dahin bleibt die größte Flexibilität hinsichtlich des Einsatzes der SIM erhalten.
- Da keine individuelle Personalisierung im Rahmen der Kartenherstellung mehr erfolgt, kann dieser Prozessschritt ersatzlos entfallen. Die genannten Nachteile des Standes der Technik werden vermieden.
- Die Schnittstelle zum Kartenhersteller vereinfacht sich wesentlich, da keine Personalisierungsparameter mehr zu übertragen sind und keine sicherheitskritischen Individualdaten mehr zurückgeliefert werden.

- Im Rahmen der Kartenherstellung erfolgt keinerlei Einrichtung in den Datenbanken des Netzbetreibers, damit auch keine Ressourcenbindung weit vor dem eigentlichen Bedarf.
- Es ist grundsätzlich keine Speicherung von Individualdaten erforderlich, weder beim Kartenhersteller, Netzbetreiber oder einer dritten Partei.
- Moderne Alternativen zur herkömmlichen SIM werden ermöglicht und erhalten zusätzliche Attraktivität: Bei Verwendung von nicht-entnehmbaren oder "M2M"-Modulen kann die Rolle des Kartenherstellers zusätzlich eingespart werden, da der Chiphersteller direkt ausliefern kann. Bei Soft-Konzepten entfielen sogar die Rolle des Chipherstellers in der Bereitstellungskette.
- Die ohnehin vom Netzbetreiber bereitzuhaltende Infrastruktur zum gezielten OTA-Customising der SIM nach Inbetriebnahme (wenn z.B. Endgerät und Tarif des Kunden feststehen) übernimmt zusätzlich die Aufgabe der Personalisierung und wird effektiver genutzt. Dadurch entstehen Synergieeffekte.

Neuartige SIM-Bauformen, die ohnehin implizit Änderungen am tradierten Rollenmodells voraussetzen bzw. verursachen (etwa maschinell eingesetzte, eingelötete oder in Software realisierte Varianten), ihre Vorteile umso besser ausspielen können, je später sie individualisiert und spezialisiert werden. Diese Varianten gelangen i.d.R. nicht mehr in die Hände des Benutzers und werden festes Bestandteil eines Endgerätes lange bevor der Netzbetreiber bekannt ist. Weiterhin kann sich dieser während des Lebenszyklus des Endgerätes verändern. So entsteht im Rahmen der Diskussion um zukünftige Formen der SIM regelmäßig die Frage nach Repersonalisierbarkeit. Ideal wäre außerdem eine weitgehende Unabhängigkeit von einem Netzbetreiber bis zum Moment der Inbetriebnahme um eine möglichst einfache Produktion zu erlauben, ohne aufwändige Schnittstellen, die Verwaltung betreiberspezifischer Nummernräume, proprietärer Authentisierungsalgorithmen, etc.

Die vorliegende Erfindung ermöglicht genau diese wichtigen Merkmale, wobei der initiale Heimatbetreiber (oder die Betreibergruppe) jederzeit feststeht aber weiter keinen Abstimmungsbedarf für individuelle Daten erfordert. Trotzdem hat der

Netzbetreiber über die Ziel-Personalisierung - die niemand außer ihm vornehmen kann - weiterhin vollständige Einfluss- und Gestaltungsmöglichkeiten.

Chipkarten gemäß der Erfindung sind vorzugsweise mit einem nicht-individuellen Satz initialer Identifizierungs- und Authentisierungsparameter

$$S^*_i = \{IMS^*_i, K^*_i, OPC^*_i, QC^*_i, OK^*_i\} \text{ mit } i = 0, 1, \dots, N-1 \text{ und } N \ll M;$$

ausgerüstet, wobei IMS^*_i die gültige Netzkennung MCC und MNC des Betreibers enthalten kann. Mit N seien die Gesamtmenge der S^*_i und mit M die Menge der solcherart insgesamt für einen Netzbetreiber hergestellten SIM bezeichnet. Innerhalb von M wiederholen sich die S^*_i also M/N -mal und sind damit nicht-eindeutig und nicht-individuell.

Als einziges individuelles Merkmal kann beispielsweise die übliche Seriennummer (ICCID) hinzukommen, die vom Hersteller während der Produktion fortlaufend zugeordnet wird. Wichtig ist, dass alle vom Hersteller im laufenden Produktionsprozess zuzuordnenden Daten vollautomatisch und ohne spezielle (individuelle) Vorgaben des Netzbetreibers vergeben werden.

Insbesondere erfolgt außerdem keine Speicherung oder Transfer individueller Daten beim SIM-Hersteller, Netzbetreiber oder einer dritten Partei.

Im Mobilfunknetz des Betreibers besteht eine spezielle Datenbank (THLR) der festen Größe N mit den S^*_i und jeweils einer fest zugeordneten Rufnummer MS/SDN^*_i . Die Teilnehmerverhältnisse in dieser Datenbank sind unveränderlich, insbesondere besteht keine Verbindung zum Chipkartenhersteller.

Eine zugehörige SIM wird nun in einem vollständig standardgemäßen (d.h. mit keinen besonderen Vorkehrungen hinsichtlich des hier beschriebenen Verfahrens ausgerüsteten) mobilen Endgerät zum ersten Mal in Betrieb genommen. Nach der ersten Inbetriebnahme mit S^*_i erfolgt die Übermittlung der endgültigen Teilnehmerdaten (S), die auf dem Teilnehmeridentifizierungsmodul SIM abgespeichert werden. Gleichzeitig werden diese endgültigen Teilnehmerdaten auch

im Heimatregister HLR abgelegt. Das Teilnehmeridentifizierungsmodul SIM ist dann mit den endgültigen Daten betriebsbereit.

Vorzugsweise erfolgt bei der ersten Inbetriebnahme der Aufbau einer Verbindung zu einem Personalisierungsserver (PS) innerhalb des Mobilfunknetzes, wobei seitens des Personalisierungsservers (PS) der individuelle und endgültige Teilnehmerdatensatz (S) für die Personalisierung generiert und an das SIM übermittelt wird, insbesondere unter Verwendung der nicht-individuellen und vorläufigen Teilnehmerdaten (S^*).

Vorzugsweise ist die vorläufige Teilnehmeridentifikation ($IMSI^*$) nicht eindeutig und kann mehreren Teilnehmeridentifizierungsmodulen (SIM) vorläufig zugeordnet werden. Hierdurch ist es möglich, die vorhandenen Ressourcen zu schonen, indem Parametersätze z.B. zyklisch wieder verwendet werden, wobei die SIM jedoch anhand einer eindeutigen Identifikation, wie beispielsweise der Seriennummer, identifizierbar und unterscheidbar bleiben können.

In einer bevorzugten Ausführungsform wird vor der Durchführung der Personalisierung eine Überprüfung der Seriennummer des SIM (ICCID) und/oder des Mobilfunkendgerätes anhand der Geräteidentitätsnummer (IMEI), über die das Mobilfunkendgerät eindeutig identifizierbar ist, und/oder eine Überprüfung anderer Sicherheitsparametern des SIM durchgeführt. Hierdurch kann die Sicherheit des Verfahrens erhöht werden.

Vorzugsweise ist die Anzahl der möglichen nicht-individuellen und vorläufigen Teilnehmerdatensätze (S^*), enthaltend zumindest eine nicht-individuelle und vorläufige Teilnehmeridentifikation ($IMSI^*$) und einen nicht-individuellen und vorläufigen Geheimschlüssel (K^*), festgelegt und insbesondere sehr viel kleiner als die Anzahl der insgesamt mit diesen Datensätzen (S^*) ausgerüsteten Teilnehmeridentifizierungsmodule (SIM), wobei es zu jedem Zeitpunkt viele Teilnehmeridentifizierungsmodule (SIM) mit identischen vorläufigen Daten (S^*) gibt.

Besonders bevorzugt werden die nicht-individuellen und vorläufigen Teilnehmerdatensätze (S^*), enthaltend zumindest eine nicht-individuelle und

vorläufige Teilnehmeridentifikation (IMSI*) und einen nicht-individuellen und vorläufigen Geheimschlüssel (K*), bei der initialen Ausrüstung der Teilnehmeridentifizierungsmodule (SIM) zyklisch wiederverwendet, insbesondere unabhängig davon, ob oder wie viele der SIM bereits mit individuellen und endgültigen Teilnehmerdaten (S) personalisiert wurden.

Hierdurch kann eine gleichmäßige Verteilung der vorläufigen, nicht-individuellen Teilnehmerdatensätze (S*) gewährleistet werden, sodass es nicht zu einer versehentlichen Häufung eines oder mehrerer dieser nicht-individuellen Teilnehmerdatensätze (S*) kommt. Hierdurch kann das Risiko einer Kollision durch zufällige gleichzeitige Nutzung desselben vorläufigen Teilnehmerdatensatzes bei zwei verschiedenen SIM-Karten, d.h. Teilnehmeridentifizierungsmodulen, vermindert werden.

Vorzugsweise wird nach erfolgtem Empfang und der Abspeicherung des endgültigen Teilnehmerdatensatz (S) auf dem SIM der Erhalt des Teilnehmerdatensatz (S) eine Bestätigung von dem Mobilfunkendgerät an das Mobilfunknetz übermittelt. Bevorzugt wird sodann ein Warmstart des Mobilfunkendgerätes unter Verwendung des neuen Teilnehmerdatensatzes (S) durchgeführt. Durch das Quittieren des korrekten Datenempfangs erhält das Mobilfunknetz eine Rückmeldung des SIM erfolgter Personalisierung sodass der Vorgang abgeschlossen werden kann.

Vorzugsweise wird der bei der Personalisierung generierte endgültige Teilnehmerdatensatz (S) im Heimatregister (HLR) gespeichert. Die Speicherung des Teilnehmerdatensatz (S) und der zugehörigen Teilnehmerdaten im Heimatregister (HLR) gestattet die Nutzung der Dienste des Mobilfunknetzes.

Das Teilnehmerverhältnis kann dabei zunächst mit spezifischen Dienstbeschränkungen versehen sein, die erst später, nach Feststellung der Kundendaten, Dienstwünsche, etc., entfernt werden.

Vorzugsweise wird bei der erstmaligen Inbetriebnahme mit dem Parametersatz (S*) das durch die (IMSI*) gegebene Teilnehmerverhältnis netzseitig auf einen Status „in Benutzung“ gesetzt, während dessen nur eine eingeschränkte Nutzung freigegeben

ist, insbesondere die Durchführung der Personalisierung, wobei nach erfolgter Personalisierung des SIM mit dem individuellen und endgültigen Teilnehmerdatensatz (S) das durch die (IMSI*) gegebene Teilnehmerverhältnis auf einen Status „freigegeben“ gesetzt wird, der die erneute Nutzung des durch (IMSI*) gegebenen Teilnehmerverhältnisses durch ein anderes Teilnehmeridentifizierungsmodul SIM gestattet.

Besonders bevorzugt erfolgt bei einem Inbetriebnahmeversuch eines oder mehrerer weiterer SIM mit einem identischen vorläufigen Parametersatz (S*) einer bereits in das Mobilfunknetz eingebuchten ersten SIM eine Einreihung in eine Warteschlange und eine Bearbeitung nach dem Zeitrang der Inbetriebnahmeversuche.

Vorzugsweise wird bei einem Inbetriebnahmeversuch eines oder mehrerer weiterer Teilnehmeridentifizierungsmodule (SIM) mit einer zu einer bereits in das Mobilfunknetz zur Personalisierung eingebuchten ersten Teilnehmeridentifizierungsmodul (SIM) identischen vorläufigen Teilnehmeridentifikation (IMSI*) eine eventuelle Blockade des Personalisierungsvorgangs (Ausbleiben der Personalisierungsdaten) vom Teilnehmeridentifizierungsmodul (SIM) erkannt und führt zur automatischen Wiederholung der Personalisierungsanfrage.

Vorzugsweise wird bei einem Inbetriebnahmeversuch eines oder mehrerer weiterer Teilnehmeridentifizierungsmodule (SIM) mit einer zu einer bereits in das Mobilfunknetz zur Personalisierung eingebuchten ersten Teilnehmeridentifizierungsmodul (SIM) identischen vorläufigen Teilnehmeridentifikation (IMSI*) eine eventuelle Fehlleitung der Personalisierungsdaten vom Teilnehmeridentifizierungsmodul (SIM) erkannt, die Daten werden verworfen und es erfolgt eine automatische Wiederholung der Personalisierungsanfrage.

Besonders bevorzugt erfolgt bei ausbleibender Bestätigung des Mobilfunkendgerätes an das Mobilfunknetz automatisch ein erneuter Versand der Personalisierungsdaten.

Vorzugsweise erfolgt erst nach Bestätigung des Mobilfunkendgerätes an das Mobilfunknetz die Speicherung des endgültigen Teilnehmerdatensatz (S) im Heimatregister (HLR).

Vorzugsweise erfolgt erst nach Bestätigung des Mobilfunkendgerätes an das Mobilfunknetz die Aktivierung und/oder Freischaltung des durch den endgültigen Teilnehmerdatensatz (S) im Heimatregister (HLR) gekennzeichneten Teilnehmerverhältnis (Subskription).

Besonders bevorzugt sind die endgültigen Teilnehmerdatensätze (S) im Heimatregister (HLR) bereits kurzfristig auf Vorrat angelegt. Hierdurch ist gewährleistet, dass eine Personalisierung von Teilnehmeridentifizierungsmodulen (SIM-Karten) jederzeit kurzfristig erfolgen kann.

Vorzugsweise sind die durch die endgültigen Teilnehmerdatensätze (S) im Heimatregister (HLR) gekennzeichneten Teilnehmerverhältnisse (Subskriptionen) bereits kurzfristig auf Vorrat angelegt.

Besonders bevorzugt sind die durch die endgültigen Teilnehmerdatensätze (S) im Heimatregister (HLR) gekennzeichneten Teilnehmerverhältnisse (Subskriptionen) mit spezifischen Dienstbeschränkungen versehen.

Vorzugsweise erfolgen im Anschluss an die erfolgte Personalisierung automatisch weitere Ladevorgänge zur Ausgestaltung der SIM-Karte mit besonderen Eigenschaften und/oder Diensten.

Vorzugsweise wird im Anschluss an die erfolgte Personalisierung automatisch ein maschineller oder persönlicher Dialog, vorzugsweise über das Mobilfunkendgerät, mit dem Kunden zur Ermittlung der Kundendaten, Dienstwünsche, etc. gestartet und insbesondere werden erst danach eventuelle spezifische Dienstbeschränkungen entfernt.

Ein Ausführungsbeispiel des erfindungsgemäßen Verfahrens ist in den Figuren dargestellt und wird nachfolgend erläutert. Es zeigen:

Fig. 1 ein Ausführungsbeispiel des erfindungsgemäßen Verfahrens der OTA-Personalisierung eines Teilnehmeridentifizierungsmoduls SIM;

Fig. 2 das Schema bei der gleichzeitigen Inbetriebnahme mehrerer SIM, insbesondere mit identischem vorläufigen Parametersatz.

Chipkarten (SIM) sind mit einem nicht-individuellen Satz initialer Identifizierungs- und Authentisierungsparameter

$$S^*_i = \{IMSI^*_i, K^*_i, OPc^*_i, Qc^*_i, OK^*_i\} \text{ mit } i = 0, 1, \dots, N-1 \text{ und } N \ll M;$$

ausgerüstet, wobei $IMSI^*_i$ die gültige Netzkennung MCC und MNC des Betreibers enthält. Mit N seien die Gesamtmenge der S^*_i und mit M die Menge der solcherart insgesamt für einen Netzbetreiber hergestellten SIM bezeichnet. Innerhalb von M wiederholen sich die S^*_i also M/N -mal und sind damit nicht-eindeutig und nicht-individuell.

Als einziges individuelles Merkmal kommt die übliche Seriennummer (ICCID) hinzu, die vom Hersteller während der Produktion fortlaufend zugeordnet wird. Wichtig ist, dass alle vom Hersteller im laufenden Produktionsprozess zuzuordnenden Daten vollautomatisch und ohne spezielle (individuelle) Vorgaben des Netzbetreibers vergeben werden.

Im Mobilfunknetz des Betreibers besteht eine spezielle Datenbank (THLR) der festen Größe N mit den S^*_i und jeweils einer fest zugeordneten Rufnummer $MSISDN^*_i$. Die Teilnehmerverhältnisse in der Datenbank sind unveränderlich, insbesondere besteht keine Verbindung zum Chipkartenhersteller.

Eine zugehörige SIM wird nun in einem vollständig standardgemäßen (d.h. mit keinen besonderen Vorkehrungen hinsichtlich des vorliegenden Vorschlags ausgerüsteten) mobilen Endgerät zum ersten Mal in Betrieb genommen. Unter Vereinfachung des sonstigen Systemvorgänge beim Einbuchen in ein Mobilfunknetz erfolgt die Personalisierung gemäß der Darstellung nach Fig. 1:

(1) Die $IMSI^*_i$ wird vom mobilen Endgerät gelesen und standardgemäß an das empfangene Mobilfunknetz, von diesem ggf. weiter an das Heimatnetz und darin an das THLR übertragen. Die dazu notwendige Routing-Information wird der $IMSI^*_i$ entnommen. Die $IMSI^*_i$ ist im THLR bekannt und es wird entsprechend des normalen Protokolls die Authentisierung zwischen Karte und THLR mit den Daten S^*_i veranlasst. Das Ergebnis ist positiv und das Teilnehmerverhältnis geht standardgemäß in den Zustand, in dem ein beiderseitiger Verbindungsaufbau möglich ist.

Als Sonderfunktion versieht das THLR die $IMSI^*_i$ zu einem frühestens möglichen Zeitpunkt mit dem Status "in Benutzung". Dieser Status bleibt bis zur Freigabe der $IMSI^*_i$, entweder durch ordentlichen Abschluss der nachfolgenden Personalisierung oder Eintritt eines Sonderfalls (siehe unten), bestehen.

(2) Netzseitig wird nun die OTA-Personalisierung gestartet, d.h. die Übermittlung der personalisierten Teilnehmerdaten über eine Funkverbindung, indem dem Personalisierungs-Server PS der Index i übergeben wird. Der PS kennt zum Index i die passende $MSISDN^*_i$ und den OTA-Schlüssel OK^*_i . Damit baut er nun eine sichere OTA-Session nach dem Stand der Technik zur betreffenden SIM auf.

Es kann nun zunächst z.B. die $ICCID$ der Karte oder *die IMEI* des Gerätes geprüft werden (beispielsweise mittels eines Black- oder White-Listing) und/oder weitere Sicherheitsparameter der Karte abgefragt werden (z.B. ein Zertifikat) bevor die eigentliche Personalisierung startet. Dazu werden endgültige Teilnehmerdaten

$$S = \{IMSI, K, OP_c, Q_c, OK\}$$

im PS generiert, über den bestehenden OTA-Kanal zur SIM gesendet und dort gespeichert - die Karte damit individuell personalisiert.

(3) Der Vorgang wird kartenseitig geeignet unterstützt und derart abgesichert, dass Verbindungsfehler oder ein nur teilweiser Empfang nicht zu einer unvollständigen (damit ungültigen) Personalisierung führen können. Erst nach komplettem und

korrektem Empfang und der Speicherung aller notwendigen Daten quittiert die SIM den Vorgang an den PS und veranlasst abschließend einen Warmstart (Full Refresh) des Endgerätes, nun mit den endgültigen Teilnehmerdaten S.

(4) Parallel zur Personalisierung der SIM veranlasst der PS die Einrichtung des Teilnehmerverhältnisses S im endgültigen HLR. Damit ist beidseitig ein Zustand erreicht wie nach der herkömmlichen Personalisierung und Einrichtung. Die SIM ist jetzt für den Standardbetrieb einsetzbar.

Vorzugsweise kann die Speicherung und Aktivierung der endgültigen Teilnehmerverhältnisse S im Heimatregister HLR erst nach Erhalt der Quittung der SIM an das Mobilfunknetz erfolgen und vorläufig mit spezifischen Dienstbeschränkungen versehen werden.

Zur Beschleunigung des Vorgangs können die endgültigen Teilnehmerverhältnisse S im HLR bereits kurzfristig auf Vorrat angelegt sein, beispielsweise indem der PS regelmäßig eine Anzahl der Teilnehmerverhältnisse S für den zeitnahen Bedarf (z.B. für die nächste Stunde oder den nächsten Tag) vorausblickend im HLR speichert und aktiviert.

(5) Die in (3) erhaltene Quittung der SIM führt im PS und THLR zur sofortigen Freigabe des Teilnehmerverhältnisses S_i^* , insbesondere der IMS/I_i^* . Sie wechselt aus dem Zustand "in Benutzung" in den Zustand "frei" und ist damit bereit zur nächsten Benutzung.

Tatsächlich ist wegen der Nicht-Eindeutigkeit der Parameterdatensätze S_i^* und der Zufälligkeit der Inbetriebnahmen, auch bei Gleichverteilung der S_i in der produzierten Gesamtmenge (die durch einfaches Hochzählen von i während der Produktion erreicht wird), mit Kollisionen bei der OTA-Personalisierung zu rechnen. Dies ist dann der Fall, wenn während der Bearbeitung des Teilnehmerverhältnisses S_i^* , d.h. wenn die IMS/I_i^* als "in Benutzung" gekennzeichnet ist, ein zweiter oder sogar weitere Einbuchversuche anderer SIM mit identische Parameterdatensatz S_i^* erfolgt. Dieser Fall ist in Fig. 3 dargestellt. Solche Kollisionen stellen jedoch einen regulären Betriebsfall dar, der wie folgt berücksichtigt wird:

- Nicht gleich bearbeitbare Einbuchversuche mit $IMSI_i^*$ werden in eine Warteschlange eingereiht und in der Reihenfolge des Eingangs abgearbeitet.
- Die Anzahl N der Parametersätze S_i^* ist so zu wählen, dass die Wahrscheinlichkeit einer Kollision (und erst recht einer Mehrfachkollision) hinreichend klein wird. Da nach wie vor $N \ll M$ gilt, bleiben die Vorteile des vorliegenden Vorschlags selbst bei $N = 1.000$ oder $N = 10.000$ vollständig erhalten.
- Die Geschwindigkeit der OTA Personalisierung ist durch optimierte Systeme so zu gestalten, dass der Zeitraum, in dem eine $IMSI_i^*$ in Benutzung ist, möglichst klein wird.
- Fehlerfälle während des Personalisierungszyklus, etwa bei Ausbleiben der Quittung der SIM, sind durch Time-Out zu begrenzen, so dass die $IMSI_i^*$ möglichst umgehend wieder frei gegeben wird.
- Eine eventuelle Blockade des Personalisierungsvorgangs (Ausbleiben der Personalisierungsdaten) wird vom SIM erkannt und führt zur automatischen Wiederholung der Personalisierungsanfrage.
- Eine eventuelle Fehlleitung der Personalisierungsdaten wird vom SIM erkannt, die Daten werden verworfen und es erfolgt eine automatische Wiederholung der Personalisierungsanfrage.
- Bei eventuell ausbleibender Quittung der SIM an das Mobilfunknetz kann automatisch ein erneuter Versand der Personalisierungsdaten erfolgen.

An den Personalisierungsprozess schließt sich automatisch ein Warmstart und Einbuchversuch mit den endgültigen Teilnehmerdaten an. Es können nun ohne Zeitdruck in einem neuen OTA-Prozess die weitere kartenseitige Konfiguration des Teilnehmerverhältnis vorgenommen werden.

Dies betrifft die weitere Ausgestaltung der SIM Karte mit besonderen Eigenschaften und Diensten, sowie die Ermittlung der Kundendaten und Dienstewünsche mittels persönlichen oder maschinellen Dialogs, vorzugsweise über das Mobilfunkendgerät. Ggf. zuvor vorhandene spezielle Dienstbeschränkungen werden abschließend entfernt.

Die Anwendung des vorgeschlagenen Konzeptes ist nicht auf den OTA-Kanal begrenzt (der jedoch für die Anwendung in Mobilfunknetzen am interessantesten sein dürfte), sondern auch in leitungsgebundenen Varianten denkbar. Etwa wenn die Personalisierung zwar dezentral, aber noch in den Verkaufspunkten (POS) des Netzbetreibers oder des Anbieters erfolgen soll. Über Internet und einem angeschlossenen Kartenleser ist dies sogar an jedem beliebigen Ort denkbar. Die Prinzipien, wie z.B. die Wiederverwendung der *IMSI*_{*i*}^{*}, gelten dabei unverändert, ebenso wie die gegenüber dem Stand der Technik zu erzielenden Vorteile.

Stichwortartig seien hier folgende vorteilhafte Ausgestaltungen angeführt:

- alle Systeme, z.B. GSM, UMTS, IMS, WLAN, WIMAX, LTE/SAE/EPS, NGMN, NGN, CDMA
- alle Chipkarten der Telekommunikation, z.B. UICC, SIM, USIM, ISIM, RUIM und zukünftige
- alle Formfaktoren, z.B. ID-1, ID-000, MiniUICC, M2M, IFF und zukünftige
- alle Ausführungsformen, z.B. removable, semi-removable, non-removable, soft
- alle OTA-Kanäle, z.B. SMS, BIP/CAT-TP, TCP/IP, auch RDM
- alle leitungsgebundenen Kanäle z.B. LAN, WAN, Internet
- alle Endgeräte, z.B. mobile oder feste Telefone, PCs und Notebook PCs, Datenmodule
- alle dezentralen Kartenleser z.B. am POS
- alle Umfänge, z.B. von (IMSI, K) bis kompl. Perso/Individualisierung und Software-Download
- mit zusätzlicher Absicherung durch PKI-Verfahren, Zertifikate und/oder Personalisierungskennwort

- mit Ableitung bestimmter Parameter
- mit Bewertung der IMEI (gerätespezifische Personalisierung)
- mit Bewertung der ICCID (kartenspezifische Personalisierung)
- als Dienstleistung durch 3. Partei
- als initiale Personalisierung oder Repersonalisierung, auch mit Netzbetreiberwechsel
- integriert in On-Line Dialog inkl. Vertragsabschluß und Aktivierung

Übersicht bzw. Übersetzungen der verwendeten Begriffe und deren international übliche Benennung und Abkürzung:

- Teilnehmeridentifizierungsmodul (Subscriber Identity Modul, SIM)
- Teilnehmeridentifikation (International Mobile Subscriber Identity, IMSI)
- Geräteidentitätsnummer (International Mobile Equipment Identity, IMEI)
- Mobilfunknummer (Mobile Subscriber Integrated Services Digital Network Number, MSISDN)
- Seriennummer des SIM (ICCID)
- Funkverbindung zur SIM (Over The Air, OTA)
- Heimatregister bzw. temporäres Heimatregister (Home Location Register, HLR bzw. THLR)
- Maschine-Maschine Kommunikation (Machine to Machine, M2M)
- Read – Lesen
- Check – Prüfung, Überprüfung, prüfen
- Network – Netzwerk
- Attach, Attached – Anfügen, Angefügt
- Hold and buffer – zwischenspeichern
- Authenticate, Authentication – Authentifizieren, Authentifizierung
- Auth. – Abkürzung für Authenticate, Authentication
- Bad – mangelhaft
- Failure – Fehler
- Send – Senden, übermitteln
- Update – Aktualisierung
- Generate – Generieren
- Session – Sitzung

- Secured – abgesichert
- Release – Ausgabe, ausgeben
- Personalisation – Personalisierung
- Perso Cycle – Personalisierungsprozess
- Install – Installieren
- Target – Ziel, Zielbereich
- Confirmation – Bestätigung
- Full refresh – vollständige Aktualisierung, vollständig aktualisieren
- Ack – Abkürzung für Acknowledgement – Rückmeldung
- Timeout – Zeitüberschreitung

Ansprüche

1. Verfahren zur Inbetriebnahme und Personalisierung eines Teilnehmeridentifizierungsmoduls SIM, dadurch gekennzeichnet, dass das SIM vor der ersten Inbetriebnahme mit einem nicht-individuellen und vorläufigen Satz (S^*) initialer Identifizierungs- und Authentisierungsparameter ausgerüstet wird, enthaltend zumindest eine nicht-individuelle und vorläufige Teilnehmeridentifikation ($IMSI^*$) und einen Geheimschlüssel (K^*), wobei der Parametersatz (S^*) eine erste Inbetriebnahme des SIM in einem Mobilfunknetz mittels eines Mobilfunkendgerätes gestattet, wobei nach der ersten Inbetriebnahme des SIM eine Personalisierung durchgeführt wird, indem ein individueller und endgültiger Teilnehmerdatensatz (S) übertragen und auf dem SIM gespeichert wird, insbesondere enthaltend eine eindeutige endgültige Teilnehmeridentifikation ($IMSI$) und einen Geheimschlüssel (K), insbesondere dass der endgültige Teilnehmerdatensatz (S) über eine reguläre Verbindung des Mobilfunksystems unter Verwendung des vorläufigen Satzes (S^*) übertragen wird.
2. Verfahren nach Anspruch 1, dadurch gekennzeichnet, dass bei der ersten Inbetriebnahme der Aufbau einer Verbindung zu einem Personalisierungsserver (PS) innerhalb des Mobilfunknetzes erfolgt, wobei seitens des Personalisierungsservers (PS) der individuelle und endgültige Teilnehmerdatensatz (S) für die Personalisierung generiert und an das SIM übermittelt wird, insbesondere unter Verwendung der nicht-individuellen und vorläufigen Teilnehmerdaten (S^*).

3. Verfahren nach Anspruch 1 oder 2, dadurch gekennzeichnet, dass vor der Durchführung der Personalisierung eine Überprüfung der Seriennummer des SIM (ICCID) und/oder der Geräteidentitätsnummer (IMEI), über die das Mobilfunkendgerät eindeutig identifizierbar ist, und/oder eine Überprüfung von weiteren Sicherheitsparametern des SIM durchgeführt wird.
4. Verfahren nach einem der vorherigen Ansprüche, dadurch gekennzeichnet, dass die vorläufige Teilnehmeridentifikation (IMSI*) nicht eindeutig ist und mehreren Teilnehmeridentifizierungsmodulen (SIM) gleichzeitig vorläufig zugeordnet wird.
5. Verfahren nach einem der vorherigen Ansprüche, dadurch gekennzeichnet, dass die Anzahl der möglichen nicht-individuellen und vorläufigen Teilnehmerdatensätze (S*), enthaltend zumindest eine nicht-individuelle und vorläufige Teilnehmeridentifikation (IMSI*) und einen nicht-individuellen und vorläufigen Geheimschlüssel (K*), festgelegt ist und insbesondere sehr viel kleiner ist als die Anzahl der insgesamt mit diesen Datensätzen (S*) ausgerüsteten Teilnehmeridentifizierungsmodule (SIM).
6. Verfahren nach einem der vorherigen Ansprüche, dadurch gekennzeichnet, dass die nicht-individuellen und vorläufigen Teilnehmerdatensätze (S*), enthaltend zumindest eine nicht-individuelle und vorläufige Teilnehmeridentifikation (IMSI*) und einen nicht-individuellen und vorläufigen Geheimschlüssel (K*), bei der initialen Ausrüstung der Teilnehmeridentifizierungsmodule (SIM) zyklisch wiederverwendet werden, insbesondere unabhängig davon, ob oder wie viele der SIM bereits mit individuellen und endgültigen Teilnehmerdaten (S) personalisiert wurden.
7. Verfahren nach einem der vorherigen Ansprüche, dadurch gekennzeichnet, dass im Rahmen der Produktion der Teilnehmeridentifizierungsmodule (SIM) keine Weitergabe oder Speicherung von zugeordneten Daten erfolgen muss.

8. Verfahren nach einem der vorherigen Ansprüche, dadurch gekennzeichnet, dass der bei der Personalisierung generierte Teilnehmerdatensatz (S) und die zugehörigen Teilnehmerdaten erst bei der ersten Inbetriebnahme des SIM im Heimatregister (HLR) gespeichert wird.
9. Verfahren nach einem der vorherigen Ansprüche, dadurch gekennzeichnet, dass nach erfolgtem Empfang und der Abspeicherung des individuellen und endgültigen Teilnehmerdatensatz (S) auf dem SIM eine Bestätigung von dem Mobilfunkendgerät an das Mobilfunknetz übermittelt wird, insbesondere dass ein Warmstart des Mobilfunkendgerätes unter Verwendung des Teilnehmerdatensatzes (S) durchgeführt wird.
10. Verfahren nach einem der vorherigen Ansprüche, dadurch gekennzeichnet, dass bei der erstmaligen Inbetriebnahme mit dem nicht-individuellen und vorläufigen Parametersatz (S*) das durch die (IMSI*) gegebene Teilnehmerverhältnis netzseitig auf einen Status „in Benutzung“ gesetzt wird, während dessen nur eine eingeschränkte Nutzung freigegeben ist, und dass nach erfolgter Personalisierung des SIM mit dem individuellen und endgültigen Teilnehmerdatensatz (S) das durch die (IMSI*) gegebene Teilnehmerverhältnis auf einen Status „freigegeben“ gesetzt wird, der die erneute Nutzung des durch (IMSI*) gegebenen Teilnehmerverhältnisses durch ein anderes Teilnehmeridentifizierungsmodul SIM gestattet.
11. Verfahren nach einem der vorherigen Ansprüche, dadurch gekennzeichnet, dass bei einem Inbetriebnahmeversuch eines oder mehrerer weiterer SIM mit einer zu einer bereits in das Mobilfunknetz zur Personalisierung eingebuchten ersten SIM identischen vorläufigen Teilnehmeridentifikation (IMSI*) eine Einreihung in eine Warteschlange und eine Bearbeitung nach dem Zeitrang der Inbetriebnahmeversuche erfolgt.
12. Verfahren nach einem der vorherigen Ansprüche, dadurch gekennzeichnet, dass bei einem Inbetriebnahmeversuch eines oder mehrerer weiterer Teilnehmeridentifizierungsmodule (SIM) mit einer zu einer bereits in das Mobilfunknetz zur Personalisierung eingebuchten ersten

Teilnehmeridentifizierungsmodul (SIM) identischen vorläufigen Teilnehmeridentifikation (IMSI*) eine eventuelle Blockade des Personalisierungsvorgangs (Ausbleiben der Personalisierungsdaten) vom Teilnehmeridentifizierungsmodul (SIM) erkannt wird und zur automatischen Wiederholung der Personalisierungsanfrage führt.

13. Verfahren nach einem der vorherigen Ansprüche, dadurch gekennzeichnet, dass bei einem Inbetriebnahmeversuch eines oder mehrerer weiterer Teilnehmeridentifizierungsmodule (SIM) mit einer zu einer bereits in das Mobilfunknetz zur Personalisierung eingebuchten ersten Teilnehmeridentifizierungsmodul (SIM) identischen vorläufigen Teilnehmeridentifikation (IMSI*) eine eventuelle Fehlleitung der Personalisierungsdaten vom Teilnehmeridentifizierungsmodul (SIM) erkannt wird, die Daten verworfen werden und eine automatische Wiederholung der Personalisierungsanfrage erfolgt.
14. Verfahren nach einem der vorherigen Ansprüche, dadurch gekennzeichnet, dass bei ausbleibender Bestätigung des Mobilfunkendgerätes an das Mobilfunknetz automatisch ein erneuter Versand der Personalisierungsdaten erfolgt.
15. Verfahren nach einem der vorherigen Ansprüche, dadurch gekennzeichnet, dass erst nach Bestätigung des Mobilfunkendgerätes an das Mobilfunknetz die Speicherung des endgültigen Teilnehmerdatensatz (S) im Heimatregister (HLR) erfolgt.
16. Verfahren nach einem der vorherigen Ansprüche, dadurch gekennzeichnet, dass erst nach Bestätigung des Mobilfunkendgerätes an das Mobilfunknetz die Aktivierung und/oder Freischaltung des durch den endgültigen Teilnehmerdatensatz (S) im Heimatregister (HLR) gekennzeichneten Teilnehmerverhältnis (Subskription) erfolgt.

17. Verfahren nach einem der vorherigen Ansprüche, dadurch gekennzeichnet, dass die endgültigen Teilnehmerdatensätze (S) im Heimatregister (HLR) bereits kurzfristig auf Vorrat angelegt sind.
18. Verfahren nach einem der vorherigen Ansprüche, dadurch gekennzeichnet, dass die durch die endgültigen Teilnehmerdatensätze (S) im Heimatregister (HLR) gekennzeichneten Teilnehmerverhältnisse (Subskriptionen) bereits kurzfristig auf Vorrat angelegt sind.
19. Verfahren nach einem der vorherigen Ansprüche, dadurch gekennzeichnet, dass die durch die endgültigen Teilnehmerdatensätze (S) im Heimatregister (HLR) gekennzeichneten Teilnehmerverhältnisse (Subskriptionen) mit spezifischen Dienstbeschränkungen versehen sind.
20. Verfahren nach einem der vorherigen Ansprüche, dadurch gekennzeichnet, dass im Anschluss an die erfolgte Personalisierung automatisch weitere Ladevorgänge zur Ausgestaltung der SIM-Karte mit besonderen Eigenschaften und/oder Diensten erfolgen.
21. Verfahren nach einem der vorherigen Ansprüche, dadurch gekennzeichnet, dass im Anschluss an die erfolgte Personalisierung automatisch ein maschineller oder persönlicher Dialog, vorzugsweise über das Mobilfunkendgerät, mit dem Kunden zur Ermittlung der Kundendaten und/oder Dienstwünsche, etc. gestartet wird und insbesondere erst danach eventuelle spezifische Dienstbeschränkungen entfernt werden.

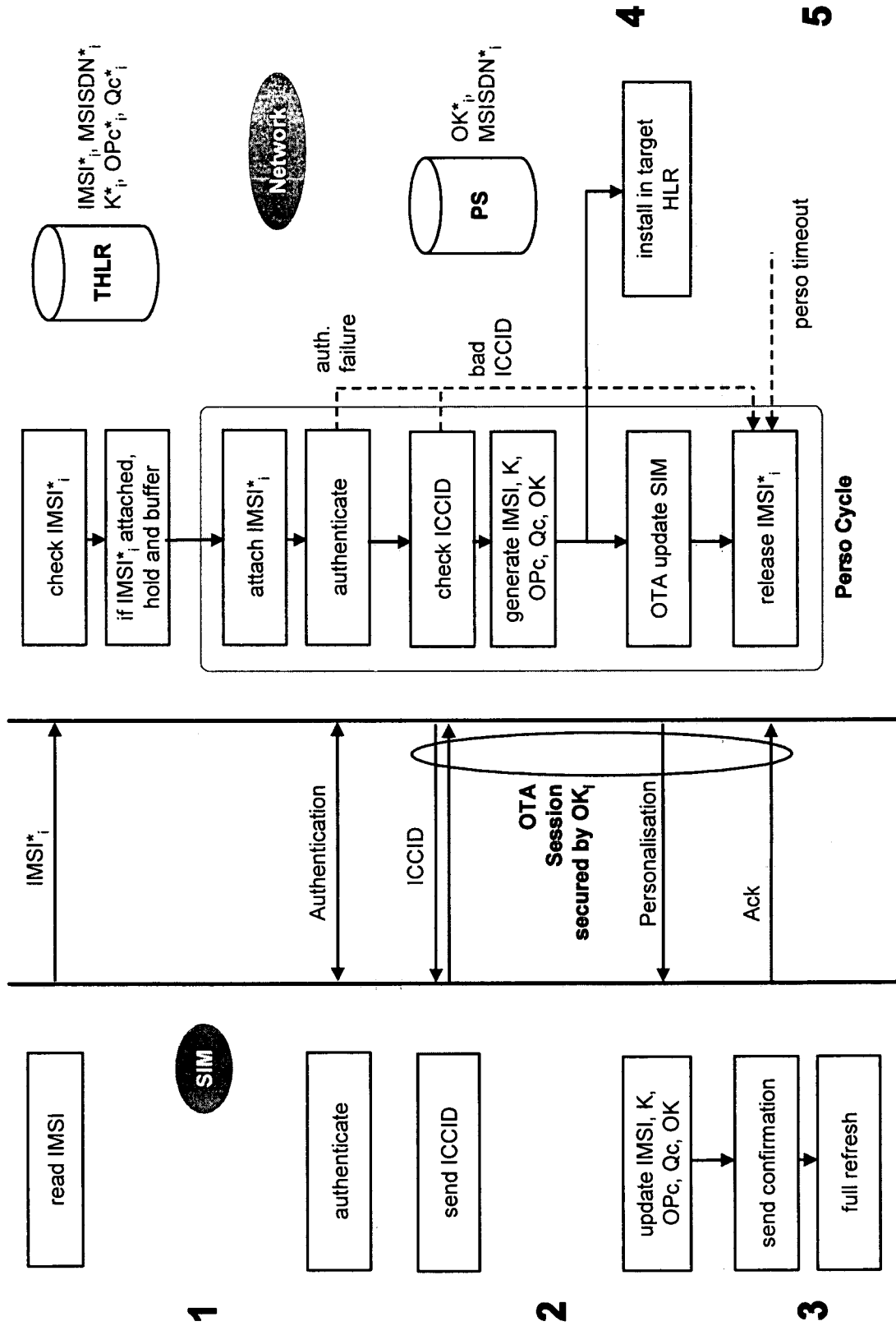


Fig. 1

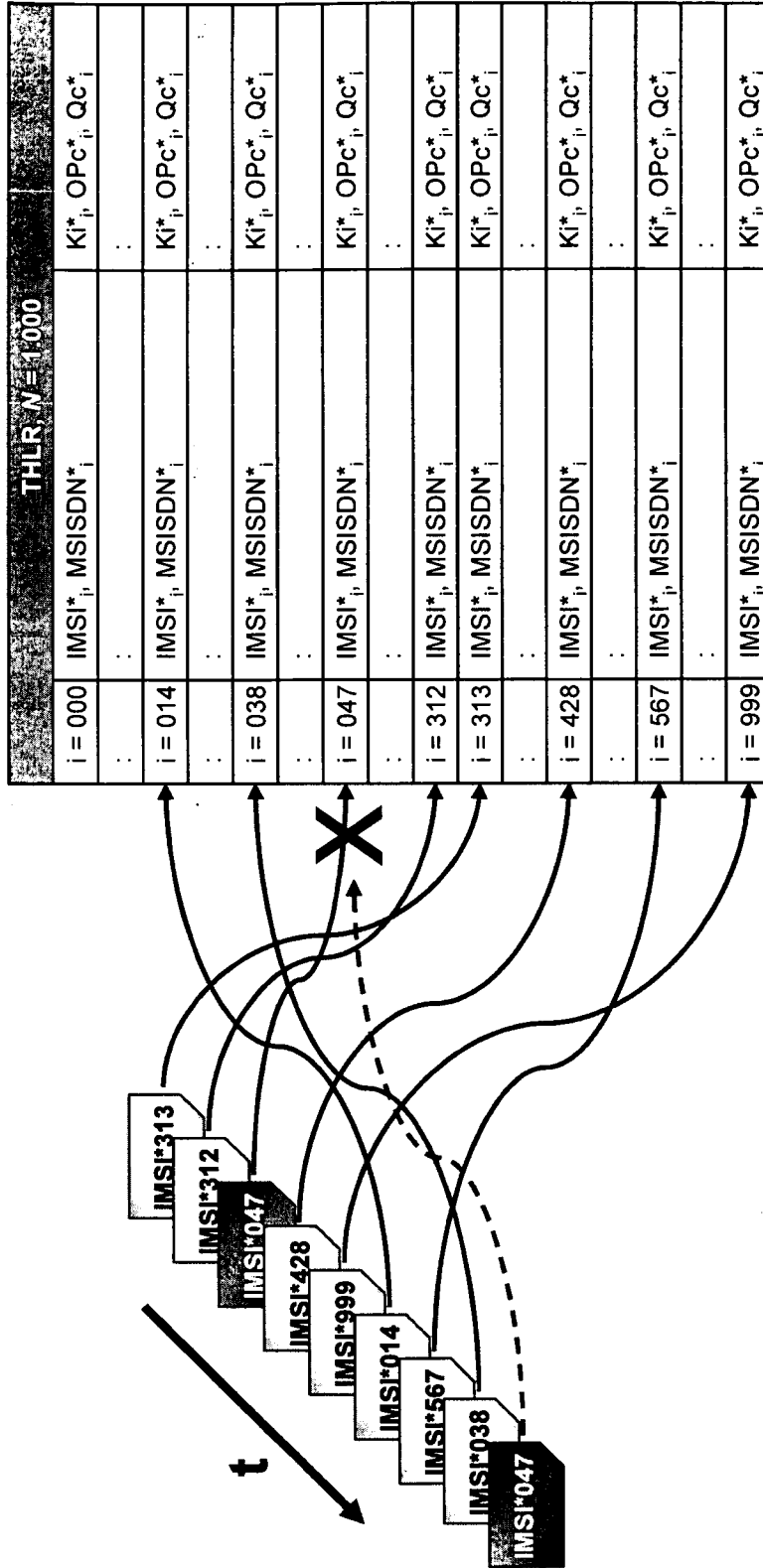


Fig. 2

INTERNATIONAL SEARCH REPORT

International application No
PCT/EP2009/002827A. CLASSIFICATION OF SUBJECT MATTER
INV. H04W8/26

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)
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 practical, search terms used)

EPO-Internal

C. DOCUMENTS CONSIDERED TO BE RELEVANT

Category*	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
X	US 7 266 371 B1 (AMIN UMESH J [US] ET AL) 4 September 2007 (2007-09-04) abstract column 1, line 21 - column 5, line 23 column 6, line 28 - column 15, line 33; claims 17,19,34; figure 4	1-21
X	WO 03/077585 A (SCHLUMBERGER SYSTEMS & SERVICE [FR]; SCHLUMBERGER MALCO INC [US]; CHOI) 18 September 2003 (2003-09-18) abstract page 2, line 1 - line 18 page 3, line 23 - page 12, line 11	1-21
	----- -/--	

 Further documents are listed in the continuation of Box C. 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 document 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

25 Juni 2009

Date of mailing of the international search report

07/07/2009

Name and mailing address of the ISA/

European Patent Office, P.B. 5818 Patentlaan 2
NL - 2280 HV Rijswijk
Tel. (+31-70) 340-2040.
Fax: (+31-70) 340-3016

Authorized officer

Sidoti, Filippo

INTERNATIONAL SEARCH REPORT

International application No
PCT/EP2009/002827

C(Continuation). DOCUMENTS CONSIDERED TO BE RELEVANT

Category*	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
X	WO 02/058361 A (AT & T WIRELESS SERVICES INC [US]; SHIEH HUGH [US]; WONG GREG A [US]) 25 July 2002 (2002-07-25) abstract page 1, line 6 - page 5, line 8 page 5, line 28 - page 11, line 5 -----	1-21
X	EP 1 895 791 A (VODAFONE HOLDING GMBH [DE]) 5 March 2008 (2008-03-05) abstract paragraphs [0001] - [0038], [0040] - [0060] -----	1-21

INTERNATIONAL SEARCH REPORT

Information on patent family members

International application No
PCT/EP2009/002827

Patent document cited in search report	Publication date	Patent family member(s)	Publication date
US 7266371	B1	04-09-2007	NONE
<hr style="border-top: 1px dashed black;"/>			
WO 03077585	A	18-09-2003	AT 361644 T 15-05-2007
		AU 2003215790 A1	22-09-2003
		CN 1444414 A	24-09-2003
		DE 60313589 T2	31-01-2008
		EP 1483935 A1	08-12-2004
		ES 2287498 T3	16-12-2007
		JP 2005520422 T	07-07-2005
		US 2006183500 A1	17-08-2006
<hr style="border-top: 1px dashed black;"/>			
WO 02058361	A	25-07-2002	AU 2002246615 A1 30-07-2002
		BR 0105120 A	25-06-2002
		CA 2358175 A1	07-05-2002
		EP 1340362 A2	03-09-2003
		JP 2004518356 T	17-06-2004
		JP 2008086046 A	10-04-2008
		MX PA01011175 A	21-05-2004
		US 2008171532 A1	17-07-2008
		US 6591098 B1	08-07-2003
<hr style="border-top: 1px dashed black;"/>			
EP 1895791	A	05-03-2008	DE 102006040086 A1 20-03-2008
<hr style="border-top: 1px dashed black;"/>			

A. KLASSIFIZIERUNG DES ANMELDUNGSGEGENSTANDES
INV. H04W8/26

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

B. RECHERCHIERTE GEBIETE

Recherchierter Mindestprüfstoff (Klassifikationssystem und Klassifikationssymbole)
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

C. ALS WESENTLICH ANGESEHENE UNTERLAGEN

Kategorie*	Bezeichnung der Veröffentlichung, soweit erforderlich unter Angabe der in Betracht kommenden Teile	Betr. Anspruch Nr.
X	US 7 266 371 B1 (AMIN UMESH J [US] ET AL) 4. September 2007 (2007-09-04) Zusammenfassung Spalte 1, Zeile 21 - Spalte 5, Zeile 23 Spalte 6, Zeile 28 - Spalte 15, Zeile 33; Ansprüche 17,19,34; Abbildung 4	1-21
X	WO 03/077585 A (SCHLUMBERGER SYSTEMS & SERVICE [FR]; SCHLUMBERGER MALCO INC [US]; CHOI) 18. September 2003 (2003-09-18) Zusammenfassung Seite 2, Zeile 1 - Zeile 18 Seite 3, Zeile 23 - Seite 12, Zeile 11 -/--	1-21

Weitere Veröffentlichungen sind der Fortsetzung von Feld C zu entnehmen 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* älteres Dokument, 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 anderen Veröffentlichungen dieser Kategorie in Verbindung gebracht wird und diese Verbindung für einen Fachmann naheliegend ist
- *Z* Veröffentlichung, die Mitglied derselben Patentfamilie ist

Datum des Abschlusses der internationalen Recherche

25. Juni 2009

Absendedatum des internationalen Recherchenberichts

07/07/2009

Name und Postanschrift der internationalen Recherchenbehörde

Europäisches Patentamt, P.B. 5818 Patentlaan 2
NL - 2280 HV Rijswijk
Tel. (+31-70) 340-2040.
Fax: (+31-70) 340-3016

Bevollmächtigter Bediensteter

Sidoti, Filippo

C. (Fortsetzung) ALS WESENTLICH ANGESEHENE UNTERLAGEN

Kategorie*	Bezeichnung der Veröffentlichung, soweit erforderlich unter Angabe der in Betracht kommenden Teile	Belr. Anspruch Nr.
X	WO 02/058361 A (AT & T WIRELESS SERVICES INC [US]; SHIEH HUGH [US]; WONG GREG A [US]) 25. Juli 2002 (2002-07-25) Zusammenfassung Seite 1, Zeile 6 - Seite 5, Zeile 8 Seite 5, Zeile 28 - Seite 11, Zeile 5 -----	1-21
X	EP 1 895 791 A (VODAFONE HOLDING GMBH [DE]) 5. März 2008 (2008-03-05) Zusammenfassung Absätze [0001] - [0038], [0040] - [0060] -----	1-21

INTERNATIONALER RECHERCHENBERICHT

Angaben zu Veröffentlichungen, die zur selben Patentfamilie gehören

Internationales Aktenzeichen

PCT/EP2009/002827

im Recherchenbericht angeführtes Patentdokument		Datum der Veröffentlichung	Mitglied(er) der Patentfamilie	Datum der Veröffentlichung
US 7266371	B1	04-09-2007	KEINE	
<hr/>				
WO 03077585	A	18-09-2003	AT 361644 T	15-05-2007
			AU 2003215790 A1	22-09-2003
			CN 1444414 A	24-09-2003
			DE 60313589 T2	31-01-2008
			EP 1483935 A1	08-12-2004
			ES 2287498 T3	16-12-2007
			JP 2005520422 T	07-07-2005
			US 2006183500 A1	17-08-2006
<hr/>				
WO 02058361	A	25-07-2002	AU 2002246615 A1	30-07-2002
			BR 0105120 A	25-06-2002
			CA 2358175 A1	07-05-2002
			EP 1340362 A2	03-09-2003
			JP 2004518356 T	17-06-2004
			JP 2008086046 A	10-04-2008
			MX PA01011175 A	21-05-2004
			US 2008171532 A1	17-07-2008
			US 6591098 B1	08-07-2003
<hr/>				
EP 1895791	A	05-03-2008	DE 102006040086 A1	20-03-2008
<hr/>				