(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
21. Dezember 2000 (21.12.2000)

PCT

(10) Internationale Veröffentlichungsnummer
WO 00/78078 A1

(51) Internationale Patentklassifikation[7]: H04Q 7/38

(21) Internationales Aktenzeichen: PCT/DE00/01788

(22) Internationales Anmeldedatum:
31. Mai 2000 (31.05.2000)

(25) Einreichungssprache: Deutsch

(26) Veröffentlichungssprache: Deutsch

(30) Angaben zur Priorität:
199 27 271.9 15. Juni 1999 (15.06.1999) DE

(71) Anmelder *(für alle Bestimmungsstaaten mit Ausnahme von US)*: **SIEMENS AKTIENGESELLSCHAFT** [DE/DE]; Wittelsbacherplatz 2, D-80333 München (DE).

(72) Erfinder; und

(75) Erfinder/Anmelder *(nur für US)*: **HORN, Günther** [DE/DE]; Eduard-Schmid-Str. 16, D-81541 München (DE). **CUELLAR, Jorge** [DE/DE]; Höllriegelskreuther Weg, D-82065 Baierbrunn (DE).

(74) Gemeinsamer Vertreter: **SIEMENS AKTIENGESELLSCHAFT**; Wittelsbacherplatz 2, D-80333 München (DE).

(81) Bestimmungsstaaten *(national)*: AU, BR, CN, IN, JP, KR, US.

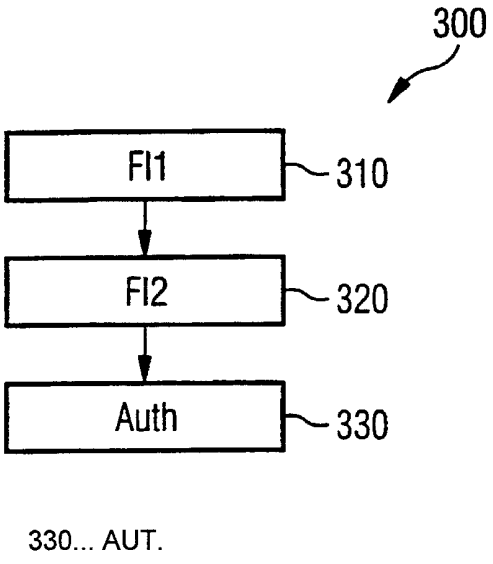
(84) Bestimmungsstaaten *(regional)*: europäisches Patent (AT, BE, CH, CY, DE, DK, ES, FI, FR, GB, GR, IE, IT, LU, MC, NL, PT, SE).

Veröffentlicht:
— *Mit internationalem Recherchenbericht.*
— *Vor Ablauf der für Änderungen der Ansprüche geltenden Frist; Veröffentlichung wird wiederholt, falls Änderungen eintreffen.*

[Fortsetzung auf der nächsten Seite]

(54) Title: METHOD AND SYSTEM FOR VERIFYING THE AUTHENTICITY OF A FIRST COMMUNICATION PARTICIPANTS IN A COMMUNICATIONS NETWORK

(54) Bezeichnung: VERFAHREN UND ANORDNUNG ZUR ÜBERPRÜFUNG EINER AUTHENTIZITÄT EINES ERSTEN KOMMUNIKATIONSTEILNEHMERS IN EINEM KOMMUNIKATIONSNETZ



330... AUT.

(57) **Abstract:** The invention relates to a method and a system for verifying the authenticity of a first communications participant in a communications network. According to the invention, a first error information is generated at the level of the first communications participant using an error-detection indication of said first communications participant and information on a random indication. A second error information is generated at the level of a second communications participant in the communications network using an error detection indication of the second communications participant and the information on the random indication. The authenticity of the first communications participant is verified using the first error information and second error information.

(57) **Zusammenfassung:** Bei dem Verfahren und der Anordnung zur Überprüfung einer Authentizität eines ersten Kommunikationsteilnehmers in einem Kommunikationsnetz wird bei dem ersten Kommunikationsteilnehmer unter Verwendung einer Fehlererkennungsangabe des ersten Kommunikationsteilnehmers und einer Information über eine Zufallsangabe eine erste Fehlerinformation gebildet. Bei einem zweiten Kommunikationsteilnehmer in dem Kommunikationsnetz wird unter Verwendung einer Fehlererkennungsangabe des zweiten Kommunikationsteilnehmers und der Information über die Zufallsangabe eine zweite Fehlerinformation gebildet. Unter Verwendung der ersten Fehlerinformation und der zweiten Fehlerinformation wird die Authentizität des ersten Kommunikationsteilnehmers überprüft.

WO 00/78078 A1

Zur Erklärung der Zweibuchstaben-Codes, und der anderen Abkürzungen wird auf die Erklärungen ("Guidance Notes on Codes and Abbreviations") am Anfang jeder regulären Ausgabe der PCT-Gazette verwiesen.

Beschreibung

Verfahren und Anordnung zur Überprüfung einer Authentizität eines ersten Kommunikationsteilnehmers in einem Kommunikationsnetz

Die Erfindung betrifft ein Verfahren und eine Anordnung zur Überprüfung einer Authentizität eines ersten Kommunikationsteilnehmers in einem Kommunikationsnetz.

In einem Kommunikationsnetz werden im allgemeinen Daten zwischen Kommunikationsteilnehmern, beispielsweise einem Dienstanbieter und einem Dienstnutzer, übertragen. Um ein Kommunikationsnetz vor einem Eindringen eines nichtberechtigten Kommunikationsteilnehmers in das Kommunikationsnetz zu schützen, wird in der Regel die Authentizität eines jeden Kommunikationsteilnehmers überprüft.

Aus Dokument [1] ist ein Verfahren und eine Anordnung zur Überprüfung einer Authentizität eines Kommunikationsteilnehmers, insbesondere eines Dienstanbieters oder eines Dienstnutzers, in einem Kommunikationsnetz bekannt.

Das aus dem Dokument [1] bekannte Verfahren und die entsprechende Anordnung basieren auf einem sogenannten 3G TS 33.102 Version 3.0.0-Draft-Standard, welcher eine Sicherheits-Architektur eines Mobilfunksystems beschreibt.

In **Fig.4** ist die Vorgehensweise bei einer Überprüfung einer Authentizität eines Kommunikationsteilnehmers, wie sie aus dem Dokument [1] bekannt ist, symbolhaft dargestellt und wird im folgenden kurz und auszugsweise erläutert.

Eine Übertragung von Daten ist in **Fig.4** jeweils durch einen Pfeil dargestellt. Eine Richtung eines Pfeils kennzeichnet eine Übertragungsrichtung bei einer Datenübertragung.

Fig.4 zeigt ein Mobilfunksystem 400, umfassend einen Nutzer 401 einer Kommunikationsdienstleistung, beispielsweise ein Mobiltelefon, und einen Anbieter 402 einer Kommunikationsdienstleistung. Der Anbieter 402 umfaßt ein Einwählnetz 403 mit einem Einwählnetzbetreiber, bei dem der Nutzer 401 lokal eine Kommunikationsdienstleistung anfordert, und ein Heimatnetz 404 mit einem Heimatnetzbetreiber, bei dem der Nutzer 401 angemeldet und registriert ist.

Ferner weisen der Nutzer 401, das Einwählnetz 403 und das Heimatnetz 404 jeweils eine zentrale Verarbeitungseinheit mit einem Speicher auf, beispielsweise einen Server (Zentralrechner), mit welcher Verarbeitungseinheit die im folgenden beschriebene Vorgehensweise überwacht und gesteuert wird und auf welchem Speicher Daten gespeichert werden und/oder sind.

Das Einwählnetz 403 und das Heimatnetz 404 sind über eine Datenleitung, über welche digitale Daten übertragen werden können, miteinander verbunden. Der Nutzer 401 und das Einwählnetz 403 sind über ein beliebiges Übertragungsmedium zur Übertragung von digitalen Daten miteinander verbunden.

Bei einer Kommunikation wählt sich der Nutzer 401 in das Einwählnetz 403 ein 410. Zu Beginn der Kommunikation erfolgt eine Überprüfung sowohl der Authentizität des Nutzers 401 als auch der Authentizität des Anbieters 402.

Dazu fordert das Einwählnetz 403 sogenannte Authentifikationsdaten, mit welchen die Überprüfung der Authentizität des Nutzers 401 und des Anbieters 402 möglich ist, von dem Heimatnetz 404 an 411.

Die Authentifikationsdaten, welche von dem Heimatnetz 404 ermittelt werden, umfassen eine Zufallszahl und eine Sequenzfolgenummer des Anbieters 402. Die Sequenzfolgennummer des Anbieters 402 wird derart ermittelt, daß ein Zähler des Anbieters 402 bei jedem Kommunikationsversuch zwischen dem Nut-

zer 401 und dem Anbieter 402 die Sequenzfolgenummer des Anbieters 402 um den Wert 1 erhöht.

Es ist anzumerken, daß die Zufallszahl und die Sequenzfolgenummer des Anbieters 402 nur einen Teil der Authentifikationsdaten darstellen und nicht abschließend zu verstehen sind. Weitere Authentifikationsdaten sind aus [1] bekannt.

Das Heimatnetz 404 überträgt die angeforderten Authentifikationsdaten an das Einwählnetz 403 412. Das Einwählnetz 403 bearbeitet die empfangenen Authentifikationsdaten in geeigneter Weise 413 und überträgt die bearbeiteten Authentifikationsdaten an den Nutzer 401 414.

Der Nutzer 401 überprüft unter Verwendung einer eigenen Sequenzfolgenummer, welche entsprechend der Sequenzfolgenummer des Anbieters 402 gehandhabt wird, und der Sequenzfolgenummer des Anbieters 402 die Authentizität des Anbieters 402 415.

Die Vorgehensweise bei der Überprüfung der Authentizität des Anbieters 402 ist in [1] beschrieben.

Ein Ergebnis der Überprüfung der Authentizität des Anbieters 402, "Authentizität des Anbieters in Ordnung" 416, "Authentizität des Anbieters in Ordnung, aber ein Sequenzfehler aufgetreten" 417 oder "Authentizität des Anbieters nicht in Ordnung" 418, wird von dem Nutzer 401 an den Anbieter 402 übertragen 419.

Bei dem Ergebnis "Authentizität des Anbieters in Ordnung" 416 überprüft das Einwählnetz 403, wie es in [1] beschrieben ist, die Authentizität des Nutzers 401 420.

Bei dem Ergebnis "Authentizität des Anbieters nicht in Ordnung" 418 wird die Kommunikation unterbrochen bzw. neu begonnen 421.

Bei dem Ergebnis "Authentizität des Anbieters in Ordnung, aber ein Sequenzfehler aufgetreten" 417 erfolgt eine Resynchronisation derart, daß das Heimatnetz 404 eine Resynchronisationsanfrage an den Nutzer 401 sendet 422. Der Nutzer antwortet mit einer Resynchronisationsantwort, bei welcher Resynchronisationsdaten an das Heimatnetz 404 übertragen werden 423. In Abhängigkeit der Resynchronisationsantwort wird die Sequenzfolgenummer des Anbieters 402 verändert 424. Anschließend erfolgt die Prüfung der Authentizität des Nutzers 401, wie es aus [1] bekannt ist.

Die beschriebene Vorgehensweise weist den Nachteil auf, daß bei einer Überprüfung einer Authentizität eines Kommunikationsteilnehmers, insbesondere bei der Überprüfung der Authentizität eines Dienstanbieters, viele Daten zwischen den Kommunikationsteilnehmern übertragen werden müssen.

Somit liegt der Erfindung das Problem zugrunde, ein gegenüber dem bekannten Verfahren und der bekannten Anordnung vereinfachtes und verbessertes Verfahren sowie eine vereinfachte und verbesserte Anordnung zur Überprüfung einer Authentizität eines Kommunikationsteilnehmers in einem Kommunikationsnetz anzugeben.

Das Problem wird durch die Verfahren sowie durch die Anordnungen mit den Merkmalen gemäß den unabhängigen Patentansprüchen gelöst.

Bei dem Verfahren zur Überprüfung einer Authentizität eines ersten Kommunikationsteilnehmers in einem Kommunikationsnetz wird bei dem ersten Kommunikationsteilnehmers unter Verwendung einer Fehlererkennungsangabe des ersten Kommunikationsteilnehmers und einer Information über eine Zufallsangabe eine erste Fehlerinformation gebildet. Bei einem zweiten Kommunikationsteilnehmer in dem Kommunikationsnetz wird unter Verwendung einer Fehlererkennungsangabe des zweiten Kommunikationsteilnehmers und der Information über die Zufallsangabe

eine zweite Fehlerinformation gebildet. Unter Verwendung der ersten Fehlerinformation und der zweiten Fehlerinformation wird die Authentizität des ersten Kommunikationsteilnehmers überprüft.

Bei der Anordnung zur Überprüfung einer Authentizität eines ersten Kommunikationsteilnehmers in einem Kommunikationsnetz ist der erste Kommunikationsteilnehmer derart eingerichtet, daß unter Verwendung einer Fehlererkennungsangabe des ersten Kommunikationsteilnehmers und einer Information über eine Zufallsangabe eine erste Fehlerinformation bildbar ist. Ferner weist die Anordnung einen zweiten Kommunikationsteilnehmer in dem Kommunikationsnetz auf, der derart eingerichtet ist, daß unter Verwendung einer Fehlererkennungsangabe des zweiten Kommunikationsteilnehmers und der Information über die Zufallsangabe eine zweite Fehlerinformation bildbar ist. Unter Verwendung der ersten Fehlerinformation und der zweiten Fehlerinformation ist die Authentizität des ersten Kommunikationsteilnehmers überprüfbar.

Unter der Überprüfung der Authentizität eines Kommunikationsteilnehmers in einem Kommunikationsnetz sind Verfahrensschritte zu verstehen, die im weiteren Sinn mit einer Überprüfung einer Berechtigung eines Kommunikationsteilnehmers zum Zugang zu einem Kommunikationsnetz oder einer Teilnahme an einer Kommunikation in einem Kommunikationsnetz durchgeführt werden.

Somit werden sowohl solche Verfahrensschritte umfaßt, die im Rahmen einer Überprüfung der Berechtigung eines Kommunikationsteilnehmers zum Zugang zu einem Kommunikationsnetz durchgeführt werden, als auch solche Verfahrensschritte umfaßt, die im Rahmen einer Bearbeitung oder einer Verwaltung von Daten, die bei der Überprüfung verwendet werden, durchgeführt werden.

Bevorzugte Weiterbildungen der Erfindung ergeben sich aus den abhängigen Ansprüchen.

Die im weiteren beschriebenen Weiterbildungen beziehen sich sowohl auf das Verfahren und die Anordnung.

Die Erfindung und die im weiteren beschriebenen Weiterbildungen können sowohl in Software als auch in Hardware, beispielsweise unter Verwendung einer speziellen elektrischen Schaltung realisiert werden.

In einer Ausgestaltung ist der erste Kommunikationsteilnehmer ein Dienstanbieter und/oder der zweite Kommunikationsteilnehmer ein Dienstnutzer in dem Kommunikationsnetz.

Bevorzugt wird als Fehlererkennungsangabe eine Sequenzfolgenummer verwendet.

In einer Ausgestaltung ist die Information über die Zufallsangabe eine Zufallszahl.

In einer Weiterbildung wird die Prüfung der Authentizität dadurch vereinfacht, daß eine Differenz zwischen der Fehlererkennungsangabe des ersten Kommunikationsteilnehmers und der Fehlererkennungsangabe des zweiten Kommunikationsteilnehmers ermittelt wird.

In einer Ausgestaltung wird die Prüfung der Authentizität dadurch hinsichtlich der Sicherheit des Kommunikationsnetzes weiter verbessert, daß die Differenz beschränkt wird

Bevorzugt wird eine Weiterbildung im Rahmen eines Mobilfunksystems eingesetzt. Bei dem Mobilfunksystem sind/ist der Dienstnutzer als Mobiltelefon und/oder der Dienstanbieter als Mobilfunknetzbetreiber realisiert.

In Figuren ist ein Ausführungsbeispiel der Erfindung dargestellt, welches im weiteren näher erläutert wird.

Es zeigen

Figur 1 ein Mobilfunksystem;

Figur 2 eine Skizze, in welcher symbolhaft eine Überprüfung einer Authentizität eines Kommunikationsteilnehmers dargestellt ist;

Figur 3 ein Ablaufdiagramm, in dem einzelne Verfahrensschritte bei einer Überprüfung einer Authentizität eines Dienstanbieters in einem Kommunikationsnetz dargestellt sind;

Figur 4 eine Skizze, in welcher symbolhaft eine Überprüfung einer Authentizität eines Kommunikationsteilnehmers gemäß dem 3G TS 33.102 Version 3.0.0-Standard dargestellt ist.

Ausführungsbeispiel: Mobilfunksystem

In **Fig.1** ist ein Mobilfunksystem 100 dargestellt. Das Mobilfunksystem 100 umfaßt ein Mobiltelefon 101, ein lokales Einwählnetz 102 mit einem Einwählnetzbetreiber 103 und ein Heimatnetz 104 mit einem Heimatnetzbetreiber 105.

Bei dem Heimatnetz 104 ist das Mobiltelefon 101 angemeldet und registriert.

Ferner weisen das Mobiltelefon 101, das Einwählnetz 102 und das Heimatnetz 104 jeweils eine zentrale Verarbeitungseinheit 106, 107, 108 mit einem Speicher 109, 110, 111 auf, mit welchen Verarbeitungseinheiten 106, 107, 108 die im folgenden beschriebene Vorgehensweise überwacht und gesteuert wird und

auf welchen Speichern 109, 110, 111 Daten gespeichert werden und/oder sind.

Das Einwählnetz 102 und das Heimatnetz 104 sind über eine Datenleitung 112, über welche digitale Daten übertragen werden können, miteinander verbunden. Das Mobiltelefon 101 und das Einwählnetz 102 sind über ein beliebiges Übertragungsmedium 113 zur Übertragung von digitalen Daten miteinander verbunden.

In **Fig.2** ist die Vorgehensweise bei einer Überprüfung einer Authentizität des Mobiltelefons 101 und die Vorgehensweise bei einer Überprüfung der Authentizität des Heimatnetzes 104 bzw. des Heimatnetzbetreibers 105 symbolhaft dargestellt und wird im folgenden kurz und auszugsweise erläutert.

Eine Übertragung von Daten ist in **Fig.2** jeweils durch einen Pfeil dargestellt. Eine Richtung eines Pfeils kennzeichnet eine Übertragungsrichtung bei einer Datenübertragung.

Die im folgende beschriebene und in **Fig.2** symbolhaft dargestellte Vorgehensweise basiert auf einem sogenannten 3G TS 33.102 Version 3.0.0-Standard, welcher eine Sicherheits-Architektur eines Mobilfunksystems beschreibt und in [1] beschrieben ist.

Bei einer Kommunikation wählt sich das Mobiltelefon 201 in das Einwählnetz 203 ein 210. Zu Beginn der Kommunikation erfolgt eine Überprüfung sowohl der Authentizität des Mobiltelefon 201 als auch der Authentizität des Heimatnetzes 204 bzw. des Heimatnetzbetreibers.

Dazu fordert das Einwählnetz 203 Authentifikationsdaten, mit welchen die Überprüfung der Authentizität des Nutzers 201 und des Heimatnetzes 204 bzw. des Heimatnetzbetreibers möglich ist, von dem Heimatnetz 204 an 211.

Die Authentifikationsdaten, welche von dem Heimatnetz 204 ermittelt werden, umfassen eine Zufallszahl und eine Sequenzfolgenummer des Heimatnetzes 204 (vgl. **Fig.3** Schritt 310). Die Sequenzfolgennummer des Heimatnetzes 204 wird derart ermittelt, daß ein Zähler des Heimatnetzes 204 bei jedem Kommunikationsversuch zwischen dem Mobiltelefon 201 und dem Heimatnetz 204 die Sequenzfolgenummer des Heimatnetzes 204 um den Wert 1 erhöht.

Es ist anzumerken, daß die Zufallszahl und die Sequenzfolgenummer des Heimatnetzes 204 nur einen Teil der Authentifikationsdaten darstellen und nicht abschließend zu verstehen sind. Weitere Authentifikationsdaten sind in [1] genannt.

Das Heimatnetz 204 überträgt die angeforderten Authentifikationsdaten an das Einwählnetz 203 212. Das Einwählnetz 203 bearbeitet die empfangenen Authentifikationsdaten in geeigneter Weise 213 und überträgt die bearbeiteten Authentifikationsdaten an das Mobiltelefon 201 214.

Das Mobiltelefon 201 überprüft unter Verwendung einer eigenen Sequenzfolgenummer, welche entsprechend der Sequenzfolgenummer des Heimatnetzes 204 gehandhabt wird, und der Sequenzfolgenummer des Heimatnetzes 204 die Authentizität des Heimatnetzes 204 215. Entsprechend des Heimatnetz 204 weist das Mobiltelefon 201 ebenfalls einen Zähler auf.

Die Vorgehensweise bei der Überprüfung der Authentizität des Heimatnetzes 204 ist in [1] beschrieben. Davon abweichende Verfahrensschritte sind im folgenden beschrieben.

Im Rahmen der Überprüfung der Authentizität des Heimatnetzes 203 wird eine sogenannte Überlaufprüfung des Zählers des Mobiltelefons 201 durchgeführt. Durch diese Überlaufprüfung wird ein Überlauf eines zulässigen Zahlenbereichs des Zählers des Mobiltelefons 201 verhindert.

Bei der Überlaufprüfung werden folgende Bedingungen geprüft:

1) Sequenzfolgenummer des Heimatnetzes 204 > Sequenzfolgenummer des Mobiltelefons 201;

2) Sequenzfolgenummer des Heimatnetzes 204 - Sequenzfolgenummer des Mobiltelefons 201 < vorgebbare Abweichung (hier: 1000000);

wobei für die vorgebbare Abweichung gilt:

- vorgebbare Abweichung hinreichend groß, um im normalen bzw. störungsfreien Kommunikationsbetrieb auszuschließen, daß:

Sequenzfolgenummer des Heimatnetzes 204 - Sequenzfolgenummer des Mobiltelefons 201 > vorgebbare Abweichung;

- max. zulässige Sequenzfolgenummer des Mobiltelefon 201/vorgebbare Abweichung hinreichend groß, um auszuschließen, daß die max. zulässige Sequenzfolgenummer des Mobiltelefon 201 im Betrieb erreicht wird.

Ein Ergebnis der Überprüfung der Authentizität des Heimatnetzes 204, "Authentizität in Ordnung" 216, "Authentizität in Ordnung, aber ein Sequenzfehler aufgetreten" 217 oder "Authentizität nicht in Ordnung" 218, wird von dem Mobiltelefon 201 an das Heimatnetz 204 übertragen 419.

Bei dem Ergebnis "Authentizität in Ordnung" 216 überprüft das Einwählnetz 203, wie es in [1] beschrieben ist, die Authentizität des Mobiltelefons 201 220.

Bei dem Ergebnis "Authentizität nicht in Ordnung" 218 wird die Kommunikation unterbrochen oder neu begonnen 221.

Bei dem Ergebnis "Authentizität in Ordnung, aber ein Sequenzfehler aufgetreten" 217 erfolgt eine Resynchronisation 222. Unter Resynchronisation ist eine Änderung der Sequenzfolgenummer des Heimatnetzes 204 zu verstehen.

Dazu überträgt das Mobiltelefon 201 Resynchronisationsdaten an das Einwählnetz 203 222.

Die Resynchronisationsdaten umfassen dieselbe Zufallszahl, die im Rahmen der Authentifikationsdaten übertragen wurde, sowie die Sequenzfolgenummer des Mobiltelefons 201 (vgl. **Fig.3** Schritt 320).

Das Einwählnetz 203 bearbeitet die Resynchronisationsdaten in geeignet Weise und überträgt die bearbeiteten Resynchronisationsdaten an das Heimatnetz 204.

Das Heimatnetz überprüft unter Verwendung der bearbeiteten Resynchronisationsdaten die Sequenzfolgenummer des Mobiltelefons 201 und die Sequenzfolgenummer des Heimatnetzes 204 und verändert gegebenenfalls die Sequenzfolgenummer des Heimatnetzes 204 223 (vgl. **Fig.3** Schritt 330).

Anschließend überträgt das Heimatnetz 204 neue Authentifikationsdaten, welche gegebenenfalls die veränderte Sequenzfolgenummer des Heimatnetzes 204 umfassen, an das Einwählnetz 203.

Zur Veranschaulichung der beschriebenen Vorgehensweise sind in **Fig.3** wichtige Schritte 300 der Vorgehensweise dargestellt.

Fig.3 zeigt einen ersten Schritt 310, im Rahmen dessen die Authentifikationsdaten (erste Fehlerinformation) ermittelt werden.

Im Rahmen eines zweiten Schritts 320 werden die Resynchronisationsdaten (zweite Fehlerinformation) ermittelt.

Im Rahmen eines dritten Schritts 330 werden unter Verwendung der Resynchronisationsdaten die Sequenzfolgenummer des Mobiltelefons und die Sequenzfolgenummer des Heimatnetzes überprüft.

Im folgenden wird eine Alternative des ersten Ausführungsbeispiels beschrieben.

Bei dem alternativen Ausführungsbeispiel ist ein Verfahren realisiert, mit dem das Heimatnetz gegenüber einem Datenverlust bei einem Systemabsturz sicherer gemacht wird.

Dazu wird jeweils in einem vorgebbaren zeitlichen Abstand die aktuelle Sequenzfolgenummer des Heimatnetzes in dem Speicher des Heimatnetzes gespeichert. Eine bei einem Systemabsturz des Heimatnetzes verloren gegangene Sequenzfolgenummer des Heimatnetzes wird derart wiederhergestellt, daß zu dem Wert der gespeicherten Sequenzfolgenummer ein vorgebbarer Aufschlagswert addiert wird. Der vorgebbare Aufschlagswert ist derart bemessen, daß ein Überschreiten der Summe aus Sequenzfolgenummer des Mobiltelefons und vorgebbare Abweichung nicht überschritten wird.

Bei dem alternativen Ausführungsbeispiel wird der vorgebbare Aufschlagswert derart bestimmt, daß eine durchschnittliche, aus Erfahrungswerten bei einem Betrieb des Kommunikationsnetzes bestimmte Zahl von Authentifikationsversuchen eines Tages des Heimatnetzes mit einem Faktor mit dem Wert 10 multipliziert wird.

In diesem Dokument ist folgende Veröffentlichung zitiert:

[1] 3G TS 33.102 Version 3.0.0-Draft-Standard, 3rd Generation Partnership Project, Technical Specification Group Services and System Aspects, 3G Security, Security Architecture, 05/1999.

Patentansprüche

1. Verfahren zur Überprüfung einer Authentizität eines ersten Kommunikationsteilnehmers in einem Kommunikationsnetz,
- bei dem bei dem ersten Kommunikationsteilnehmer unter Verwendung einer Fehlererkennungsangabe des Dienstanbieters und einer Information über eine Zufallsangabe eine erste Fehlerinformation gebildet wird;
- bei dem bei einem zweiten Kommunikationsteilnehmer in dem Kommunikationsnetz unter Verwendung einer Fehlererkennungsangabe des zweiten Kommunikationsteilnehmers und der Information über die Zufallsangabe eine zweite Fehlerinformation gebildet wird;
- bei dem unter Verwendung der ersten Fehlerinformation und der zweiten Fehlerinformation die Authentizität des ersten Kommunikationsteilnehmers überprüft wird.

2. Verfahren nach Anspruch 1,
bei dem eine Differenz zwischen der Fehlererkennungsangabe des ersten Kommunikationsteilnehmers und der Fehlererkennungsangabe des zweiten Kommunikationsteilnehmers ermittelt wird.

3. Verfahren nach Anspruch 2,
bei dem die Differenz beschränkt wird.

4. Verfahren nach einem der Ansprüche 1 bis 3,
eingesetzt im Rahmen eines Mobilfunksystems.

5. Anordnung zur Überprüfung einer Authentizität eines ersten Kommunikationsteilnehmers in einem Kommunikationsnetz,
- bei der der erste Kommunikationsteilnehmer, derart eingerichtet ist, daß unter Verwendung einer Fehlererkennungsangabe des ersten Kommunikationsteilnehmers und einer Information über eine Zufallsangabe eine erste Fehlerinformation bildbar ist;

- bei der ein zweiter Kommunikationsteilnehmer in dem Kommunikationsnetz derart eingerichtet ist, daß unter Verwendung einer Fehlererkennungsangabe des zweiten Kommunikationsteilnehmers und der Information über die Zufallsangabe eine zweite Fehlerinformation bildbar ist;
- bei der unter Verwendung der ersten Fehlerinformation und der zweiten Fehlerinformation die Authentizität des ersten Kommunikationsteilnehmers überprüfbar ist.

6. Anordnung nach Anspruch 5,
bei der der erste Kommunikationsteilnehmer ein Dienstanbieter und/oder der zweite Kommunikationsteilnehmer ein Dienstnutzer in dem Kommunikationsnetz sind/ist.

7. Anordnung nach Anspruch 5 oder 6,
bei der eine Fehlererkennungsangabe eine Sequenzfolgenummer ist.

8. Anordnung nach einem der Ansprüche 5 bis 7,
bei der die Information über die Zufallsangabe eine Zufallszahl ist.

9. Anordnung nach einem der Ansprüche 5 bis 8,
bei der der erste Kommunikationsteilnehmer ein Dienstanbieter in dem Kommunikationsnetz und/oder der zweite Kommunikationsteilnehmer ein Dienstnutzer in dem Kommunikationsnetz sind/ist.

10. Anordnung nach Anspruch 9,
bei der der Dienstanbieter ein Mobilfunkbetreiber und/oder der Dienstnutzer ein Mobiltelefon sind/ist.

11. Anordnung nach einem der Ansprüche 5 bis 10,
eingesetzt im Rahmen eines Mobilfunksystems.

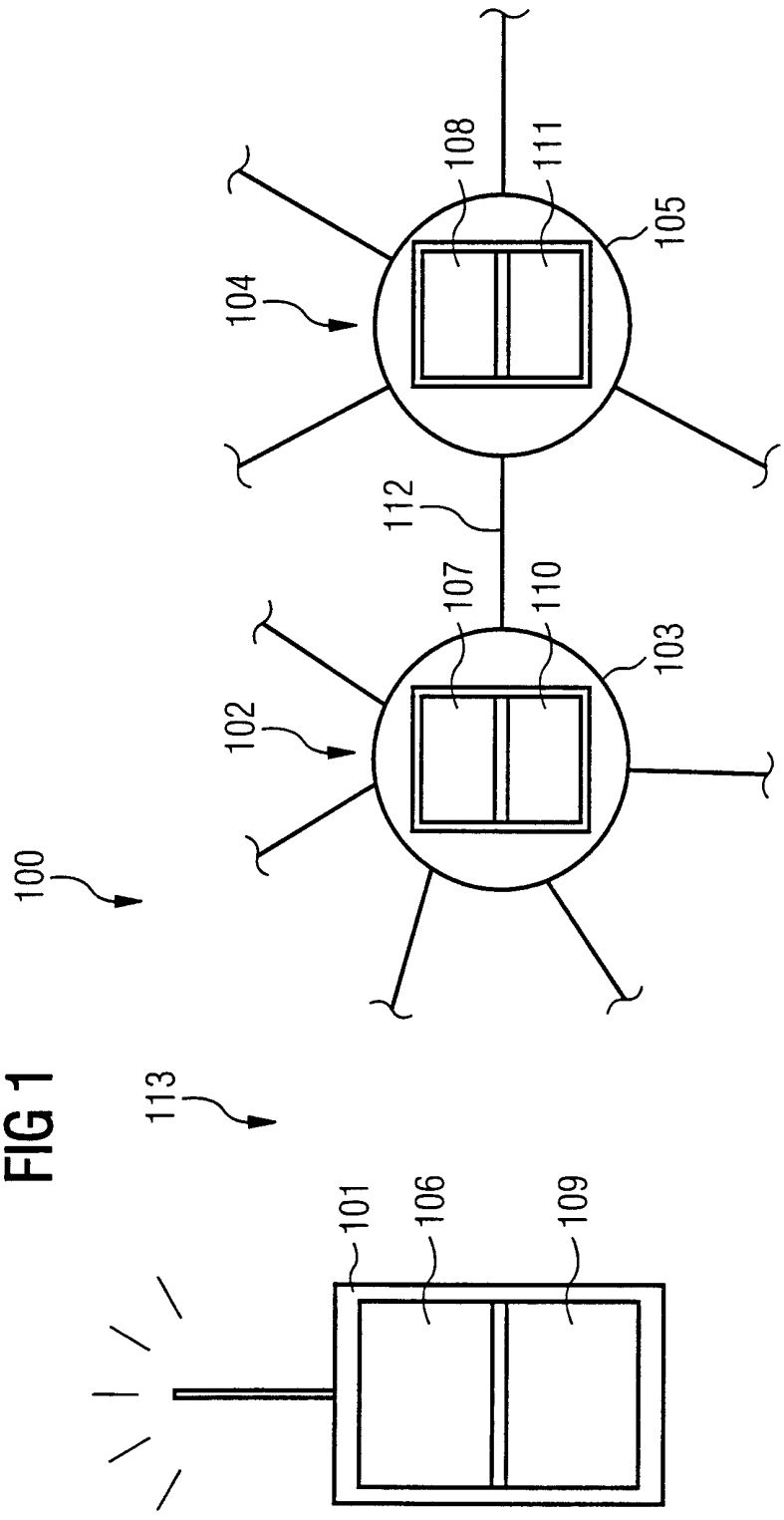


FIG 1

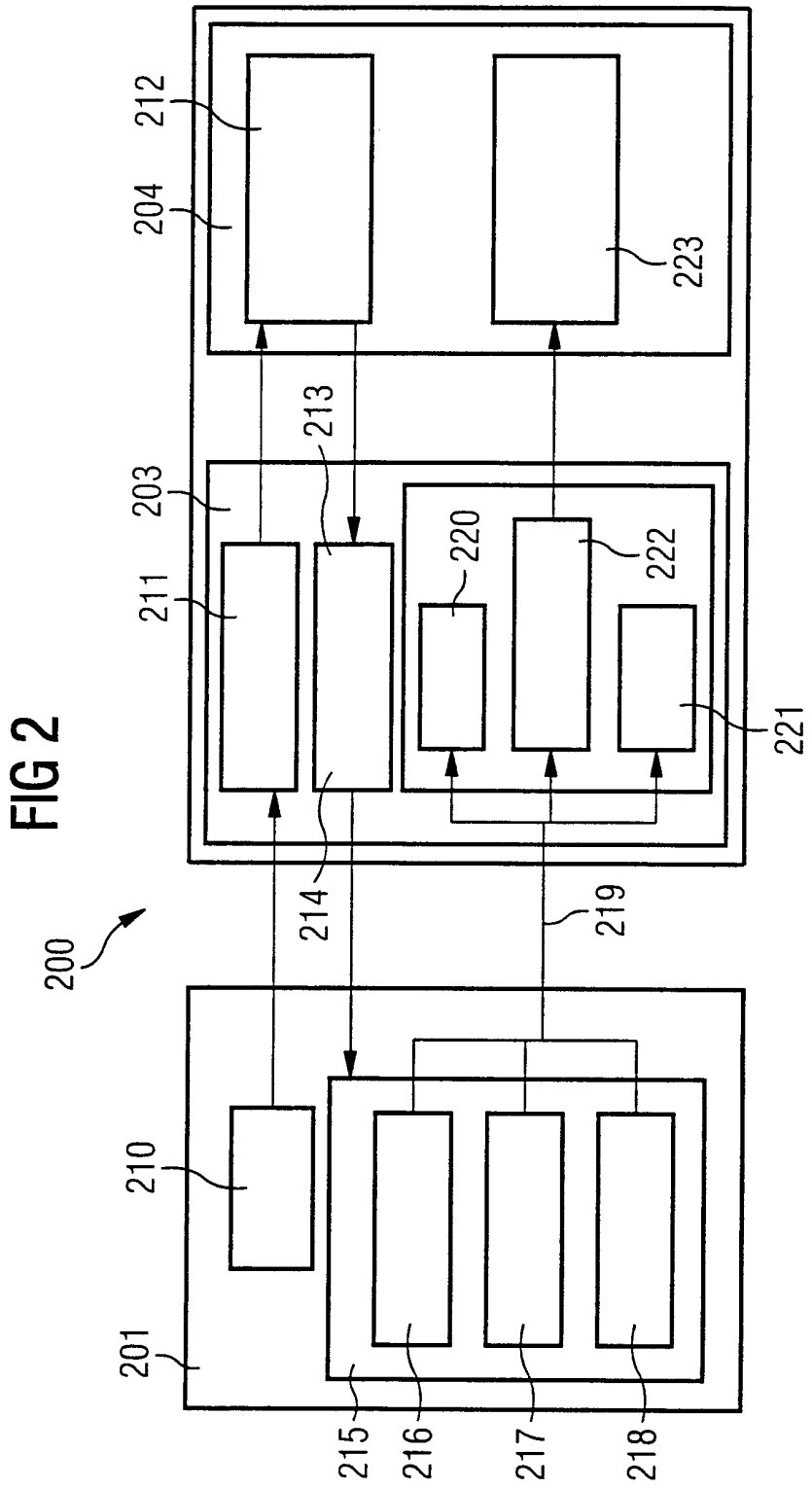

212
204
223
213
203
220
222
211
221
214
219
200
210
201
215
216
217
218

FIG 2

FIG 3

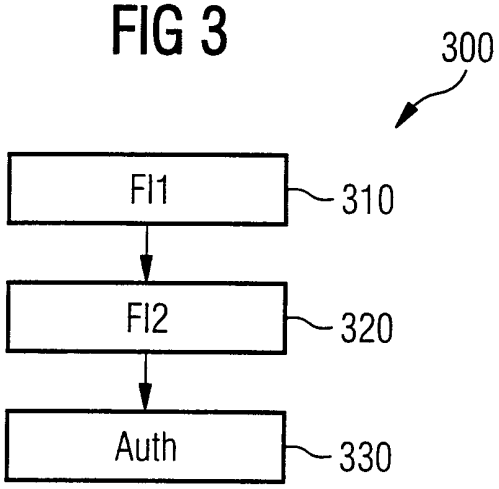
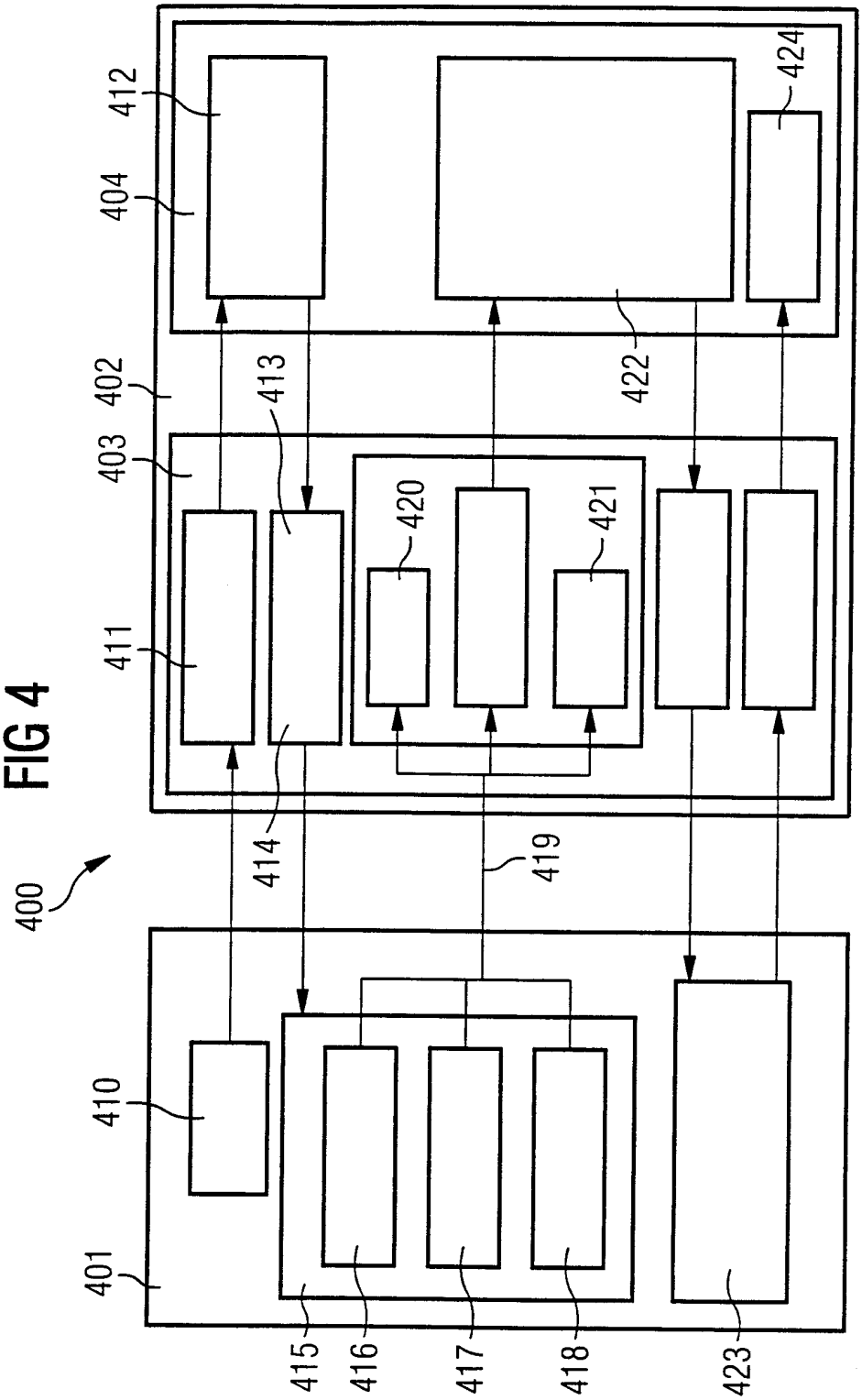


FIG 4


400
401
402
403
404
410
411
412
413
414
415
416
417
418
419
420
421
422
423
424

INTERNATIONAL SEARCH REPORT

Int onal Application No
PCT/DE 00/01788

A. CLASSIFICATION OF SUBJECT MATTER
IPC 7 H04Q7/38

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)
IPC 7 H04Q

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 5 799 084 A (GALLAGHER MICHAEL D ET AL) 25 August 1998 (1998-08-25) column 5, line 45 -column 6, line 26	1-11
X	WO 91 01067 A (MOTOROLA INC) 24 January 1991 (1991-01-24) page 4, line 22 -page 5, line 22	1,2,4-11

☐ Further documents are listed in the continuation of box C.

☒ Patent family members are listed in 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	Date of mailing of the international search report
4 October 2000	17/10/2000

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, Tx. 31 651 epo nl, Fax: (+31–70) 340–3016	Bernedo Azpiri, P

1

Form PCT/ISA/210 (second sheet) (July 1992)

INTERNATIONAL SEARCH REPORT

Information on patent family members

Int ional Application No
PCT/DE 00/01788

Patent document cited in search report	Publication date	Patent family member(s)	Publication date
US 5799084 A	25-08-1998	NONE	
WO 9101067 A	24-01-1991	AU 6034790 A	06-02-1991
		CA 2063447 A,C	13-01-1991
		IL 94467 A	31-12-1995
		JP 2684118 B	03-12-1997
		JP 5503816 T	17-06-1993
		MX 166091 B	17-12-1992
		US 5239294 A	24-08-1993

INTERNATIONALER RECHERCHENBERICHT

Internationales Aktenzeichen
PCT/DE 00/01788

A. KLASSIFIZIERUNG DES ANMELDUNGSGEGENSTANDES
IPK 7 H04Q7/38

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

B. RECHERCHIERTE GEBIETE

Recherchierter Mindestprüfstoff (Klassifikationssystem und Klassifikationssymbole)
IPK 7 H04Q

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 5 799 084 A (GALLAGHER MICHAEL D ET AL) 25. August 1998 (1998-08-25) Spalte 5, Zeile 45 -Spalte 6, Zeile 26	1-11
X	WO 91 01067 A (MOTOROLA INC) 24. Januar 1991 (1991-01-24) Seite 4, Zeile 22 -Seite 5, Zeile 22	1,2,4-11

☐ 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
"&" Veröffentlichung, die Mitglied derselben Patentfamilie ist

Datum des Abschlusses der internationalen Recherche	Absendedatum des internationalen Recherchenberichts
4. Oktober 2000	17/10/2000

Name und Postanschrift der Internationalen Recherchenbehörde	Bevollmächtigter Bediensteter
Europäisches Patentamt, P.B. 5818 Patentlaan 2 NL – 2280 HV Rijswijk Tel. (+31–70) 340–2040, Tx. 31 651 epo nl, Fax: (+31–70) 340–3016	Bernedo Azpiri, P

1

INTERNATIONALER RECHERCHENBERICHT

Angaben zu Veröffentlich ...n, die zur selben Patentfamilie gehören

Int... onales Aktenzeichen
PCT/DE 00/01788

Im Recherchenbericht angeführtes Patentdokument		Datum der Veröffentlichung	Mitglied(er) der Patentfamilie		Datum der Veröffentlichung
US 5799084	A	25-08-1998	KEINE		
WO 9101067	A	24-01-1991	AU	6034790 A	06-02-1991
			CA	2063447 A,C	13-01-1991
			IL	94467 A	31-12-1995
			JP	2684118 B	03-12-1997
			JP	5503816 T	17-06-1993
			MX	166091 B	17-12-1992
			US	5239294 A	24-08-1993