PCT WELTORGANISATION FÜR GEISTIGES EIGENTUM
Internationales Büro

INTERNATIONALE ANMELDUNG VERÖFFENTLICHT NACH DEM VERTRAG ÜBER DIE INTERNATIONALE ZUSAMMENARBEIT AUF DEM GEBIET DES PATENTWESENS (PCT)

(51) Internationale Patentklassifikation 7 :		(11) Internationale Veröffentlichungsnummer: **WO 00/18061**
H04L 9/32, G07F 7/10	**A1**	(43) Internationales Veröffentlichungsdatum: 30. März 2000 (30.03.00)

(21) **Internationales Aktenzeichen:** PCT/EP99/06664

(22) **Internationales Anmeldedatum:** 9. September 1999 (09.09.99)

(30) **Prioritätsdaten:**
98117939.3 22. September 1998 (22.09.98) EP

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

(72) **Erfinder; und**
(75) **Erfinder/Anmelder** *(nur für US)*: POCKRANDT, Wolfgang [DE/DE]; Ilmstrasse 1, D–85293 Reichertshausen (DE).

(81) **Bestimmungsstaaten:** BR, CN, IN, JP, KR, MX, RU, UA, US, europäisches Patent (AT, BE, CH, CY, DE, DK, ES, FI, FR, GB, GR, IE, IT, LU, MC, NL, PT, SE).

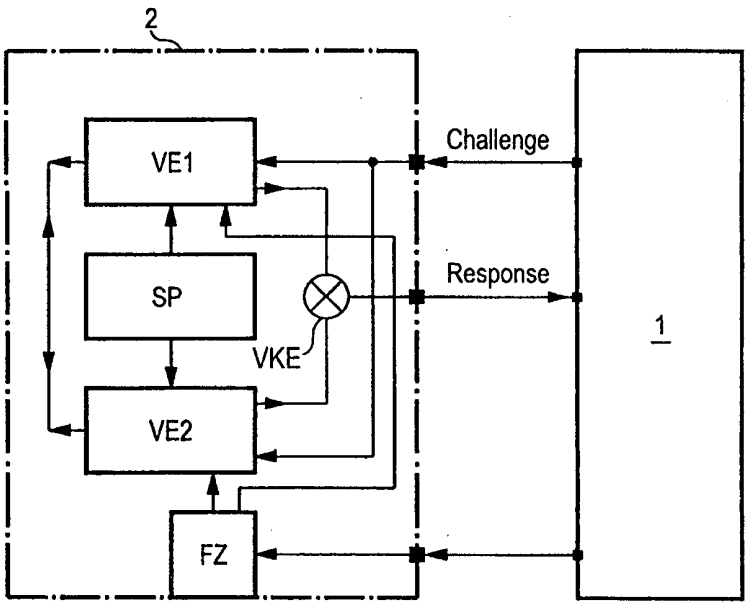
Veröffentlicht
Mit internationalem Recherchenbericht.
Vor Ablauf der für Änderungen der Ansprüche zugelassenen Frist; Veröffentlichung wird wiederholt falls Änderungen eintreffen.

(54) **Title:** METHOD FOR AUTHENTICATING AT LEAST ONE SUBSCRIBER DURING A DATA EXCHANGE

(54) **Bezeichnung:** VERFAHREN ZUR AUTHENTIFIKATION ZUMINDEST EINES TEILNEHMERS BEI EINEM DATENAUSTAUSCH

(57) **Abstract**

The invention relates to a method for authenticating at least one subscriber (2) during a data exchange between at least two subscribers (1, 2), whereby a first item of data (challenge) is transmitted from a first subscriber (1) to a second subscriber (2), the second subscriber (2) processes this item of data (challenge) into a second item of data (response) by means an algorithm and transmits it to the first subscriber (1) who verifies the exactitude thereof. While the first item of data (challenge) is being processed by the algorithm, further processing of said data item (challenge) occurs.



(57) **Zusammenfassung**

Bei einem Verfahren zur Authentifikation zumindest eines Teilnehmers (2) bei einem Datenaustausch zwischen zumindest zwei Teilnehmern (1, 2) wird von einem ersten Teilnehmer (1) einem zweiten Teilnehmer (2) ein erstes Datum (Challenge) übermittelt, der zweite Teilnehmer (2) verarbeitet dieses erste Datum (Challenge) mittels eines Algorithmus zu einem zweiten Datum (Response) und übermittelt es an den ersten Teilnehmer (1), der es auf dessen Richtigkeit überprüft. Gleichzeitig zur Verarbeitung des ersten Datums (Challenge) mittels des Algorithmus findet zumindest eine weitere Verarbeitung des ersten Datums (Challenge) statt.

LEDIGLICH ZUR INFORMATION

Codes zur Identifizierung von PCT-Vertragsstaaten auf den Kopfbögen der Schriften, die internationale Anmeldungen gemäss dem PCT veröffentlichen.

AL	Albanien
AM	Armenien
AT	Österreich
AU	Australien
AZ	Aserbaidschan
BA	Bosnien-Herzegowina
BB	Barbados
BE	Belgien
BF	Burkina Faso
BG	Bulgarien
BJ	Benin
BR	Brasilien
BY	Belarus
CA	Kanada
CF	Zentralafrikanische Republik
CG	Kongo
CH	Schweiz
CI	Côte d'Ivoire
CM	Kamerun
CN	China
CU	Kuba
CZ	Tschechische Republik
DE	Deutschland
DK	Dänemark
EE	Estland
ES	Spanien
FI	Finnland
FR	Frankreich
GA	Gabun
GB	Vereinigtes Königreich
GE	Georgien
GH	Ghana
GN	Guinea
GR	Griechenland
HU	Ungarn
IE	Irland
IL	Israel
IS	Island
IT	Italien
JP	Japan
KE	Kenia
KG	Kirgisistan
KP	Demokratische Volksrepublik Korea
KR	Republik Korea
KZ	Kasachstan
LC	St. Lucia
LI	Liechtenstein
LK	Sri Lanka
LR	Liberia
LS	Lesotho
LT	Litauen
LU	Luxemburg
LV	Lettland
MC	Monaco
MD	Republik Moldau
MG	Madagaskar
MK	Die ehemalige jugoslawische Republik Mazedonien
ML	Mali
MN	Mongolei
MR	Mauretanien
MW	Malawi
MX	Mexiko
NE	Niger
NL	Niederlande
NO	Norwegen
NZ	Neuseeland
PL	Polen
PT	Portugal
RO	Rumänien
RU	Russische Föderation
SD	Sudan
SE	Schweden
SG	Singapur
SI	Slowenien
SK	Slowakei
SN	Senegal
SZ	Swasiland
TD	Tschad
TG	Togo
TJ	Tadschikistan
TM	Turkmenistan
TR	Türkei
TT	Trinidad und Tobago
UA	Ukraine
UG	Uganda
US	Vereinigte Staaten von Amerika
UZ	Usbekistan
VN	Vietnam
YU	Jugoslawien
ZW	Zimbabwe

Beschreibung

Verfahren zur Authentifikation zumindest eines Teilnehmers bei einem Datenaustausch

Die Erfindung betrifft ein Verfahren zur Authentifikation zumindest eines Teilnehmers bei einem Datenaustausch zwischen zumindest zwei Teilnehmern, bei dem einem ersten Teilnehmer von einem zweiten Teilnehmer ein erstes Datum übermittelt wird, der erste Teilnehmer dieses erste Datum mittels eines Algorithmus zu einem zweiten Datum verarbeitet und an den zweiten Teilnehmer übermittelt, und der zweite Teilnehmer das zweite Datum auf dessen Richtigkeit überprüft.

Solche Verfahren sind aus der Schrift "Cryptographic Identification Methods for Smart Cards in the Process of Standardization" von Hanns-Peter Königs aus IEEE Communications Magazine, Vol. 29, No. 6, June 1991, pp. 42 - 48 bekannt. Bei dem dortigen Verfahren wird als erstes Datum eine Zufallszahl von einem Schreib/Lese-Terminal zu einer Smartcard gesendet und dort mittels eines geheimen Algorithmus und zumindest einer Geheimzahl verschlüsselt. Das verschlüsselte Ergebnis wird von der Smartcard zum Terminal zurückgesendet und dort entweder entschlüsselt oder ebenfalls in gleicher Weise verschlüsselt. Das jeweilige Ergebnis wird mit der anfänglich gesendeten Zufallszahl beziehungsweise dem empfangenen zweiten Datum verglichen. Ein positives Vergleichsergebnis zeigt an, daß beide Datenaustauschteilnehmer über den richtigen Algorithmus und die richtige Geheimzahle beziehungsweise den richtigen Schlüssel verfügen und damit authentisch sind.

Authentifikationsverfahren werden vor allem dann angewendet, wenn es sich beim Datenaustausch um geldwerte oder sicherheitskritische Vorgänge handelt. Solche Vorgänge sind naturgemäß Angriffen ausgesetzt. Einem Angreifer stellt sich dabei die Aufgabe, die beteiligten Schlüssel, Geheimzahlen und Algorithmen herauszufinden. Aus dem Ablauf der Kommunikation

läßt sich auf die Art der verwendeten Authentifikation schließen und der Angriff damit gezielt fahren.

Die Aufgabe vorliegender Erfindung ist es, die Art des durchgeführten Authentifikationsverfahrens möglichst gut zu verbergen.

Die Aufgabe wird durch ein Verfahren gemäß Anspruch 1 gelöst. Vorteilhafte Weiterbildungen sind in den Unteransprüchen angegeben.

Durch die gleichzeitige Ausführung zumindest zweier Verarbeitungsvorgänge wird es einem Angreifer deutlich erschwert, aus einer Untersuchung beispielsweise der zeitabhängigen Leistungsaufnahme auf den internen Ablauf der Authentifikation zu schließen.

Die Erfindung wird nachfolgend anhand eines Ausführungsbeispiels mit Hilfe einer Figur näher erläutert.

Die prinzipielle Darstellung eines Datenaustauschsystems gemäß Figur 1 zeigt einen ersten Teilnehmer 1, der beispielsweise ein Lese/Schreib-Terminal sein kann und einen zweiten Teilnehmer 2, der im Beispiel eine Smartcard oder Chipkarte sein soll. Beim im folgenden erläuterten Beispiel soll sich der zweite Teilnehmer, also die Karte, gegenüber dem ersten Teilnehmer, dem Terminal authentifizieren. Aus diesem Grund sind nur die nötigen Schaltungseinrichtungen in der Karte dargestellt. Für den Fall, daß sich auch das Terminal 1 gegenüber der Karte 2 authentifizieren soll, müßte auch das Terminal 1 entsprechende Schaltungseinrichtungen aufweisen.

Als erstes sendet das Terminal 1 ein erstes Datum, eine sogenannte Challenge, zur Karte 2. Die Challenge wird in erfindungsgemäßer Weise dort sowohl einer ersten Verarbeitungseinrichtung VE1 als auch einer zweiten Verarbeitungseinrichtung VE2 zugeführt. Zur für die Authentifizierung nötigen Verar-

beitung der Challenge werden den Verarbeitungseinrichtungen VE1, VE2 aus einem Speicherbereich SP die nötigen Informationen wie Geheimzahlen oder Schlüssel zugeführt.

Die Verarbeitung selbst kann entweder ein einfacher Vergleich der Challenge mit einem erwarteten, im Speicherbereich SP abgespeicherten Wert sein oder aber eine komplizierte Verschlüsselung beispielsweise entsprechend dem DES- oder dem RSA-Algorithmus. Zu diesem Zweck würden die Verarbeitungseinheiten VE1, VE2 als komplexe Mikroprozessoren mit zugeordneten Krypto-Coprozessoren ausgebildet sein. Häufig verwendet werden hardwaremäßig realisierte Einwegverschlüsselungsvorrichtungen, die beispielsweise mit einem rückgekoppelten Schieberegister gebildet sind.

Die Ausgangsdaten der Verarbeitungseinrichtungen VE1, VE2 werden einer Verknüpfungseinrichtung zugeführt, deren Ausgangssignal als Response an das Terminal 1 weitergeleitet wird. die Verknüpfungseinrichtung VKE muß die Ausgangsdaten der Verarbeitungseinrichtungen VE1, VE2 nicht zwangsläufig mit einander verknüpfen, sondern kann auch nur das Ausgangsdatum der ersten Verarbeitungseinrichtung VE1 unverändert als Response durchlassen und das Ausgangsdatum der zweiten Verarbeitungseinrichtung VE2 sperren, da der wesentliche Aspekt der Erfindung im gleichzeitigen Ablauf zumindest zweier, vorzugsweise unterschiedlicher Verarbeitungsvorgänge ist, um beispielsweise aus der Leistungsaufnahme nicht auf den internen Aufbau und die zugehörigen Daten schließen zu können.

Es ist jedoch von Vorteil, wenn die Ausgangsdaten der Verarbeitungseinrichtungen VE1, VE2 beispielsweise mittels eines die Verknüpfungseinrichtung VKE realisierenden EXOR-Gatters miteinander verknüpft werden.

Das Blockschaltbild der Figur zeigt auch die erfindungsgemäß weiterbildende Verknüpfung der beiden Verarbeitungseinheiten VE1, VE2. Verknüpfung heißt hier das Zwischen- oder Endergeb-

nisse der Datenverarbeitung in einer Verarbeitungseinheit in die Verarbeitung der jeweils anderen Verarbeitungseinheit einbezogen wird. Dabei können in einer ersten Weiterbildung der Erfindung Ausgangsdaten nur einer Verarbeitungseinheit in der anderen berücksichtigt werden und in einer weiteren Weiterbildung Ausgangsdaten beider Verarbeitungseinheiten in der jeweils anderen berücksichtigt werden.

Wie bereits in der Beschreibungseinleitung ausgeführt wurde, kann die Richtigkeit der Response im Terminal 1 auf verschiedene Weise überprüft werden. Hierzu sind einige Möglichkeiten in der bereits genannten Schrift ausführlich dargestellt und erläutert und aus diesem Grund in der Figur nicht näher ausgeführt.

In einer weiteren Ausbildung der Erfindung ist ein Fehlerzähler FZ vorgesehen, der die Anzahl der negativen Vergleichsergebnisse festhält und bei einer bestimmten voreingestellten Anzahl die Verarbeitungseinrichtungen VE1, VE2 sperrt, so daß keine weitere Authentifizierung und damit kein weiterer Datenaustausch zwischen dem Terminal 1 und der Karte 2 stattfinden kann. Hierdurch wird erreicht, daß keine beliebige Anzahl von Versuchen zur Untersuchung des Authentifikationsvorgangs durchgeführt werden kann.

Patentansprüche

1. Verfahren zur Authentifikation zumindest eines Teilnehmers (2) bei einem Datenaustausch zwischen zumindest zwei Teilnehmern (1, 2), bei dem von einem ersten Teilnehmer (1) einem zweiten Teilnehmer (2) ein erstes Datum (Challenge) übermittelt wird, der zweite Teilnehmer (2) dieses erste Datum (Challenge) mittels eines Algorithmus zu einem zweiten Datum (Response) verarbeitet und an den ersten Teilnehmer (1) übermittelt und der erste Teilnehmer (1) das zweite Datum (Response) auf dessen Richtigkeit überprüft,
dadurch gekennzeichnet,
daß gleichzeitig zur Verarbeitung des ersten Datums (Challenge) mittels des Algorithmus zumindest eine weitere Verarbeitung des ersten Datums (Challenge) stattfindet.

2. Verfahren nach Anspruch 1, **dadurch gekennzeichnet,** daß die weitere Verarbeitung mittels eines zweiten Algorithmus erfolgt.

3. Verfahren nach Anspruch 1, **dadurch gekennzeichnet,** daß die weitere Verarbeitung ein Vergleich des ersten Datums (Challenge) mit einem vorgegebenen Datum ist.

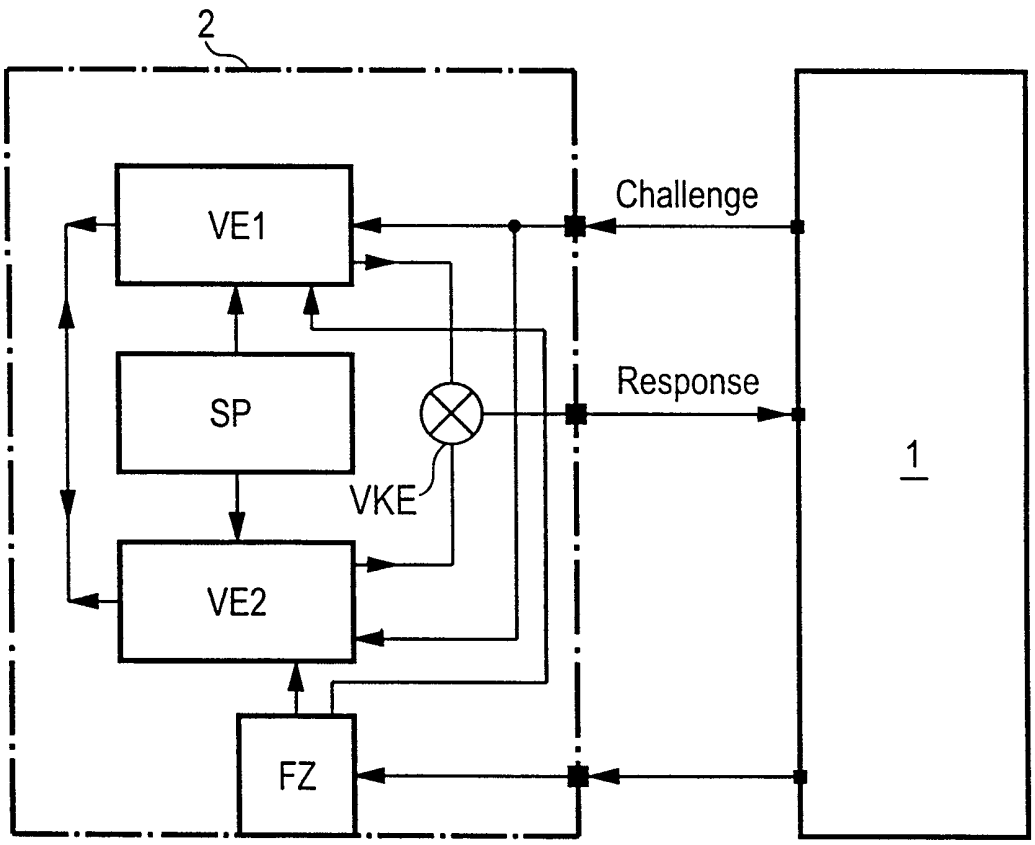
4. Verfahren nach einem der vorhergehenden Ansprüche, **dadurch gekennzeichnet,** daß die Ergebnisse der beiden Verarbeitungen zum zweiten Datum (Response) miteinander verknüpft werden.

5. Verfahren nach einem der vorhergehenden Ansprüche, **dadurch gekennzeichnet,** daß das End- oder ein Zwischenergebnis der weiteren Verarbeitung des ersten Datums (Challenge) zur Verarbeitung des ersten Datums (Challenge) mittels des ersten Algorithmus herangezogen wird.

6. Verfahren nach einem der vorhergehenden Ansprüche, **dadurch gekennzeichnet,** daß das End- oder ein Zwischenergebnis der Verarbeitung des ersten Datums (Challenge) mittels des ersten

Algorithmus zur weiteren Verarbeitung des ersten Datums (Challenge) herangezogen wird.

7. Verfahren nach einem der vorhergehenden Ansprüche, **dadurch gekennzeichnet,** daß die Anzahl der Verarbeitungsvorgänge durch einen Fehlerzähler (FZ) begrenzt ist.


2
VE1
SP
VKE
VE2
FZ
Challenge
Response
1

INTERNATIONAL SEARCH REPORT

Inter nal Application No
PCT/EP 99/06664

A. CLASSIFICATION OF SUBJECT MATTER
IPC 7 H04L9/32 G07F7/10

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 H04L G07F

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)

C. DOCUMENTS CONSIDERED TO BE RELEVANT

Category °	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
X	WO 97 15161 A (NOKIA) 24 April 1997 (1997-04-24) page 11, paragraph 1; figure 3	1,2
A	DE 43 39 460 C (SIEMENS) 6 April 1995 (1995-04-06) abstract column 3, line 54 -column 4, line 11	1,7

☐ 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
10 January 2000	18/01/2000

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	Holper, G

1

INTERNATIONAL SEARCH REPORT

...formation on patent family members

Inter ...nal Application No
PCT/EP 99/06664

Patent document cited in search report	Publication date	Patent family member(s)	Publication date
WO 9715161 A	24-04-1997	US 5991407 A	23-11-1999
		AU 7299196 A	07-05-1997
		CA 2234655 A	24-04-1997
		EP 0856233 A	05-08-1998
DE 4339460 C	06-04-1995	EP 0654919 A	24-05-1995

INTERNATIONALER RECHERCHENBERICHT

Internationales Aktenzeichen
PCT/EP 99/06664

A. KLASSIFIZIERUNG DES ANMELDUNGSGEGENSTANDES
IPK 7 H04L9/32 G07F7/10

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

B. RECHERCHIERTE GEBIETE

Recherchierter Mindestprüfstoff (Klassifikationssystem und Klassifikationssymbole)
IPK 7 H04L G07F

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)

C. ALS WESENTLICH ANGESEHENE UNTERLAGEN

Kategorie°	Bezeichnung der Veröffentlichung, soweit erforderlich unter Angabe der in Betracht kommenden Teile	Betr. Anspruch Nr.
X	WO 97 15161 A (NOKIA) 24. April 1997 (1997-04-24) Seite 11, Absatz 1; Abbildung 3 ---	1,2
A	DE 43 39 460 C (SIEMENS) 6. April 1995 (1995-04-06) Zusammenfassung Spalte 3, Zeile 54 -Spalte 4, Zeile 11 -----	1,7

☐ 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
10. Januar 2000	18/01/2000

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	Holper, G

1

INTERNATIONALER RECHERCHENBERICHT

Angaben zu Veröffentlichungen, die zur selben Patentfamilie gehören

Internationales Aktenzeichen
PCT/EP 99/06664

Im Recherchenbericht angeführtes Patentdokument	Datum der Veröffentlichung	Mitglied(er) der Patentfamilie	Datum der Veröffentlichung
WO 9715161 A	24-04-1997	US 5991407 A	23-11-1999
		AU 7299196 A	07-05-1997
		CA 2234655 A	24-04-1997
		EP 0856233 A	05-08-1998
DE 4339460 C	06-04-1995	EP 0654919 A	24-05-1995