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

(19) Weltorganisation für geistiges Eigentum
Internationales Büro

PCT

(43) Internationales Veröffentlichungsdatum
22. Dezember 2005 (22.12.2005)

(10) Internationale Veröffentlichungsnummer
WO 2005/122055 A3

(51) Internationale Patentklassifikation:
G06F 1/00 (2006.01)

(21) Internationales Aktenzeichen: PCT/EP2005/006111

(22) Internationales Anmeldedatum:
7. Juni 2005 (07.06.2005)

(25) Einreichungssprache: Deutsch

(26) Veröffentlichungssprache: Deutsch

(30) Angaben zur Priorität:
10 2004 027 686.2 7. Juni 2004 (07.06.2004) DE

(71) Anmelder *(für alle Bestimmungsstaaten mit Ausnahme von US)*: **SCM MICROSYSTEMS GMBH** [DE/DE]; Oskar-Messter-Strasse 13, 85737 Ismaning (DE).

(72) Erfinder; und

(75) Erfinder/Anmelder *(nur für US)*: **GENEVOIS, Christophe** [FR/FR]; Chemin des Buissières, F-30500 Saint Brès (FR). **NEIFER, Wolfgang** [DE/DE]; Altenhauser Strasse 13, 85356 Freising (DE).

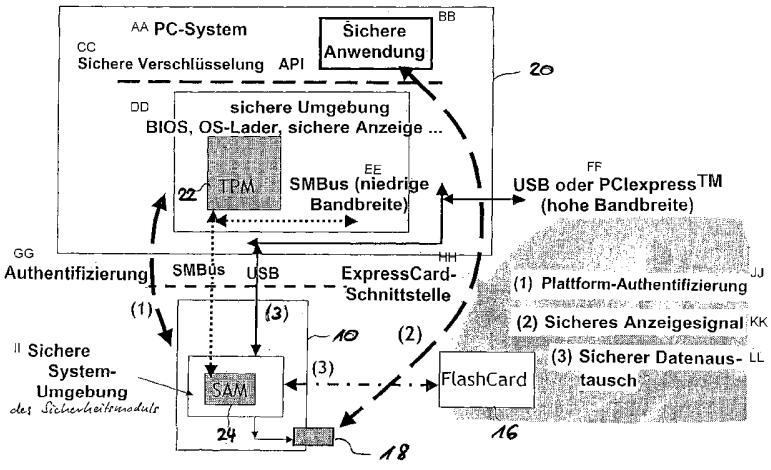
(74) Anwalt: **STRASS, Jürgen**; Prinz & Partner GbR, Manzingerweg 7, 81241 München (DE).

(81) Bestimmungsstaaten *(soweit nicht anders angegeben, für jede verfügbare nationale Schutzrechtsart)*: AE, AG, AL, AM, AT, AU, AZ, BA, BB, BG, BR, BW, BY, BZ, CA, CH, CN, CO, CR, CU, CZ, DE, DK, DM, DZ, EC, EE, EG, ES, FI, GB, GD, GE, GH, GM, HR, HU, ID, IL, IN, IS, JP, KE, KG, KM, KP, KR, KZ, LC, LK, LR, LS, LT, LU, LV, MA, MD, MG, MK, MN, MW, MX, MZ, NA, NG, NI, NO, NZ, OM, PG, PH, PL, PT, RO, RU, SC, SD, SE, SG, SK, SL,

[Fortsetzung auf der nächsten Seite]

(54) Title: DETACHABLE SECURITY MODULE

(54) Bezeichnung: ABNEHMBARES SICHERHEITSMODUL



AA ... PC SYSTEM
BB ... SECURE USE
CC ... SECURE ENCODING API
DD ... SECURE ENVIRONMENT BIOS, OS LOADER, SECURE DISPLAY...
EE ... SMBUS (LOW BAND WIDTH)
FF ... USB OR PCIEXPRESSTM (HIGH BAND WIDTH)

GG ... AUTHENTICATION
HH ... EXPRESS CARD INTERFACE
II ... SECURE SYSTEM ENVIRONMENT OF THE SECURITY MODULE
JJ ... PLATFORM AUTHENTICATION
KK ... SECURE DISPLAY SIGNAL
LL ... SECURE DATA EXCHANGE

(57) **Abstract:** According to one aspect of the invention, at least essential components of a security platform module, in particular a TPM, are provided for a host system (20) on a detachable security module (10), which are used to electrically connect to a host system (20). According to a second aspect of the invention, the host system (20) comprises an integrated first authentication means (22) which is used to construct a first security step, and the security module (10) supports a second authentication means (24). The second authentication means (24) can be constructed by interacting a second security step, which is superior to the first security step, with the first authentication means (22).

(57) **Zusammenfassung:** Gemäß einem ersten Aspekt sind auf einem abnehmbaren Sicherheitsmodul (10) zur elektrischen Verbindung mit einem Host-System (20) wenigstens wesentliche Bestandteile eines sicheren Plattformmoduls, insbesondere eines TPM, für ein Host-System (20) vorgesehen. Gemäß einem zweiten Aspekt weist das Host-System

[Fortsetzung auf der nächsten Seite]

WO 2005/122055 A3

SM, SY, TJ, TM, TN, TR, TT, TZ, UA, UG, US, UZ, VC, VN, YU, 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, HU, IE, IS, IT, LT, LU, MC, NL, PL, PT, RO, SE, SI, SK, TR), OAPI (BF, BJ, CF, CG, CI, CM, GA, GN, GQ, GW, ML, MR, NE, SN, TD, TG).

Veröffentlicht:

— *mit internationalem Recherchenbericht*

— *vor Ablauf der für Änderungen der Ansprüche geltenden Frist; Veröffentlichung wird wiederholt, falls Änderungen eintreffen*

(88) Veröffentlichungsdatum des internationalen Recherchenberichts: 6. April 2006

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.

(20) ein eingebautes erstes Authentifizierungsmittel (22) zum Aufbau einer ersten Sicherheitsstufe auf, und das Sicherheitsmodul (10) trägt ein zweites Authentifizierungsmittel (24). Das zweite Authentifizierungsmittel (24) kann durch Interaktion mit dem ersten Authentifizierungsmittel (22) eine der ersten Sicherheitsstufe überlegene zweite Sicherheitsstufe aufbauen.

INTERNATIONAL SEARCH REPORT

International Application No
PCT/EP2005/006111

A. CLASSIFICATION OF SUBJECT MATTER
G06F1/00

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

B. FIELDS SEARCHED

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

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.
Y	ST MICROELECTRONICS: "Trusted Platform Module (TPM)" May 2004 (2004-05), ST MICROELECTRONICS , XP002345888 the whole document -----	1-3
Y	TRUSTED COMPUTING GROUP, INCORPORATED: "TCG Specification Architecture Overview Specification Revision 1.2" 28 April 2004 (2004-04-28), TRUSTED COMPUTING GROUP, INCORPORATED , XP002352046 the whole document -----	1-3
A	EP 0 440 158 A (KABUSHIKI KAISHA TOSHIBA) 7 August 1991 (1991-08-07) siehe Formblatt PCT/ISA/206 -----	1-3

☐ 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
2 November 2005	**23.01.2006**
Name and mailing address of the ISA 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	Authorized officer Harms, C

Form PCT/ISA/210 (second sheet) (January 2004)

INTERNATIONAL SEARCH REPORT

International application No.
PCT/EP2005/006111

Box I Observations where certain claims were found unsearchable (Continuation of item 1 of first sheet)

This international search report has not been established in respect of certain claims under Article 17(2)(a) for the following reasons:

1. ☐ Claims Nos.:
because they relate to subject matter not required to be searched by this Authority, namely:

2. ☐ Claims Nos.:
because they relate to parts of the international application that do not comply with the prescribed requirements to such an extent that no meaningful international search can be carried out, specifically:

3. ☐ Claims Nos.:
because they are dependent claims and are not drafted in accordance with the second and third sentences of Rule 6.4(a).

Box II Observations where unity of invention is lacking (Continuation of item 2 of first sheet)

This International Searching Authority found multiple inventions in this international application, as follows:

See the Supplemental Sheet

1. ☐ As all required additional search fees were timely paid by the applicant, this international search report covers all searchable claims.

2. ☐ As all searchable claims could be searched without effort justifying an additional fee, this Authority did not invite payment of any additional fee.

3. ☐ As only some of the required additional search fees were timely paid by the applicant, this international search report covers only those claims for which fees were paid, specifically claims Nos.:

4. ☒ No required additional search fees were timely paid by the applicant. Consequently, this international search report is restricted to the invention first mentioned in the claims; it is covered by claims Nos.:

1-3

Remark on Protest

☐ The additional search fees were accompanied by the applicant's protest.

☐ No protest accompanied the payment of additional search fees.

Continuation of Box III

The International Searching Authority has found that the international application contains multiple (groups of) inventions, as follows:

1. Claims 1-3

   Adding the functionality of a secure platform module, more particularly a TPM (Trusted Platform Module), to a host system that was originally supplied without a built-in security system (see the description, page 2, lines 17 to 23).

2. Claims 4-5 and 9

   Host system with a first authentication means and detachable security module with a second authentication means; authentication of the security module by a Trusted Platform Module.

3. Claims 6-7

   Host system with a first authentication means and detachable security module with a second authentication means; authentication of the host system by a SAM (Secure Authentication Means) that can be accommodated in or is embedded in the security module.

4. Claim 8

   Host system with a first authentication means and detachable security module with a second authentication means; automatic establishment of communication links between the detachable security module and the host system.

5. Claim 10

   Host system with a first authentication means and detachable security module with a second authentication means; encrypted communication link between the security module and the host system.

6. Claims 11-17

   Host system with a first authentication means and detachable security module with a second authentication means; validation of the security level (of a particular component) of the host system.

7. Claims 18-19

   Host system with a first authentication means and detachable security module with a second authentication means; extending the detachable security module by adding a flash memory card (on which are stored all the essential elements of the operating system).

8. Claims 20-22

   Host system with a first authentication means and detachable security module with a second authentication means; monitoring the security level by means of an optical and/or acoustic signal.

9. Claims 23-25

   Host system with a first authentication means and detachable security module with a second authentication means; connecting the detachable security module to a network (PCMCIA, ExpressCard, wireless network).

10. Claim 26

    Host system with a first authentication means and detachable security module with a second authentication means; facility for entering a PIN on the detachable security module.

11. Claim 27

    Host system with a first authentication means and detachable security module with a second authentication means; provision of a set of Boot ROM commands for execution in the host system by the detachable security module.

12. Claim 28

    Host system with a first authentication means and detachable security module with a second authentication means; checking the integrity of data transmission from the security module to the host system.

13. Claims 29-37

    Host system with a first authentication means and detachable security module with a second authentication means; monitoring the locking mechanism.

INTERNATIONAL SEARCH REPORT

Information on patent family members

International Application No
PCT/EP2005/006111

Patent document cited in search report	Publication date	Patent family member(s)	Publication date
EP 0440158 A	07-08-1991	DE 69127560 D1	16-10-1997
		DE 69127560 T2	23-04-1998
		US 5225664 A	06-07-1993

INTERNATIONALER RECHERCHENBERICHT

Internationales Aktenzeichen
PCT/EP2005/006111

A. KLASSIFIZIERUNG DES ANMELDUNGSGEGENSTANDES
G06F1/00

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

B. RECHERCHIERTE GEBIETE

Recherchierter Mindestprüfstoff (Klassifikationssystem und Klassifikationssymbole)
G06F

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.
Y	ST MICROELECTRONICS: "Trusted Platform Module (TPM)" Mai 2004 (2004-05), ST MICROELECTRONICS , XP002345888 das ganze Dokument	1-3
Y	TRUSTED COMPUTING GROUP, INCORPORATED: "TCG Specification Architecture Overview Specification Revision 1.2" 28. April 2004 (2004-04-28), TRUSTED COMPUTING GROUP, INCORPORATED , XP002352046 das ganze Dokument	1-3
A	EP 0 440 158 A (KABUSHIKI KAISHA TOSHIBA) 7. August 1991 (1991-08-07) siehe Formblatt PCT/ISA/206	1-3

☐ 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
2. November 2005	**23.01.2006**
Name und Postanschrift der Internationalen Recherchenbehörde 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	Bevollmächtigter Bediensteter Harms, C

Formblatt PCT/ISA/210 (Blatt 2) (Januar 2004)

INTERNATIONALER RECHERCHENBERICHT

Internationales Aktenzeichen
PCT/EP2005/006111

Feld II Bemerkungen zu den Ansprüchen, die sich als nicht recherchierbar erwiesen haben (Fortsetzung von Punkt 2 auf Blatt 1)

Gemäß Artikel 17(2)a) wurde aus folgenden Gründen für bestimmte Ansprüche kein Recherchenbericht erstellt:

1. ☐ Ansprüche Nr.
weil sie sich auf Gegenstände beziehen, zu deren Recherche die Behörde nicht verpflichtet ist, nämlich

2. ☐ Ansprüche Nr.
weil sie sich auf Teile der internationalen Anmeldung beziehen, die den vorgeschriebenen Anforderungen so wenig entsprechen, daß eine sinnvolle internationale Recherche nicht durchgeführt werden kann, nämlich

3. ☐ Ansprüche Nr.
weil es sich dabei um abhängige Ansprüche handelt, die nicht entsprechend Satz 2 und 3 der Regel 6.4 a) abgefaßt sind.

Feld III Bemerkungen bei mangelnder Einheitlichkeit der Erfindung (Fortsetzung von Punkt 3 auf Blatt 1)

Die internationale Recherchenbehörde hat festgestellt, daß diese internationale Anmeldung mehrere Erfindungen enthält:

siehe Zusatzblatt

1. ☐ Da der Anmelder alle erforderlichen zusätzlichen Recherchengebühren rechtzeitig entrichtet hat, erstreckt sich dieser internationale Recherchenbericht auf alle recherchierbaren Ansprüche.

2. ☐ Da für alle recherchierbaren Ansprüche die Recherche ohne einen Arbeitsaufwand durchgeführt werden konnte, der eine zusätzliche Recherchengebühr gerechtfertigt hätte, hat die Behörde nicht zur Zahlung einer solchen Gebühr aufgefordert.

3. ☐ Da der Anmelder nur einige der erforderlichen zusätzlichen Recherchengebühren rechtzeitig entrichtet hat, erstreckt sich dieser internationale Recherchenbericht nur auf die Ansprüche, für die Gebühren entrichtet worden sind, nämlich auf die Ansprüche Nr.

4. ☒ Der Anmelder hat die erforderlichen zusätzlichen Recherchengebühren nicht rechtzeitig entrichtet. Der internationale Recherchenbericht beschränkt sich daher auf die in den Ansprüchen zuerst erwähnte Erfindung; diese ist in folgenden Ansprüchen erfaßt:
1-3

Bemerkungen hinsichtlich eines Widerspruchs

☐ Die zusätzlichen Gebühren wurden vom Anmelder unter Widerspruch gezahlt.

☐ Die Zahlung zusätzlicher Recherchengebühren erfolgte ohne Widerspruch.

WEITERE ANGABEN PCT/ISA/ 210

Die internationale Recherchenbehörde hat festgestellt, dass diese internationale Anmeldung mehrere (Gruppen von) Erfindungen enthält, nämlich:

1. Ansprüche: 1-3

   Nachrüsten eines Host-Systems, das ursprünglich ohne eingebaute Sicherheitseinrichtung ausgeliefert wurde, mit der Funktionalität eines sicheren Plattformmoduls, insbesondere TPM (vgl. Beschreibung der Anmeldung Seite 2 Zeile 17-23)

   ---

2. Ansprüche: 4-5, 9

   Host System mit einem ersten Authentifizierungsmittel und abnehmbares Sicherheitsmodul mit einem zweiten Authentifizierungsmittel; Authentifizierung des Sicherheitsmoduls durch ein Trusted Platform Module

   ---

3. Ansprüche: 6-7

   Host System mit einem ersten Authentifizierungsmittel und abnehmbares Sicherheitsmodul mit einem zweiten Authentifizierungsmittel; Authentifizierung des Host-Sytems durch ein vom Sicherheitsmodul aufnehmbares oder eingebettetes SAM (secure authentication means)

   ---

4. Anspruch: 8

   Host System mit einem ersten Authentifizierungsmittel und abnehmbares Sicherheitsmodul mit einem zweiten Authentifizierungsmittel; automatischer Aufbau der Kommunikationsverbindungen zwischen dem abnehmbaren Sicherheitsmodul und dem Host-System

   ---

5. Anspruch: 10

   Host System mit einem ersten Authentifizierungsmittel und abnehmbares Sicherheitsmodul mit einem zweiten Authentifizierungsmittel; verschlüsselte Kommunikationsverbindung zwischen dem Sicherheitsmodul und dem Host-System

   ---

6. Ansprüche: 11-17

   Host System mit einem ersten Authentifizierungsmittel und abnehmbares Sicherheitsmodul mit einem zweiten Authentifizierungsmittel; Validierung der Sicherheitsstufe (einer bestimmten Komponente) des Host Systems

   ---

WEITERE ANGABEN PCT/ISA/ 210

7. Ansprüche: 18-19

Host System mit einem ersten Authentifizierungsmittel und abnehmbares Sicherheitsmodul mit einem zweiten Authentifizierungsmittel; Erweitern des abnehmbaren Sicherheitsmoduls um eine Flashspeicherkarte (auf der wesentliche Bestandteile des Betriebssystems abgelegt sind)

---

8. Ansprüche: 20-22

Host System mit einem ersten Authentifizierungsmittel und abnehmbares Sicherheitsmodul mit einem zweiten Authentifizierungsmittel; Überwachung der Sicherheitsstufe durch ein optisches und/oder akkustisches Signal

---

9. Ansprüche: 23-25

Host System mit einem ersten Authentifizierungsmittel und abnehmbares Sicherheitsmodul mit einem zweiten Authentifizierungsmittel; Anbindung des abnehmbaren Sicherheitsmoduls an ein Netzwerk (PCMCIA, ExpressCard, drahtloses Netzwerk)

---

10. Anspruch: 26

Host System mit einem ersten Authentifizierungsmittel und abnehmbares Sicherheitsmodul mit einem zweiten Authentifizierungsmittel; PIN-Eingabemöglichkeit auf dem abnehmbaren Sicherheitsmodul

---

11. Anspruch: 27

Host System mit einem ersten Authentifizierungsmittel und abnehmbares Sicherheitsmodul mit einem zweiten Authentifizierungsmittel; Bereitstellung von einem Satz von Boot-ROM-Befehlen für die Ausführung auf dem Host-System durch das abnehmbare Sicherheitsmodul

---

12. Anspruch: 28

Host System mit einem ersten Authentifizierungsmittel und abnehmbares Sicherheitsmodul mit einem zweiten Authentifizierungsmittel; Überprüfung der Integrität der Datenübertragung vom Sicherheitsmodul auf das Host-System

---

13. Ansprüche: 29-37

WEITERE ANGABEN PCT/ISA/ 210

Host System mit einem ersten Authentifizierungsmittel und abnehmbares Sicherheitsmodul mit einem zweiten Authentifizierungsmittel; Überwachung des Verriegelungsmechanismus

---

INTERNATIONALER RECHERCHENBERICHT

Angaben zu Veröffentlichungen, die derselben Patentfamilie gehören

Internationales Aktenzeichen
PCT/EP2005/006111

Im Recherchenbericht angeführtes Patentdokument	Datum der Veröffentlichung	Mitglied(er) der Patentfamilie	Datum der Veröffentlichung
EP 0440158 A	07-08-1991	DE 69127560 D1	16-10-1997
		DE 69127560 T2	23-04-1998
		US 5225664 A	06-07-1993