

(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
13. Oktober 2011 (13.10.2011)



(10) Internationale Veröffentlichungsnummer
WO 2011/124335 A1

(51) Internationale Patentklassifikation:
H04L 9/32 (2006.01)

(21) Internationales Aktenzeichen: PCT/EP2011/001527

(22) Internationales Anmeldedatum:
25. März 2011 (25.03.2011)

(25) Einreichungssprache: Deutsch

(26) Veröffentlichungssprache: Deutsch

(30) Angaben zur Priorität:
10 2010 013 200.4 29. März 2010 (29.03.2010) DE

(71) Anmelder (für alle Bestimmungsstaaten mit Ausnahme
von US): **GIESECKE & DEVRIENT GMBH** [DE/DE];
Patent- und Lizenzabteilung, Prinzregentenstrasse 159,
81677 München (DE).

(72) Erfinder; und

(75) Erfinder/Anmelder (nur für US): **WEIß, Dieter**
[DE/DE]; Königssee-Str. 50, 81825 München (DE). **FIN-
KENZELLER, Klaus** [DE/DE]; Ahornstrasse 19, 85774
Unterföhring (DE). **GAWLAS, Florian** [DE/DE]; Main-
zer Strasse 7a, 80804 München (DE). **MEISTER, Gisela**
[DE/DE]; Stademannstrasse 11, 81737 München (DE).
EICHHOLZ, Jan [DE/DE]; Schweidnitzer Strasse 3,
80997 München (DE).

(74) Gemeinsamer Vertreter: **GIESECKE & DEVRIENT
GMBH**; Prinzregentenstrasse 159, 81677 München (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, CL, CN, CO, CR, CU, CZ, DE, DK, DM,
DO, DZ, EC, EE, EG, ES, FI, GB, GD, GE, GH, GM,
GT, HN, HR, HU, ID, IL, IN, IS, JP, KE, KG, KM, KN,
KP, KR, KZ, LA, LC, LK, LR, LS, LT, LU, LY, MA,
MD, ME, MG, MK, MN, MW, MX, MY, MZ, NA, NG,
NI, NO, NZ, OM, PE, PG, PH, PL, PT, RO, RS, RU, SC,
SD, SE, SG, SK, SL, SM, ST, SV, SY, TH, TJ, TM, TN,
TR, TT, TZ, UA, UG, US, UZ, VC, VN, ZA, ZM, ZW.

(84) Bestimmungsstaaten (soweit nicht anders angegeben, für
jede verfügbare regionale Schutzrechtsart): ARIPO (BW,
GH, GM, KE, LR, LS, MW, MZ, NA, SD, SL, SZ, TZ,
UG, ZM, ZW), eurasisches (AM, AZ, BY, KG, KZ, MD,
RU, TJ, TM), europäisches (AL, AT, BE, BG, CH, CY,
CZ, DE, DK, EE, ES, FI, FR, GB, GR, HR, HU, IE, IS,
IT, LT, LU, LV, MC, MK, MT, NL, NO, PL, PT, RO,
RS, SE, SI, SK, SM, TR), OAPI (BF, BJ, CF, CG, CI,
CM, GA, GN, GQ, GW, ML, MR, NE, SN, TD, TG).

Erklärungen gemäß Regel 4.17:

— hinsichtlich der Berechtigung des Anmelders, ein Patent
zu beantragen und zu erhalten (Regel 4.17 Ziffer ii)

[Fortsetzung auf der nächsten Seite]

(54) Title: SYSTEM FOR ENTERING A SECRET

(54) Bezeichnung : SYSTEM ZUM EINGEBEN EINES GEHEIMNISSES

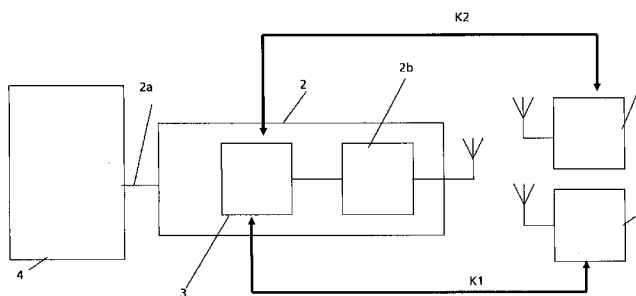


Fig. 1

(57) Abstract: The invention relates to a method and a system for entering a secret for authenticating a user for carrying out an action on a data processing device (4), comprising a trustworthy entity (2) provided with a security module (3), interfaces for data communication (2a, 2b), wherein the trustworthy entity (2) is connected to the data processing device (4) via an interface (2a) in an electrically conductive manner, and an entry unit (5) for entering the secret by the user using a contactless interface for contactless communication with the security module (3) of the trustworthy entity (2), the secret being transmitted to the trustworthy entity (2) in a contactless manner.

(57) Zusammenfassung: Die Erfindung betrifft ein Verfahren und ein System zum Eingeben eines Geheimnisses zum Authentifizieren eines Benutzers für eine Aktion an einem Datenverarbeitungsgerät (4) aufweisend eine vertrauenswürdige Instanz (2) ausgestattet mit einem Sicherheitsmodul (3), Schnittstellen zur Datenkommunikation (2a, 2b), wobei die vertrauenswürdige Instanz (2) über eine Schnittstelle (2a) mit der Datenverarbeitungsgerät (4) elektrisch leitend verbunden ist und eine Eingabeeinheit (5) zum Eingeben des Geheimnisses durch den Benutzer mit einer kontaktlosen Schnittstelle zum kontaktlosen Kommunizieren mit dem Sicherheitsmodul (3) der vertrauenswürdigen Instanz (2) das Geheimnis kontaktlos an die vertrauenswürdige Instanz (2) übertragen wird.



WO 2011/124335 A1



-
- hinsichtlich der Berechtigung des Anmelders, die Priorität einer früheren Anmeldung zu beanspruchen (Regel 4.17 Ziffer iii) — vor Ablauf der für Änderungen der Ansprüche geltenden Frist; Veröffentlichung wird wiederholt, falls Änderungen eingehen (Regel 48 Absatz 2 Buchstabe h)

Veröffentlicht:

- mit internationalem Recherchenbericht (Artikel 21 Absatz 3)

S y s t e m z u m E i n g e b e n e i n e s G e h e i m n i s -
s e s

- 5 Die Erfindung betrifft ein System und ein Verfahren zum Eingeben eines Geheimnisses zum Authentifizieren eines Benutzers für eine Aktion an einem Datenverarbeitungsgerät.

10 Mit Geheimnis ist hierbei eine geheime Information gemeint, mit der sich ein Benutzer an einem Datenverarbeitungsgerät, zum Beispiel einem Notebook, einem PC oder ähnlichem, authentifiziert, um eine Aktion durchführen zu können. Ein Geheimnis ist insbesondere eine PIN, ein Passwort, eine vertrauenswürdige Information.

- 15 Unter einer Aktion ist beispielsweise das Aufrufen und /oder Bereitstellen einer Anwendung und/oder das Durchführen einer Transaktion mit Hilfe des Datenverarbeitungsgeräts zu verstehen, beispielsweise eine Bezahltransaktionen, das Anmelden an einen entfernten Server eines Diensteanbieters und der gleichen mehr zu verstehen.

20 Um derartige Aktionen durchführen zu können, wird der Benutzer durch das Datenverarbeitungsgerät aufgefordert, ein Geheimnis am Datenverarbeitungsgerät einzugeben. Da es sich bei dem Gerät um ein nicht vertrauenswürdiges Gerät handelt, ist das direkte Eingeben des Geheimnisses über eine
25 am Datenverarbeitungsgerät vorhandene Eingabevorrichtung nicht sicher.

Beispielsweise kann Schadsoftware, beispielsweise ein Virusprogramm, ein Trojaner und/oder ein sogenannter Wurm, auf dem Rechner installiert sein. Die Schadsoftware späht dann das Geheimnis des Benutzers nach dessen
30 Eingeben aus. In der Folge kann durch die Schadsoftware das Geheimnis benutzt werden, um ohne das Wissen des Benutzers bzw. dessen Zustim-

- 2 -

mung weitere Authentifizierungen vorzunehmen. Dies führt in der Regel zu vom Benutzer ungewollten Aktionen.

Es ist daher Aufgabe dieser Anmeldung ein einfaches und sicheres Authentifizieren eines Benutzers durch Eingeben eines Geheimnisses zu gewährleisten. Weiterhin soll auch eine sichere Anzeige von Informationen bezüglich der Aktion ermöglicht werden.

Die Aufgabe wird mit den in den unabhängig nebengeordneten Ansprüchen beschriebenen Maßnahmen gelöst.

Die Aufgabe wird insbesondere durch ein System zum Eingeben eines Geheimnisses zum Authentifizieren eines Benutzers für eine Aktion an einem Datenverarbeitungsgerät gelöst. Das System beinhaltet eine vertrauenswürdige Instanz, ausgestattet mit einem Sicherheitsmodul, Schnittstellen zur Datenkommunikation, wobei die vertrauenswürdige Instanz über eine Schnittstelle mit dem Datenverarbeitungsgerät elektrisch leitend verbunden ist. Weiterhin weist das System eine Eingabeeinheit zum Eingeben des Geheimnisses durch den Benutzer auf, wobei die Eingabeeinheit mit einer kontaktlosen Schnittstelle zum kontaktlosen Kommunizieren mit dem Sicherheitsmodul der vertrauenswürdigen Instanz ausgestattet ist, sodass das Geheimnis kontaktlos an die vertrauenswürdige Instanz übertragen wird. Dabei wird zur Kommunikation zwischen der Eingabeeinheit und dem Sicherheitsmodul der vertrauenswürdigen Instanz ein direkter Kommunikationskanal aufgebaut, wobei dieser Kommunikationskanal vom Datenverarbeitungsgerät unabhängig ist.

Bevorzugt ist der der Kommunikationskanal ein erster kryptographisch gesicherter Kanal basierend auf einer kryptographischen Information.

Bevorzugt ist eine Datenträgereinheit im System vorgesehen. Diese Datenträgereinheit, insbesondere eine Chipkarte, Smart Card, Token, eID Token, elektronisches Identitätsdokument mit auf einem Chip gespeicherten maschinenlesbaren Identifikationsdaten des Benutzers, enthält ebenfalls das Geheimnis in einem geschützten Bereich. Die Datenträgereinheit weist weiterhin eine kontaktlose Schnittstelle zum kontaktlosen Kommunizieren mit dem Sicherheitsmodul der Vertrauenswürdige Instanz auf, wobei zur Kommunikation zwischen der Datenträgereinheit und dem Sicherheitsmodul der Vertrauenswürdige Instanz ein zweiter kryptographisch gesicherter Kanal basierend auf einer zweiten kryptographischen Information aufgebaut wird, sodass zum Authentifizieren des Benutzers ein Vergleich zwischen eingegebenem Geheimnis und in der Datenträgereinheit enthaltenem Geheimnis in der Vertrauenswürdige Instanz durchgeführt werden kann.

Die vertrauenswürdige Instanz ist beispielsweise ein Smart Reader oder Smart Terminal und ist insbesondere ein kontaktlos kommunizierendes Lesegerät, wie z.B. RFID-Lesegerät bzw. sog. Terminal, welches mit der Eingabeeinheit und/oder Datenträgereinheiten kontaktlos über eine entsprechende NFC und/oder Bluetooth Schnittstelle kommunizieren kann. Das in der vertrauenswürdigen Instanz bzw. Terminals enthaltene Sicherheitselement bzw. Sicherheitsmodul ist zum Beispiel ein Secure-Element bzw. ein SAM-Modul (SAM = Secure Application Module). Als ein Sicherheitsmodul wird bevorzugt ein Smart Card Chip verwendet. Die vertrauenswürdige Instanz ist dabei beispielsweise eine Lesegeräteinheit, die im Datenverarbeitungsgerät integriert ist. Das Sicherheitsmodul innerhalb der vertrauenswürdigen Instanz kann beispielsweise eine SIM Chipkarte sein. Die vertrauenswürdige Instanz kann auch mittels einer USB Schnittstelle an das Datenverarbeitungsgerät angeschlossen werden.

Dieser Smart Reader verfügt allerdings selbst über keine sichere Möglichkeit ein Geheimnis für das Sicherheitsmodul und/ oder eine Datenträgereinheit einzugeben. Zur Freigabe von Aktionen, die auf dem Datenverarbeitungsgerät ausgeführt oder initialisiert werden sollen, wird in dem erfindungsgemä-
5 ßen System eine Eingabeeinheit zum Eingeben des Geheimnisses vorgesehen. Diese Eingabeeinheit ist mit einer kontaktlosen Schnittstelle ausgestattet. Zum Beispiel ist die Eingabeeinheit eine separate NFC-Tastatur, eine Bluetooth-Tastatur oder lediglich ein Ziffernblock zur Drahtloskommunika-
10 tion ausschließlich mit dem Sicherheitsmodul der vertrauenswürdigen Instanz.

Dies hat den Vorteil, dass das Datenverarbeitungsgerät, z.B. ein Notebook, nicht direkt auf diese Eingabeeinheit zugreifen kann. Lediglich der Smart
15 Reader kann auf die Eingabeeinheit zugreifen. Ziel ist, dass der Smart Reader eine Abfrage des Geheimnisses im Bedarfsfall, zum Beispiel auf Anfrage des Datenverarbeitungsgeräts initiiert. Das über die Eingabeeinheit eingegebene Geheimnis, insbesondere eine PIN, wird nur an den Smart Reader übertragen. Ein Zugriff auf das Geheimnis ist vom Notebook aus nicht möglich.
20 Somit ist der Kommunikationskanal zwischen Eingabeeinheit und vertrauenswürdiger Instanz unabhängig vom Datenverarbeitungsgerät. Somit verlässt das Geheimnis nie den sicheren Bereich, der aus Smart Reader, Sicherheitsmodul, Datenträgereinheit und Eingabeeinheit besteht. Ist der direkte Kommunikationskanal verschlüsselt, ist es nicht möglich, mittels einer
25 Schadsoftware das eingegebene Geheimnis auszuspionieren.

Die Kommunikation zwischen den Einheiten und dem Smart Reader erfolgt direkt und ohne Zwischeneinheiten. Die Kommunikation ist lokal zwischen

beiden Datenträgereinheiten und auf die Reichweiten der Kontaktlosschnittstellen beschränkt.

5 In einer besonders geeigneten Ausführungsform handelt die Eingabeeinheit mit der vertrauenswürdigen Instanz einen ersten kryptographischen Schlüssel aus, über den der erste kryptographisch gesicherte Kanal aufgebaut wird. Die Datenträgereinheit handelt mit der vertrauenswürdigen Instanz einen zweiten kryptographischen Schlüssel aus, über den der zweite kryptographisch gesicherte Kanal aufgebaut wird.

10

Um zu verhindern, dass über eine fremde Kontaktlosschnittstelle die Kommunikation zwischen Eingabeeinheit, Datenträgereinheit und Smart Reader abgehört werden kann, ist durch diese Ausführung sicher gestellt, dass die Eingabeeinheit mit der Vertrauenswürdigen Instanz gekoppelt ist, sodass die
15 Eingabeeinheit nur Kommandos von dem zugeordneten Smart Reader verarbeitet.

Dies kann beispielsweise über eine eindeutige Kennung in der Installationsphase vom Sicherheitsmodul der vertrauenswürdigen Instanz an die Eingabeeinheit gelöst werden, wobei die Kennung in einem Speicherbereich der
20 Eingabeeinheit abgelegt wird. Durch zusätzlichen Austausch von Schlüsseln wird die Kommunikation zwischen Eingabeeinheit und Smart Reader abhörsicher.

25 Optional kann auch anstatt einer NFC Kommunikation ein Bluetooth Kommunikationsprotokoll zwischen Smart Reader und Eingabeeinheit verwendet werden. In diesem Fall ist ein Pairing zwischen Eingabeeinheit und Smart Reader zwingend erforderlich, da anderenfalls die Kommunikation durch andere Bluetooth Geräte initiiert und abgehört werden könnte.

- Zum Aushandeln der Schlüssel können wiederum aus dem Stand der Technik bekannte Verfahren eingesetzt werden. Beispielsweise kann der Diffie-Hellmann-Schlüsselaustausch zur Erzeugung des ersten bzw. zweiten kryptographischen Schlüssels verwendet werden. Die Kanäle können über sogenanntes Secure Messaging aufgebaut wird. Das Secure Messaging erfolgt vorzugsweise basierend auf einem passwortbasierten Transportprotokoll und besonders bevorzugt basierend auf dem PACE-Protokoll.
- 5
- 10 Weiterhin kann auch ein sicheres Display über die NFC-Schnittstelle angebunden werden, oder mit der Eingabeeinheit kombiniert werden. Eine derartige Anzeigevorrichtung dient dann zur Anzeige von Informationen die beispielsweise die Aktion betreffen. Die Information ist insbesondere ein von der vertrauenswürdigen Instanz generiertes dynamisches Passwort. Alternativ können Transaktionsdaten angezeigt werden.
- 15
- Im Erfindungsgedanken ist ebenfalls ein Verfahren zum Eingeben eines Geheimnisses in dem System enthalten. Die Verfahrensschritte sind:
- Betreiben der vertrauenswürdigen Instanz an dem Datenverarbeitungsgerät
- 20 über eine Datenkommunikationsschnittstelle; Aufbau des direkten Kommunikationskanals über die Kontaktlosschnittstelle zwischen einer Eingabeeinheit und dem Sicherheitsmodul der vertrauenswürdigen Instanz; Eingeben des Geheimnisses an der Eingabeeinheit durch den Benutzer; Übertragen des Geheimnisses von der Eingabeeinheit über Kommunikationskanal; Verifizieren des Geheimnisses in der vertrauenswürdigen Instanz zum Freigeben einer Aktion im Datenverarbeitungsgerät.
- 25

Ausführungsbeispiele der Erfindung werden nachfolgend anhand der beige-fügten Figuren detailliert beschrieben.

Es zeigen:

Fig. 1 eine Ausführungsform eines erfindungsgemäßen Systems zum Eingeben eines Geheimnisses;

5

Fig. 2 ein erfindungsgemäßes Ablaufdiagramm für die sichere Eingabe des Geheimnisses

Fig. 1 zeigt eine erste Ausführungsform des erfindungsgemäßen Systems, bei dem ein Smart Reader 2 über eine kontaktbehaftete Schnittstelle 2a mit einem Datenverarbeitungsgerät 4 elektrisch leitend verbunden ist. Der Smart Reader 2 beinhaltet ein Sicherheitsmodul 3 und eine NFC-Schnittstelle 2b. Das System der Figur 1 beinhaltet weiterhin eine NFC-Tastatur 5 oder ein NFC-fähiges Mobiltelefon und eine Datenträgereinheit 1. Der Smart Reader 2 ist dabei fest in dem Notebook integriert oder mittels einer USB-Schnittstelle mit dem Notebook verbunden.

Insbesondere kann die erste Datenträgereinheit 1 beispielsweise ein Token, eine Smart Card oder ein eID Token sein. Die Datenträgereinheit 1 und die NFC-Tastatur 5 bzw. das NFC-fähige Mobiltelefon kommunizieren kontaktlos über die NFC-Schnittstelle 2b mit dem Sicherheitsmodul 3 des Smart Readers 2.

Ziel ist es nunmehr, das Eingeben eines Geheimnisses sicher auszugestalten. Dazu wird eine kryptographische Information A, zum Beispiel eine eindeutige Kennung, in der NFC-Tastatur 5 hinterlegt. Eine kryptographische Information B, zum Beispiel eine andere eindeutige Kennung wird in der Datenträgereinheit 1 hinterlegt. Mit diesen Informationen A, B wird zu einem späteren Zeitpunkt jeweils ein Kanal K1, K2 aufgebaut. Um dies zu errei-

- chen, handelt die NFC-Tastatur 5 bzw. das NFC-fähige Mobiltelefon mit dem Smart Reader 2 im Rahmen des Aufbaus eines ersten kryptographisch gesicherten Kanals K1 einen symmetrischen Sitzungsschlüssel A aus. Es können dabei aus dem Stand der Technik bekannte Verfahren zum Aushandeln des Schlüssels verwendet werden (z.B. ein Diffie-Hellmann-Schlüsselaustausch), insbesondere basierend auf Secure Messaging. Im Besonderen kann dabei ein passwortbasiertes oder asymmetrisches Transportprotokoll (z.B. das aus dem Stand der Technik bekannte PACE-Protokoll) verwendet werden. Es wird somit ein Schlüssel A zwischen Smart Reader 2 und NFC-Tastatur 5 bzw. das NFC-fähige Mobiltelefon generiert. In analoger Weise wird mit dem gleichen Mechanismus im Rahmen des Aufbaus eines zweiten sicheren Kanals K2 zwischen der NFC-Smart Card 1 und dem Smart Reader 2 ein zweiter Sitzungsschlüssel B generiert. In einer bevorzugten Variante wird bei der Generierung der entsprechenden Schlüssel eine Kartenkennung der Smart card 1 verwendet, welche nicht der Identitätskennung der Karten entspricht. Vorzugsweise wird eine sog. Restricted ID eingesetzt. Die Verwendung einer Restricted ID innerhalb von entsprechenden Authentisierungsprotokollen ist wiederum bekannt.
- 20 In einer Nutzungsphase wird der Kanal K1 dazu verwendet, ein an der NFC-Tastatur 5 eingegebenes Geheimnis an den Smart Reader 2 zu übertragen. Dieser Kanal ist abhörsicher und kann von keinem anderen NFC-fähigen Gerät verwendet werden. In gleicher Weise wird Kanal K2 dazu verwendet, das in der Smart Card 1 hinterlegte Geheimnis an den Smart Reader 2 zu übertragen. Im Sicherheitsmodul 3 werden beide übertragenen Geheimnisse miteinander verglichen. Alternativ wird das eingegebene Geheimnis von dem Smart Reader 2 an die Datenträgereinheit 1 über den sicheren Kanal K2 übertragen und in der Datenträgereinheit 1 der Vergleich durchgeführt. Das Vergleichsergebnis wird anschließend an den Smart Reader 2 gemeldet.

In Abhängigkeit des Vergleichs erfolgt die Freigabe einer Aktion an dem Datenverarbeitungsgerät 4. Dies kann beispielsweise eine Zugriffsberechtigung für einen sicheren Speicherbereich oder aber das Aufrufen eines Diensteanbieters eines eService sein.

Die NFC-Tastatur 5 bzw. das NFC-fähige Mobiltelefon umfasst weiterhin ein vertrauenswürdigen Display. Dann kann ein dynamisches Passwort am Display des Mobiles angezeigt werden und für den weiteren Ablauf der Authentifizierung des Benutzers genutzt werden. Das für das System lokal zusätzlich erforderliche Geheimnis, zum Beispiel bei Nutzung eines „unbekannten“ Datenverarbeitungsgeräts, z.B. einem Geldautomat, bei Nutzung eines fremden PC, bei Anmeldung am Netz, kann durch Pairing von NFC-Tastatur 5 bzw. dem NFC-fähigen Mobiltelefon und dem Smart Reader 2 über ein Secure Messaging gesichert eingegeben werden.

In Figur 2 ist ein möglicher Ablauf zur sicheren Eingabe eines Geheimnisses in dem erfindungsgemäßen System gezeigt.

Hierzu sendet das Datenverarbeitungsgerät 4 im Schritt S1 für die Durchführung einer Aktion eine Anfrage zur Authentifizierung eines Benutzers für diese Aktion, zum Beispiel für eine Bezahltransaktion, die Anmeldung an einen eService etc. Im Schritt S2 werden Informationen die Aktion betreffend auf dem Display der NFC-Tastatur 5 bzw. dem NFC-fähigen Mobiltelefon angezeigt. Die Übertragung dieser Informationen erfolgt über den gesicherten Kanal K1. Dieser Schritt entfällt bei Ausgestaltungen ohne Display. Im Schritt S3 fordert der Smart Reader 2 über den gesicherten Kanal K2 das Geheimnis an, mit welchem der Benutzer sich für die Aktion authentifiziert. Im Schritt S4 wird das durch den Benutzer an der NFC-Tastatur 5 bzw. dem

NFC-fähige Mobiltelefon eingegebene Geheimnis über den sicheren Kanal K2 drahtlos an den Smart Reader 2 übertragen.

Im Schritt S5 wird das eingegebene Geheimnis oder eine eindeutige Information, z.B. Hashwert etc. vom Smart Reader 2 an die Datenträgereinheit 1 über den sicheren Kanal K2 übertragen mit der Aufforderung, einen Vergleich zwischen eingegebenem Geheimnis und auf der Datenträgereinheit 1 abgelegtem Geheimnis durchzuführen und das Ergebnis an den Smart Reader 2 zurückzumelden.

10

In einer nicht dargestellten Variante sendet die Datenträgereinheit 1 das abgelegte Geheimnis auf Anforderung von dem Smart Reader 2 zum Zweck des Vergleichs an den Smart Reader 2 über den sicheren Kanal K2.

15 Im Schritt S6 und in Abhängigkeit der erfolgreichen Authentifizierung des Benutzers durch Eingeben des richtigen Geheimnisses fordert der Smart Reader 2 die Datenträgereinheit 1 zur Ausfertigung eines Aktionszertifikats aus. Dieses Zertifikat wird im Folgeschritt S7 von der Datenträgereinheit 1 zum Smart Reader 2 über den Kanal K2 übertragen. Das Zertifikat wird im
20 Folgeschritt S8 an das Datenverarbeitungsgerät 4 übertragen, wodurch die geforderte Aktion im Datenverarbeitungsgerät 4 durchgeführt werden kann.

Eine Aktion kann neben den bereits erwähnten Beispielen auch das Aufrufen sogenannter eServices sein. Unter eServices sind alle Dienste und Aktivitäten
25 zusammengefasst, die mittels Computern erstellt und über elektronische Medien, wie das Internet, interaktiv angeboten und ausgeführt werden, beispielsweise Informations- und Bildungsdienste handeln, Beschaffungs-, Handels- und Bestelldienste, kulturelle und administrative Dienste, Verbes-

serung der Dienstleistungen des Marketings, des Produktes oder der Kundenbeziehung, elektronische Beratung wie E-Consult oder E-Advising.

Bevorzugt handelt es sich bei der Anwendung um sicherheitsrelevante Dienste, produktionstechnische, wissenschaftliche oder logistische Dienste.

- 5 E-Dienste werden in Zukunft in vielen weiteren Anwendungen eingesetzt.

B e z u g s z e i c h e n l i s t e

- | | |
|------|---|
| 1 | Datenträgereinheit |
| 2 | Smart Reader, vertrauenswürdige Instanz |
| 5 2a | Kontaktbehaftete Schnittstelle |
| 2b | Kontaktlose Schnittstelle |
| 3 | Sicherheitsmodul, SAM-Modul |
| 4 | Datenverarbeitungsgerät, Notebook |
| 5 | Eingabeeinheit (mit Display) |

P a t e n t a n s p r ü c h e

1. System zum Eingeben eines Geheimnisses zum Authentifizieren eines Benutzers für eine Aktion an einem Datenverarbeitungsgerät (4) aufweisend:
- eine vertrauenswürdige Instanz (2) ausgestattet mit einem Sicherheitsmodul (3), Schnittstellen zur Datenkommunikation (2a, 2b), wobei die vertrauenswürdige Instanz (2) über eine Schnittstelle (2a) mit dem Datenverarbeitungsgerät (4) elektrisch leitend verbunden ist;
 - eine Eingabeeinheit (5) zum Eingeben des Geheimnisses durch den Benutzer mit einer kontaktlosen Schnittstelle zum kontaktlosen Kommunizieren mit dem Sicherheitsmodul (3) der vertrauenswürdigen Instanz (2), wobei das Geheimnis kontaktlos an die vertrauenswürdige Instanz (2) übertragen wird;
 - wobei zur Kommunikation zwischen der Eingabeeinheit (5) und dem Sicherheitsmodul (3) der vertrauenswürdigen Instanz (2) ein direkter Kommunikationskanal (K1) aufgebaut wird und dieser Kommunikationskanal (K1) vom Datenverarbeitungsgerät (4) unabhängig ist.
2. System nach Anspruch 1, dadurch gekennzeichnet, dass der Kommunikationskanal (K1) ein erster kryptographisch gesicherter Kanal (K1) basierend auf einer kryptographischen Information (A) ist.
3. System nach Anspruch 1 oder 2, dadurch gekennzeichnet, dass eine Datenträgereinheit (1) im System vorgesehen ist und die Datenträgereinheit(1):
- das Geheimnis enthält;
 - eine kontaktlose Schnittstelle zum kontaktlosen Kommunizieren mit dem Sicherheitsmodul (3) der vertrauenswürdigen Instanz (2) aufweist;

- wobei zur Kommunikation zwischen der Datenträgereinheit (1) und dem Sicherheitsmodul (3) der vertrauenswürdigen Instanz (2) ein zweiter kryptographisch gesicherter Kanal (K2) basierend auf einer zweiten kryptographischen Information (B) aufgebaut wird, sodass zum Authentifizieren des Benutzers ein Vergleich zwischen eingegebenem Geheimnis und in der Datenträgereinheit (1) enthaltenem Geheimnis durchgeführt werden kann und /oder ein Zertifikat über die Aktion von der Datenträgereinheit (1) ausgestellt werden kann.
- 5
- 10 4. System nach Anspruch 1 bis 3, dadurch gekennzeichnet, dass die Eingabeeinheit (5) mit der vertrauenswürdigen Instanz (2) einen ersten kryptographischen Schlüssel (A) aushandelt, über den der erste kryptographisch gesicherte Kanal (K1) aufgebaut wird, und die Datenträgereinheit (1) mit der vertrauenswürdigen Instanz (2) einen zweiten
- 15 kryptographischen Schlüssel (B) aushandelt, über den der zweite kryptographisch gesicherte Kanal (K2) aufgebaut wird.
5. System nach einem der vorhergehenden Ansprüche, dadurch gekennzeichnet, dass die kryptographische Information (A) eine eindeutige
- 20 Kennung ist, die nach einem Initialisierungsschritt in der Eingabeeinheit (5) abgelegt ist.
6. System nach einem der vorhergehenden Ansprüche, dadurch gekennzeichnet, dass die Eingabeeinheit (1) weiterhin eine Anzeigevorrichtung zur Anzeige von Informationen die Aktion betreffend, aufweist.
- 25
7. System nach Anspruch 6, dadurch gekennzeichnet, dass die Information ein von der vertrauenswürdigen Instanz (2) generiertes dynamisches Passwort ist.

8. System nach einem der vorhergehenden Ansprüche, dadurch gekennzeichnet, dass die Eingabeeinheit eine Tastatur oder ein Ziffernblock ist.
- 5
9. System nach einem der Ansprüche 3 bis 8, dadurch gekennzeichnet, dass die Datenträgereinheit (1) eine Chipkarte, ein Token und/oder ein elektronisches Identitätsdokument ist.
- 10
10. System nach einem der vorhergehenden Ansprüche, dadurch gekennzeichnet, dass die kontaktlose Schnittstelle (2b) eine NFC-Schnittstelle und /oder eine Bluetooth-Schnittstelle ist.
11. Verfahren zum Eingeben eines Geheimnisses in einem System gemäß einem der Ansprüche 1 bis 10 mit den Verfahrensschritten:
- 15
- Betreiben der vertrauenswürdigen Instanz (2) an dem Datenverarbeitungsgerät (4) über eine Datenkommunikationsschnittstelle (2a);
 - Aufbau des direkten Kommunikationskanals (K1) über die

20

 - Kontaktlosschnittstelle (2b) zwischen einer Eingabeeinheit (5) und dem Sicherheitsmodul (3) der vertrauenswürdigen Instanz (2);
 - Eingeben des Geheimnisses an der Eingabeeinheit (5) durch den Benutzer;
 - Übertragen des Geheimnisses von der Eingabeeinheit (5) über

25

 - Kommunikationskanal (K1)
 - Verifizieren des Geheimnisses in der vertrauenswürdigen Instanz (2) zum Freigeben einer Aktion im Datenverarbeitungsgerät (4).

12. Verfahren gemäß Anspruch 11, dadurch gekennzeichnet, dass die Eingabeeinheit eine Anzeigevorrichtung aufweist, und die Anzeigevorrichtung ein dynamisch generiertes Passwort anzeigt.
- 5 13. Verfahren gemäß Anspruch 12, dadurch gekennzeichnet, dass eine Datenträgereinheit (1) dazu vorgesehen ist, über einen zweiten kryptographisch gesicherten Kanal (K2) das eingegebene Geheimnis zu verifizieren und/oder ein Zertifikat über die Aktion auszustellen.
- 10 14. Verfahren gemäß Anspruch 12, dadurch gekennzeichnet, dass eine Datenträgereinheit (1) dazu vorgesehen ist, über einen zweiten kryptographisch gesicherten Kanal (K2) das in der Datenträgereinheit (1) enthaltene Geheimnis an die Lesegeräteinheit (2) zu übertragen.

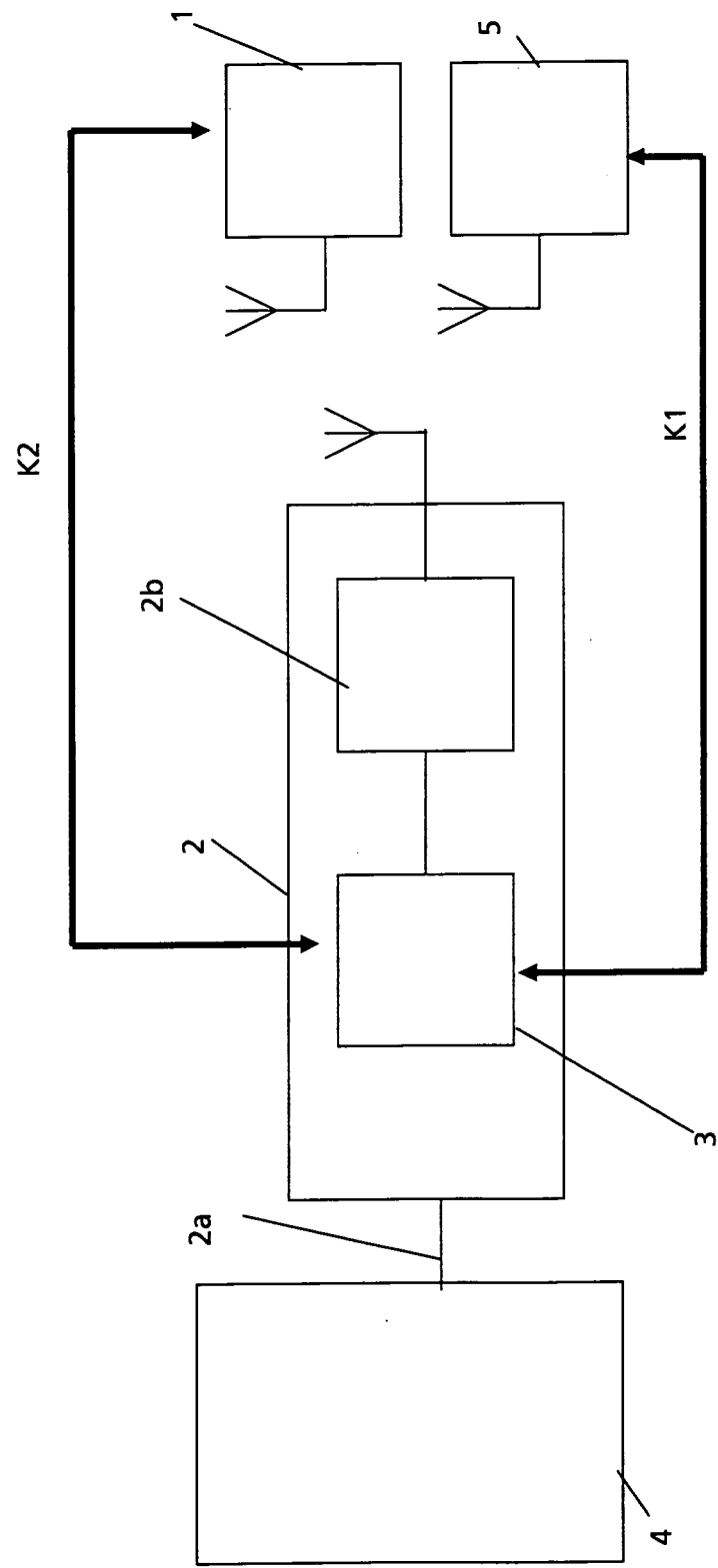


Fig. 1

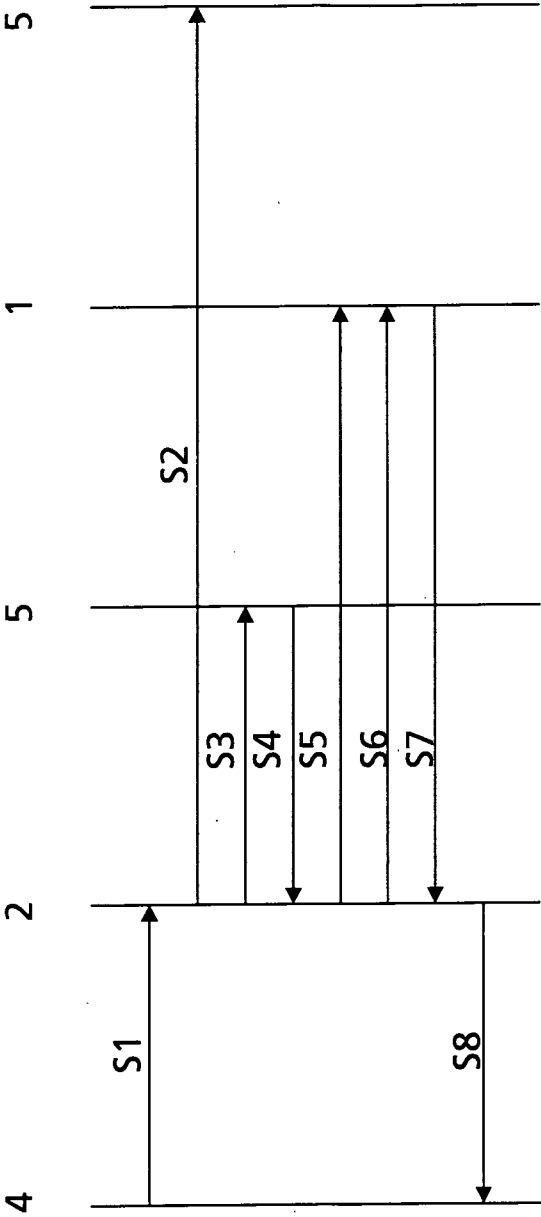


Fig. 2

INTERNATIONAL SEARCH REPORT

International application No

PCT/EP2011/001527

A. CLASSIFICATION OF SUBJECT MATTER

INV. H04L9/32

ADD.

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

B. FIELDS SEARCHED

Minimum documentation searched (classification system followed by classification symbols)

H04L G06F 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)

EPO-Internal, WPI Data

C. DOCUMENTS CONSIDERED TO BE RELEVANT

Category*	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
X	WO 2007/003429 A1 (GIESECKE & DEVRIENT GMBH [DE]; FINKENZELLER KLAUS [DE]; GAWLAS FLORIAN) 11 January 2007 (2007-01-11) page 1, line 20 - page 2, line 28 page 5, line 11 - line 21 page 7, line 10 - page 9, line 25 page 10, line 25 - page 11, line 23 page 14, line 15 - line 25 page 15, line 19 - page 16, line 7 page 17, line 10 - page 19, line 13 -----	1-14
A	WO 2004/090800 A2 (GIESECKE & DEVRIENT GMBH [DE]; GRAF HANS [DE]; FINKENZELLER KLAUS [DE]) 21 October 2004 (2004-10-21) page 2 - page 3 page 7 - page 9 page 11 - page 12 ----- -/-	1-14



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

19 August 2011

Date of mailing of the international search report

29/08/2011

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

Apostolescu, Radu

INTERNATIONAL SEARCH REPORT

International application No

PCT/EP2011/001527

C(Continuation). DOCUMENTS CONSIDERED TO BE RELEVANT		
Category*	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
A	WO 2007/017288 A2 (GIESECKE & DEVRIENT GMBH [DE]; MEISTER GISELA [DE]; URMANN JENS [DE]) 15 February 2007 (2007-02-15) the whole document -----	1-14
A	EP 2 136 528 A1 (GIESECKE & DEVRIENT GMBH [DE]) 23 December 2009 (2009-12-23) paragraph [0010] paragraph [0024] - paragraph [0026] -----	1-14

INTERNATIONAL SEARCH REPORT

Information on patent family members

International application No

PCT/EP2011/001527

Patent document cited in search report	Publication date	Patent family member(s)	Publication date
WO 2007003429	A1	11-01-2007	CN 101243452 A 13-08-2008
			DE 102005031629 A1 11-01-2007
			EP 1902404 A1 26-03-2008
			JP 2009500735 A 08-01-2009
			US 2008297313 A1 04-12-2008
WO 2004090800	A2	21-10-2004	AT 428152 T 15-04-2009
			CN 1799058 A 05-07-2006
			DE 10317257 A1 04-11-2004
			EP 1616291 A2 18-01-2006
			EP 2081135 A2 22-07-2009
			JP 2006524851 A 02-11-2006
			PT 1616291 E 14-07-2009
			US 2007063055 A1 22-03-2007
WO 2007017288	A2	15-02-2007	DE 102005038106 A1 15-02-2007
			EP 1915718 A2 30-04-2008
EP 2136528	A1	23-12-2009	DE 102008028701 A1 24-12-2009

INTERNATIONALER RECHERCHENBERICHT

Internationales Aktenzeichen

PCT/EP2011/001527

A. KLASSIFIZIERUNG DES ANMELDUNGSGEGENSTANDES
INV. H04L9/32
ADD.

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

B. RECHERCHIERTE GEBIETE

Recherchierter Mindestprüfstoff (Klassifikationssystem und Klassifikationssymbole)
H04L G06F 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)

EPO-Internal, WPI Data

C. ALS WESENTLICH ANGESEHENE UNTERLAGEN

Kategorie*	Bezeichnung der Veröffentlichung, soweit erforderlich unter Angabe der in Betracht kommenden Teile	Betr. Anspruch Nr.
X	WO 2007/003429 A1 (GIESECKE & DEVRIENT GMBH [DE]; FINKENZELLER KLAUS [DE]; GAWLAS FLORIAN) 11. Januar 2007 (2007-01-11) Seite 1, Zeile 20 - Seite 2, Zeile 28 Seite 5, Zeile 11 - Zeile 21 Seite 7, Zeile 10 - Seite 9, Zeile 25 Seite 10, Zeile 25 - Seite 11, Zeile 23 Seite 14, Zeile 15 - Zeile 25 Seite 15, Zeile 19 - Seite 16, Zeile 7 Seite 17, Zeile 10 - Seite 19, Zeile 13 -----	1-14
A	WO 2004/090800 A2 (GIESECKE & DEVRIENT GMBH [DE]; GRAF HANS [DE]; FINKENZELLER KLAUS [DE]) 21. Oktober 2004 (2004-10-21) Seite 2 - Seite 3 Seite 7 - Seite 9 Seite 11 - Seite 12 ----- -/-	1-14



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

19. August 2011

Absendedatum des internationalen Recherchenberichts

29/08/2011

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

Apostolescu, Radu

C. (Fortsetzung) ALS WESENTLICH ANGESEHENE UNTERLAGEN		
Kategorie*	Bezeichnung der Veröffentlichung, soweit erforderlich unter Angabe der in Betracht kommenden Teile	Betr. Anspruch Nr.
A	WO 2007/017288 A2 (GIESECKE & DEVRIENT GMBH [DE]; MEISTER GISELA [DE]; URMANN JENS [DE]) 15. Februar 2007 (2007-02-15) das ganze Dokument -----	1-14
A	EP 2 136 528 A1 (GIESECKE & DEVRIENT GMBH [DE]) 23. Dezember 2009 (2009-12-23) Absatz [0010] Absatz [0024] - Absatz [0026] -----	1-14

INTERNATIONALER RECHERCHENBERICHT

Angaben zu Veröffentlichungen, die zur selben Patentfamilie gehören

Internationales Aktenzeichen

PCT/EP2011/001527

Im Recherchenbericht angeführtes Patentdokument	Datum der Veröffentlichung	Mitglied(er) der Patentfamilie	Datum der Veröffentlichung
WO 2007003429 A1	11-01-2007	CN 101243452 A	13-08-2008
		DE 102005031629 A1	11-01-2007
		EP 1902404 A1	26-03-2008
		JP 2009500735 A	08-01-2009
		US 2008297313 A1	04-12-2008

WO 2004090800 A2	21-10-2004	AT 428152 T	15-04-2009
		CN 1799058 A	05-07-2006
		DE 10317257 A1	04-11-2004
		EP 1616291 A2	18-01-2006
		EP 2081135 A2	22-07-2009
		JP 2006524851 A	02-11-2006
		PT 1616291 E	14-07-2009
		US 2007063055 A1	22-03-2007

WO 2007017288 A2	15-02-2007	DE 102005038106 A1	15-02-2007
		EP 1915718 A2	30-04-2008

EP 2136528 A1	23-12-2009	DE 102008028701 A1	24-12-2009
