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

(19) Weltorganisation für geistiges Eigentum
Internationales Büro

(43) Internationales Veröffentlichungsdatum
26. Oktober 2006 (26.10.2006)

PCT

(10) Internationale Veröffentlichungsnummer
WO 2006/111135 A1

(51) Internationale Patentklassifikation:
H04L 9/08 (2006.01) *G07F 19/00* (2006.01)

(21) Internationales Aktenzeichen: PCT/DE2006/000655

(22) Internationales Anmeldedatum:
12. April 2006 (12.04.2006)

(25) Einreichungssprache: Deutsch

(26) Veröffentlichungssprache: Deutsch

(30) Angaben zur Priorität:
10 2005 018 676.9 21. April 2005 (21.04.2005) DE

(71) Anmelder *(für alle Bestimmungsstaaten mit Ausnahme von US)*: **WINCOR NIXDORF INTERNATIONAL GMBH** [DE/DE]; Heinz-Nixdorf-Ring 1, 33106 Paderborn (DE).

(72) Erfinder; und

(75) Erfinder/Anmelder *(nur für US)*: **NOLTE, Michael** [DE/DE]; Koberg Weg 2a, 33034 Brakel (DE).

(74) Gemeinsamer Vertreter: **WINCOR NIXDORF INTERNATIONAL GMBH**; Heinz-Nixdorf-Ring 1, 33106 Paderborn (DE).

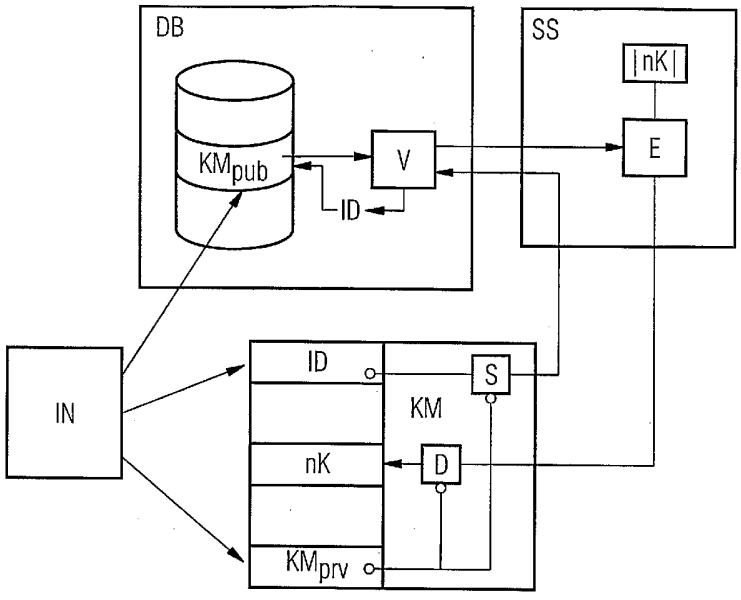
(81) Bestimmungsstaaten *(soweit nicht anders angegeben, für jede verfügbare nationale Schutzrechtsart)*: AE, AG, AL, AM, AT, AU, AZ, BA, BB, BG, BR, BW, BY, BZ, CA, CH, CN, CO, CR, CU, CZ, DK, DM, DZ, EC, EE, EG, ES, FI, GB, GD, GE, GH, GM, HR, HU, ID, IL, IN, IS, JP, KE, KG, KM, KN, KP, KR, KZ, LC, LK, LR, LS, LT, LU, LV, LY, 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, 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, LV, MC,

[Fortsetzung auf der nächsten Seite]

(54) Title: METHOD FOR KEY ADMINISTRATION FOR CRYPTOGRAPHY MODULES

(54) Bezeichnung: VERFAHREN ZUR SCHLÜSSELVERWALTUNG FÜR KRYPTOGRAPHIEMODULE



(57) Abstract: The invention relates to a method for a central key station (SS), for setting a new key (nK) in a cryptography module (KM) without a public key being stored in the cryptography module (KM), the authenticity of the new key (nK) being secured by a protocol. According to said method, the public key (KMpub) of the cryptography module is only transported in an encoded manner and only transmitted to key points (SS) that have access to the cryptography module (KM).

[Fortsetzung auf der nächsten Seite]

WO 2006/111135 A1

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*

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.

(57) Zusammenfassung: Verfahren für eine Schlüsselzentrale (SS) zum Setzen eines neuen Schlüssels (nK) in einem Kryptographiemodul (KM), ohne daß in dem Kryptographiemodul (KM) ein öffentlicher Schlüssel gespeichert ist, indem die Authentizität des neuen Schlüssels (nK) durch ein Protokoll gesichert wird, bei dem der öffentliche Schlüssel (KMpub) des Kryptographiemoduls nur verschlüsselt transportiert wird und nur an Schlüsselstellen (SS) weitergegeben wird, die ihrerseits Zugang zu dem Kryptographiemodul (KM) haben.

Verfahren zur Schlüsselverwaltung für Kryptographiemodule

Die Erfindung betrifft die Schlüsselverwaltung, d.h. die Initialisierung und Aktualisierung, von kryptographischen Schlüsseln, die insbesondere für Bankautomaten oder andere Selbstbedienungsgeräten verwendet werden.

Zur Sicherung von Selbstbedienungsgeräten wie insbesondere Geldautomaten gegen unbefugte Benutzung werden kryptographische Verfahren verwendet, deren Sicherheit auf der Sicherheit der Schlüssel beruht. Ein Geldautomat enthält demgemäß ein versiegeltes Kryptographiemodul, in dem ein oder mehrere Schlüssel derart gespeichert sind, daß diese nicht ausgelesen, sondern lediglich für kryptographische Transformationen verwendet werden können, in der Regel nach Freigabe durch eine PIN-Tastatur, die integraler Bestandteil des kryptographischen Prozessors ist.

Insbesondere bei der Verwendung symmetrischer Kryptographie ist sicherzustellen, daß der in dem Kryptographiemodul gespeicherte Schlüssel auch im Host, d.h. bei Geldautomaten in der Bankenzentrale, jedoch nur dort, vorhanden ist. Daher sind aufwendige Sicherheitsmaßnamen notwendig, wenn ein Schlüssel erstmalig installiert oder im laufenden Betrieb ausgetauscht werden soll. Ein Austausch im laufenden Betrieb erfolgt standardgemäß dadurch, daß mit dem bisherigen Schlüsselpaar eine gesicherte Übertragung des neuen Schlüssels bewirkt wird. Das ist aber nur möglich, wenn der initiale Schlüssel bereits dem Host zugeordnet ist und diese Zuordnung erhalten bleibt. Der Schlüsselaustausch ist also nur im Rahmen der gesicherten Anwendung möglich und damit unflexibel.

In der Patentschrift US 5,745,576 wird ein Verfahren beschrieben, bei dem ein allen Geräten gemeinsamer Schlüssel, der mit der Gerätenummer modifiziert wird, lediglich zur Schlüsselinitialisierung und zum Schlüsselaustausch verwendet wird. Da die Gerätenummer als bekannt gelten muss, beruht die Sicherheit nur noch auf dem für alle Kryptographiemodule gleichen Initialisierungsschlüssel.

In der US 5,761,306 wird ein asymmetrisches Verschlüsslungsverfahren verwendet. In dem Kryptographiemodul ist der private Schlüssel und in einer Schlüsselzentrale ist der öffentliche Schlüssel gespeichert, und das Verfahren betrifft den Austausch der privaten und öffentlichen Schlüssel. Dabei werden Hashwerte verwendet, um den Austausch zu authentisieren.

In der US 6,442,690 wird gleichfalls vorgeschlagen, public-key Verfahren zu verwenden und jedes Gerät zunächst mit einem, von einer Zentrale signierten

öffentlichen Schlüssel und dem zugehörigen privaten Schlüssel auszustatten. Dieses Schlüsselpaar wird dann durch ein anderes Schlüsselpaar ersetzt, wobei die bekannten Eigenschaften von public-key Verfahren ausgenutzt werden.

In allen diesen Fällen muß in dem Kryptographiemodul ein öffentlicher Schlüssel gespeichert sein, und es werden nur solche Schlüsseländerungen akzeptiert, die damit signiert sind. Daher ist es notwendig, den öffentlichen Schlüssel im Kryptographiemodul in einem aufwendigen Verfahren auszutauschen.

Aufgabe der Erfindung ist es daher, ein Verfahren zur Schlüsselverwaltung anzugeben, dass einen sicheren und einfachen Austausch von Schlüsseln für ein Kryptographiemodul ermöglicht.

Die Erfindung löst diese Aufgabe durch ein Verfahren für eine Schlüsselzentrale zum Setzen eines Schlüssels in einem Kryptographiemodul, wobei in dem Kryptographiemodul kein öffentlicher Schlüssel gespeichert ist, indem die Authentizität des neuen Schlüssels durch ein Protokoll gesichert wird, bei dem der öffentliche Schlüssel des Kryptographiemoduls nur verschlüsselt transportiert wird und nur an Schlüsselstellen weitergegeben wird, die ihrerseits Zugang zu dem Kryptographiemodul haben.

Die Erfindung wird für ein Kryptographiemodul beschrieben, das sowohl über symmetrische als auch asymmetrische Verschlüsslung verfügt und einen änderbaren Schlüsselspeicher für ein oder mehrere geheime Schlüssel für symmetrische Verschlüsslung sowie einen permanenten Schlüsselspeicher für den privaten Schlüssel einer asymmetrischen Verschlüsslung hat. Die Lösung gemäß der Erfindung benötigt keinen Speicher für einen öffentlichen Schlüssel, wie er im Stand der Technik zur Sicherung der Authentizität vorgesehen ist. Weiter hat jedes Kryptographiemodul eine eindeutige Gerätenummer, die gleichfalls im Innern gespeichert ist. Diese kann zudem außen aufgedruckt bzw. elektronisch auslesbar sein; zur Erhöhung der Sicherheit wird in einer Variante der Erfindung jedoch nur ein Hashwert der Gerätenummer auslesbar gemacht bzw. außen lesbar angebracht. Bevorzugt umfasst das Kryptographiemodul auch eine gepufferte Tagesuhr, mit der die im folgenden beschriebenen Nachrichten mit einem Zeitstempel versehen werden können, so dass die Gültigkeit der Nachrichten auf ein vordefiniertes Zeitintervall begrenzt werden kann.

Bei symmetrischer Verschlüsslung ist durch die Verwendung desselben Schlüssels für Ver- und Entschlüsslung dieser notwendigerweise geheim zu halten; daher kann jede erfolgreich entschlüsselte Nachricht mit ausreichend prüfbarer Redundanz auch gleichzeitig als authentisch angesehen werden. Da es

bei asymmetrischer Verschlüsslung für die Sicherung der Vertraulichkeit nicht notwendig ist, den öffentlichen Schlüssel geheim zu halten, wird allgemein davon ausgegangen, dass zur Sicherung der Authentizität ein zweites Schlüsselpaar notwendig sei, wobei der Absender mit seinem privaten Schüssel signiert und der Empfänger mit dem zugehörigen öffentlichen Schlüssel die Signatur prüft, bevor er die restliche Nachricht mit dem eigenen privaten Schlüssel entschlüsselt. Denn es ist gerade der entscheidende Vorteil der asymmetrischen Verschlüsslung, daß nur noch ein Schlüssel, der private Schlüssel, geheim gehalten werden muss, und der andere, der öffentliche Schlüssel, lediglich authentisch sein muss. Wird hingegen entgegen der herkömmlichen Verwendung auch der "öffentliche" Schlüssel keineswegs veröffentlicht, sondern im Gegenteil vertraulich gehalten, so wird, wie bei symmetrischer Verschlüsslung, durch ein erfolgreiches Entschlüsseln einer Nachricht mit dem privaten Schlüssel gleichzeitig sichergestellt, daß die Nachricht authentisch ist, insoweit sie nur von einer Stelle kommen kann, die über den "öffentlichen" Schlüssel verfügt. Insofern ist der Begriff "öffentlicher Schlüssel" als der nicht-private Schlüssel eines Schlüsselpaars bei einer asymmetrischer Verschlüsslung vom Wortsinn her im Rahmen der vorliegenden Erfindung nicht zutreffend; er wird jedoch auch weiterhin verwendet, da es sich um einen allgemein akzeptierten technischen Begriff handelt.

Von dem Hersteller eines Kryptographiemoduls wird in einem gesicherten Bereich der Produktionsstätte ein individuelles Paar eines öffentlichen und privaten Schlüssels generiert und der private Schlüssel wird in das Kryptographiemodul übertragen, wobei sichergestellt wird, dass keine weiteren Kopien verbleiben. Der öffentliche Schlüssel wird in einer Datenbank unter der Gerätenummer gespeichert und sowohl gegen Datenverlust als auch gegen illegitime Zugriffe geschützt. Bei Verwendung eines Hashwerts wird der Hashwert als Schlüssel verwendet und die Klartext-Gerätenummer zusammen mit dem öffentlichen Schlüssel gespeichert.

Das Kryptographiemodul umfaßt eine Funktion, mit der ein bestimmter geheimer Schlüssel für symmetrische Verschlüsslung geschrieben werden kann. Dieser Schlüssel wird auf dem Weg in das Kryptographiemodul gesichert, indem er durch asymmetrische Verschlüsslung mit dem zu dem im Kryptographiemodul enthaltenen privaten Schlüssel gehörigen öffentlichen Schlüssel verschlüsselt ist. Wie bereits ausgeführt, ist eine erfolgreiche Entschlüsslung gleichzeitig ein Nachweis, daß der Absender im Besitz des öffentlichen Schlüssels war.

Dies ist einerseits der Hersteller des Kryptographiemoduls, der ja originär im Besitz des öffentlichen Schlüssels ist. Zwar muß der Benutzer des Kryptographiemoduls ohnehin ein erhebliches Vertrauen in den Hersteller haben, daß keine Sicherheitsmängel vorhanden sind. Dennoch ist es nicht sinnvoll, die zukünftig für die Sicherheit des Betriebs mit entscheidenden neuen geheimen Schlüssel, die von der Schlüsselstelle erzeugt werden, zunächst an den Hersteller des Kryptographiemoduls zu übermitteln und dort mit dem öffentlichen Schlüssel verschlüsseln zu lassen. Dies ist insbesondere nicht sinnvoll, wenn die Personalisierung und die Herstellung voneinander getrennt sind.

Vielmehr wird durch die Erfindung vorgesehen, dass der öffentliche Schlüssel vom Hersteller des Kryptographiemoduls an den derzeitigen bzw. zukünftigen Betreiber übermittelt wird und dort in einer Schlüsselzentrale, die den neuen geheimen Schlüssel erzeugt, zur Verschlüsslung der Nachricht an das Kryptographiemodul verwendet wird. Diese Übertragung des öffentlichen Schlüssels an das Kryptographiemodul erfolgt gemäß der Erfindung mit gesicherter Authentizität und Vertraulichkeit. Das kann durch bereits existierende Mittel geschehen, beispielsweise durch kryptographisch gesicherte Nachrichten nach dem SOAP-Protokoll oder über HTTPS-Verbindungen.

Fig. 1 zeigt eine entsprechende Skizze. Durch die Initialisierung IN wird das Schlüsselpaar KM_{pub} und KM_{prv} sowie die Gerätenummer ID erzeugt und in die gesicherte Datenbank DB sowie das Kryptographiemodul KM übertragen. Beide Komponenten (KM und DB) befinden sich in einer Sicherheitsumgebung mit dem gleichen gemeinsamen Sicherheitsniveau. Das Kryptographiemodul KM hat einen Speicher für die Gerätenummer ID, den neu zu setzenden Schlüssel nK und den privaten Schlüssel KM_{prv}. Eine Signierfunktion S des Kryptographiemoduls KM erzeugt einen Identifikationsdatensatz, der die Gerätenummer ID enthält und mit dem privaten Schlüssel KM_{prv} signiert ist. Außerdem ist das Kryptographiemodul mit einer Entschlüsselungsfunktion D ausgestattet, die einen Datensatz mit dem neuen Schlüssel nK entschlüsseln kann. In der gesicherten Datenbank DB ist der öffentliche Schlüssel KM_{pub} via ID zugreifbar. Ein Vergleicher V entnimmt aus dem von der Signierfunktion S erzeugten Identifikationsdatensatz die Gerätenummer ID, bestimmt damit den öffentlichen Schlüssel KM_{pub}, prüft die Signatur der ID und sendet bei positiver Prüfung den öffentlichen Schlüssel KM_{pub} an die Schlüsselstelle SS. Die Schlüsselstelle SS hat einen Verschlüssler E, mit dem der von ihr erzeugte neue Schlüssel nK mit dem von der gesicherten Datenbank DB erhaltenen öffentlichen Schlüssel KM_{pub} verschlüsselt werden kann. Die

Schlüsselstelle SS schickt diesen verschlüsselten Schlüssel nK zum Kryptographiemodul KM, wo er von D entschlüsselt wird.

In den Protokolldiagrammen von Fig. 2 bis Fig. 4 wird die Signierung von Daten durch eckige Klammern mit angehängtem Schlüssel, die Verschlüsslung durch spitze Klammern symbolisiert. Die senkrechten Balken mit den Bezeichnungen KM, SS und DB stehen für den Kryptographiemodul, die Schlüsselstelle und die gesicherte Datenbank.

Fig. 2 zeigt den weiteren Ablauf in symbolischer Form: Das Kryptographiemodul KM sendet den Identifikationsdatensatz $[ID]_{KMprv}$ über die Schlüsselstelle SS an die gesicherte Datenbank DB, welche nach Prüfung den öffentlichen Schlüssel KM_{pub} an die Schlüsselstelle SS zurückschickt. Diese erzeugt den verschlüsselten neuen Schlüssel $<nK>_{KMpub}$. Der öffentliche Schlüssel KM_{pub} ist somit nicht im Kryptographiemodul, sondern in einer separaten Datenbank gespeichert und dient zur Verschlüsselung des neuen Schlüssels nK, der mit dem privaten Schlüssel im Kryptographiemodul entschlüsselt wird.

Die bevorzugte Ausführungsform der Erfindung integriert weitere Maßnahmen zur Sicherung von Integrität und Vertraulichkeit. Der Ablauf einer solchen verbesserten Variante ist in Fig. 3 dargestellt.

Hierzu schickt zunächst die Schlüsselstelle SS an das Kryptographiemodul einen Anfragedatensatz, in dem der öffentliche Schlüssel SS_{pub} der Schlüsselstelle enthalten ist, der hier auch nicht vertraulich gehalten werden muss. Dieser öffentliche Schlüssel wird in den Identifizierungsdatensatz $[ID, SS_{pub}]_{KMpriv}$ aufgenommen und zusammen mit der Gerätenummer mit dem privaten Schlüssel des Kryptographiemoduls signiert und an die Schlüsselstelle zurückgeschickt. Da der Datensatz nicht verschlüsselt, sondern signiert ist, kann und wird die Schlüsselstelle prüfen, ob die Gerätenummer und der eigene öffentliche Schlüssel in dem Identifizierungsdatensatz enthalten sind. Eine Überprüfung der Signatur ist noch nicht möglich, da die Schlüsselstelle noch nicht über den öffentlichen Schlüssel KM_{pub} des Kryptographiemoduls verfügt.

Der Identifizierungsdatensatz wird von der Schlüsselstelle über beliebige Verbindungen, insbesondere auch unter Verwendung von Web-Services, als Anfrage an die gesicherte Datenbank DB des Herstellers des Kryptographiemoduls KM geschickt. Dieser verwendet die Gerätenummer ID, um den Datensatz mit dem öffentlichen Schlüssel KM_{pub} aufzufinden, und prüft sodann mit dem aufgefundenen, bislang nur hier vorliegenden öffentlichen Schlüssel KM_{pub} des Kryptographiemoduls die Signatur des Identifizierungs-

datensatz. Damit ist sichergestellt, daß der öffentliche Schlüssel KM_{pub} nur an eine Schlüsselstelle SS weitergegeben wird, die Zugang zu dem entsprechenden Kryptographiemodul KM hat.

Ist die Signatur passend, dann wird ein Bereitstellungsdatensatz $<KM_{pub}>_{SSpub}$ erzeugt, in dem der öffentliche Schlüssel des Kryptographiemoduls enthalten ist. Dieser Bereitstellungsdatensatz wird mit dem öffentlichen Schlüssel SS_{pub} der Schlüsselstelle verschlüsselt, optional noch mit einem privaten Schlüssel der gesicherten Datenbank signiert und an die Schlüsselstelle SS zurückgeschickt. Damit ist sichergestellt, daß der öffentliche Schlüssel des Kryptographiemoduls nur der Schlüsselstelle SS zugänglich ist.

Die Schlüsselstelle SS, die über ihren eigenen privaten Schlüssel SS_{priv} verfügt, kann nunmehr den Bereitstellungsdatensatz entschlüsseln und den öffentlichen Schlüssel KM_{pub} des Kryptographiemoduls entnehmen.

Mit diesem wird, wie zuvor, ein Setzdatensatz $<nk>_{KMpub}$, der den neuen Schlüssel nK enthält, mit dem öffentlichen Schlüssel KM_{pub} des Kryptographiemoduls KM verschlüsselt und an letzteren gesendet, welcher wie zuvor den Datensatz entschlüsselt und nach Redundanzprüfung den neuen Schlüssel nK einträgt. Nicht notwendig, aber zweckmäßig ist es, die Gerätenummer ID mit in den Setzdatensatz aufzunehmen.

Diese Variante hat noch den Nachteil, daß der öffentliche Schlüssel der Schlüsselstelle ungesichert zum Kryptographiemodul KM übertragen wird, welcher damit nicht prüfen kann, ob die Anfrage berechtigt ist.

In der bevorzugten Weiterbildung nach Fig. 4 wird dies verhindert, indem zunächst die Schlüsselstelle SS von der gesicherten Datenbank DB unter Angabe der Gerätenummer ID den Anfragedatensatz, der den öffentlichen Schlüssel SS_{pub} der Schlüsselstelle enthält, mit dem öffentlichen Schlüssel KM_{pub} des Kryptographiemoduls KM verschlüsseln läßt. Der Anfragedatensatz wird in der Regel die Gerätenummer (ID) mit enthalten; notwendig ist dies jedoch nicht. Zur Sicherung dieser Operation verfügt die gesicherte Datenbank über ein Verzeichnis der öffentlichen Schlüssel der Schlüsselstellen, so daß nur eine registrierte Schlüsselstelle einen verschlüsselten Anfragedatensatz erhalten kann. Das Kryptographiemodul entschlüsselt in dieser Ausführungsform jeden Anfragedatensatz vor der weiteren Bearbeitung mit dem eigenen privaten Schlüssel KM_{prv}, so daß eine nicht autorisierte Anfrage abgewiesen werden kann und der für die Erlangung des öffentlichen Schlüssels notwendige Identifizierungsdatensatz erst gar nicht erzeugt wird.

In den beiden Ausführungsformen nach Fig. 3 und Fig. 4 ist es zusätzlich zweckmäßig, daß die Schlüsselstelle SS den Identifizierungsdatensatz zusätzlich mit dem eigenen privaten Schlüssel SS_{prv} signiert und diese Signatur von der gesicherten Datenbank (DB) überprüft wird. Hierzu kann einerseits der in dem Datensatz enthaltene öffentliche Schlüssel dienen. Besser ist es wenn, wie in der Ausführungsform nach Fig. 4, von der gesicherten Datenbank (DB) ein durch andere Mittel gesichertes Verzeichnis der öffentlichen Schlüssel der Schlüsselstellen vorliegt und mit verwendet wird.

Bei einer weiteren Variante der Erfindung nach Fig. 3 oder Fig. 4 verschlüsselt das Kryptographiemodul den Identifizierungsdatensatz mit dem öffentlichen Schlüssel SS_{pub} der Schlüsselstelle SS. Diese entschlüsselt den Identifizierungsdatensatz und signiert ihn vor der Weiterleitung an die gesicherte Datenbank DB. Auf die Signierung kann auch verzichtet werden.

In einer weiteren Variante kann zusätzlich noch die Datenbank DB über ein Schlüsselpaar DB_{priv} und DB_{pub} verfügen, um den Austausch mit SS, IN und KM noch sicherer zu gestalten. Auch die Initialisierung IN kann über ein Schlüsselpaar IN_{priv} und IN_{pub} für eine noch sichere Verbindung mit DB und KM verfügen.

Wie bereits oben angedeutet, enthält das Kryptographiemodul KM auch eine Tagesuhr und setzt bzw. prüft Zeitstempel in den gesendeten und empfangenen Datensätzen, um eine Wiederholung älterer Datensätze zu verhindern. Zur Unterstützung dieser Funktion enthält das Kryptographiemodul KM ferner ein Register, in dem der Zeitstempel des letzten erzeugten Identifizierungsdatensatzes abgelegt wird und ein Setzdatensatz nur innerhalb einer vorgegebenen Zeitspanne danach akzeptiert wird.

Bei einer anderen Weiterbildung verfügt das Kryptographiemodul KM über einen Zufallszahlengenerator und einen Speicher für eine Zufallszahl. Jeder Identifizierungsdatensatz enthält zusätzlich eine Zufallszahl, die in dem Setzdatensatz wieder enthalten sein muß, damit die Funktion durchgeführt wird. Zudem wird dieser Speicher gelöscht, sobald ein Setzdatensatz empfangen wird, so daß Wiederholungen veralteter Setzdatensätze nicht wirksam sind. Anstelle einer Zufallszahl, für die in der Regel ohnehin ein Generator im Kryptographiemodul KM vorhanden ist, kann auch ein Zähler verwendet werden.

Bekannte Maßnahmen zur Sicherung der Datensätze gegen Kryptoanalyse, wie dem Einfügen von Seriennummern und Zufallszahlen bei Verschlüsslung, sind dem Fachmann geläufig und nicht weiter aufgeführt.

Da die Eigenschaften der zu den Schlüsselspeichern gehörigen Verschlüsslung keine Rolle spielen, können anstelle geheimer Schlüssel für symmetrische Verschlüsslung alternativ oder gemischt die Schlüssel auch für asymmetrische Verschlüsslung gesetzt werden.

Ansprüche

1. Verfahren zum gesicherten Übertragen eines neuen Schlüssels (nK) von einer Schlüsselstelle (SS) in ein Kryptographiemodul (KM), das dafür einen beschreibbaren Schlüsselspeicher und zudem einen weiteren Schlüsselspeicher für einen privaten Schlüssel (KM_{prv}) umfaßt, mit den Schritten:

- In einer gesicherten Umgebung (IN) wird eine Gerätenummer (ID) des Kryptographiemoduls sowie ein Schlüsselpaar aus privatem und öffentlichem Schlüssel (KM_{prv}, KM_{pub}) für ein asymmetrisches Verschlüsslungsverfahren erzeugt, der private Schlüssel (KM_{prv}) wird in das Kryptographiemodul (KM) übertragen und der öffentliche Schlüssel (KM_{pub}) in einer gesicherten Datenbank (DB) unter der Gerätenummer (ID) abgelegt;

- von der Schlüsselstelle (SS) wird aus dem Kryptographiemodul (KM) ein die Gerätenummer (ID) enthaltender, mit dem privaten Schlüssel (KM_{prv}) signierter erster Datensatz ausgelesen und an die gesicherte Datenbank (DB) übertragen;

- die gesicherte Datenbank (DB) ermittelt mit Hilfe der Gerätenummer (ID) den öffentlichen Schlüssel (KM_{pub}), prüft damit die Signatur des die Gerätenummer (ID) enthaltenden Datensatzes und sendet an die Schlüsselstelle (SS) den öffentlichen Schlüssel (KM_{pub}) zurück;

- die Schlüsselstelle (SS) erzeugt einen Setzdatensatz, der den neuen Schlüssel (nK) enthält und mit dem öffentlichen Schlüssel (KM_{pub}) des Kryptographiemoduls (KM) verschlüsselt ist, und sendet diesen Setzdatensatz an das Kryptographiemodul (KM);

- das Kryptographiemodul (KM) entschlüsselt den Setzdatensatz, prüft die darin enthaltene Redundanz und setzt den neuen Schlüssel (nK).

2. Verfahren zum gesicherten Übertragen eines neuen Schlüssels (nK) von einer Schlüsselstelle (SS) in ein Kryptographiemodul (KM), das dafür einen beschreibbaren Schlüsselspeicher und zudem einen weiteren Schlüsselspeicher für einen privaten Schlüssel (KM_{prv}) umfaßt, mit den Schritten:

- In einer gesicherten Umgebung (IN) wird eine Gerätenummer (ID) sowie ein Schlüsselpaar aus einem privaten (KM_{prv}) und einem öffentlichem (KM_{pub}) Schlüssel für ein asymmetrisches Verschlüsslungsverfahren erzeugt, der private Schlüssel (KM_{prv}) wird in das Kryptographiemodul übertragen und der öffentliche

Schlüssel (KM_{pub}) in einer gesicherten Datenbank (DB) unter der Gerätenummer (ID) abgelegt;

- die Schlüsselstelle (SS) hat ein Schlüsselpaar für eine asymmetrische Verschlüsslung und sendet an das Kryptographiemodul (KM) einen Anfragedatensatz, der ihren öffentlichen Schlüssel (SS_{pub}) enthält;

- das Kryptographiemodul (KM) erzeugt ein die Gerätenummer (ID) und den öffentlichen Schlüssel (SS_{pub}) der Schlüsselstelle (SS) enthaltenden, mit dem gespeicherten privaten Schlüssel (KM_{prv}) signierten Identifizierungs-Datensatz und sendet diesen an die Schlüsselstelle (SS), die ihn an die gesicherte Datenbank (DB) weitersendet;

- die gesicherte Datenbank (DB) ermittelt mit Hilfe der Gerätenummer (ID) den öffentlichen Schlüssel (KM_{pub}) des Kryptographiemoduls, prüft damit die Signatur des Identifizierungs-Datensatzes, erzeugt einen Bereitstellungs-Datensatz, verschlüsselt diesen mit dem dem Identifizierungs-Datensatz entnommenen öffentlichen Schlüssel (SS_{pub}) der Schlüsselstelle (SS) und sendet diesen Bereitstellungs-Datensatz an die Schlüsselstelle (SS) zurück;

- die Schlüsselstelle (SS) entschlüsselt den Bereitstellungs-Datensatz und erzeugt einen Setzdatensatz, der den neuen Schlüssel (nK) enthält und mit dem dem Bereitstellungsdatensatz entnommenen öffentlichen Schlüssel des Kryptographiemoduls (KM_{pub}) verschlüsselt ist, und sendet diesen Setzdatensatz an das Kryptographiemodul (KM);

- das Kryptographiemodul (KM) entschlüsselt den Setzdatensatz, prüft die darin enthaltende Redundanz und setzt den neuen Schlüssel (nK).

3. Verfahren nach Anspruch 2, wobei der Identifizierungsdatensatz von der Schlüsselstelle (SS) zusätzlich mit ihrem privaten Schlüssel (SS_{prv}) signiert wird und die gesicherte Datenbank (DB) diese Signatur vor Weiterverarbeitung prüft.

4. Verfahren nach Anspruch 2 oder 3, wobei im zweiten Schritt die Schlüsselstelle (SS) von der gesicherten Datenbank (DB) unter Angabe der Gerätenummer (ID) den Anfragedatensatz angefordert, der den öffentliche Schlüssel (SS_{pub}) der Schlüsselstelle enthält und der mit dem öffentlichen Schlüssel (KM_{pub}) des Kryptographiemoduls (KM) verschlüsselt ist.

5. Verfahren nach Anspruch 4, wobei der Identifizierungsdatensatz von dem Kryptographiemodul (KM) mit dem öffentlichen Schlüssel (SS_{pub}) der Schlüsselstelle (SS) verschlüsselt, von der Schlüsselstelle (SS) mit deren privaten Schlüssel (SS_{prv}) entschlüsselt und vor der Weitersendung an die gesicherte

Datenbank (DB) mit einem öffentlichen Schlüssel der gesicherten Datenbank verschlüsselt wird.

6. Verfahren nach einem der vorhergehenden Ansprüche, wobei das Kryptographiemodul (KM) eine Tagesuhr enthält, die ausgetauschten Datensätze Zeitstempel oder Gültigkeits-Zeitintervalle enthalten und die Prüfung von Signatur und Redundanz diese Zeitangaben gegenüber vorgegebenen Schranken umfasst.

7. Verfahren nach dem vorigen Anspruch, wobei das Kryptographiemodul (KM) ferner einen Speicher für einen Zeitstempel enthält, in dem der Zeitpunkt der Erstellung eines Identifizierungsdatensatzes abgelegt wird, und wobei das Kryptographiemodul nur innerhalb einer vorgegebenen Zeitspanne nach dem letzten gespeicherten Zeitpunkt der Erstellung eines Identifizierungsdatensatzes einen Setzdatensatz ausführt.

8. Verfahren nach einem der vorhergehenden Ansprüche, wobei das Kryptographiemodul (KM) einen weiteren Speicher und Generator für einen Zufallswert umfaßt, diesen in den Datensatz an die Schlüsselstelle (SS) einfügt, die den Zufallswert in den Setzdatensatz einfügt und das Kryptographiemodul (KM) bei der Redundanzprüfung den Zufallswert auf Gleichheit überprüft.

9. Verfahren nach einem der vorhergehenden Ansprüche, wobei die Datenbank DB über einen öffentlichen Schlüssel DB_{pub} und einen privaten Schlüssel DB_{prv} verfügt, mit dem Datensätze, die zwischen der Schlüsselstelle SS, der Initialisierung IN und dem Kryptographiemodul KM ausgetauscht werden, verschlüsselt werden können.

10. Verfahren nach einem der vorhergehenden Ansprüche, wobei die Initialisierung IN über einen öffentlichen Schlüssel IN_{pub} und einen privaten Schlüssel IN_{prv} verfügt, mit dem Datensätze, die zwischen der Schlüsselstelle SS, der Datenbank DB und dem Kryptographiemodul KM ausgetauscht werden, verschlüsselt werden können.

11. Verfahren nach einem der vorhergehenden Ansprüche, wobei das Verfahren nach einem der Ansprüche 1 bis 10 bei einem Selbstbedienungsgerät, insbesondere einem Geldautomaten eingesetzt wird.

12. Kryptographiemodul (KM) zur Durchführung eines der Verfahren nach Anspruch 1 bis 11, wobei das Kryptographiemodul (KM) ein Mittel zur Erzeugung eines Identifizierungsdatensatzes enthält, welcher die Gerätenummer (ID) umfaßt und mit dem gespeicherten privaten Schlüssel (KM_{prv}) signiert ist, sowie ein Mittel zum Setzen eines Schlüsselspeichers mit einem neuen Schlüssel (nK) nach

Empfang eines Setzdatensatzes enthält, welches Mittel den Setzdatensatz mit dem gespeicherten privaten Schlüssel (KM_{prv}) vor dessen Ausführung entschlüsselt.

13. Kryptographiemodul (KM) nach Anspruch 9, wobei ein Identifizierungsdatensatz als Reaktion auf einen Anfragedatensatz erstellt wird, der mit dem geheimen Schlüssel (KM_{prv}) entschlüsselt, auf Plausibilität überprüft und ganz oder in Teilen in den Identifizierungsdatensatz übernommen wird, bevor dieser signiert wird.

14. Kryptographiemodul (KM) nach einem der vorhergehenden Ansprüche, wobei das Kryptographiemodul (KM) nach Anspruch 12 oder 23 bei einem Selbstbedienungsgerät, insbesondere einem Geldautomaten eingesetzt wird.

FIG 1

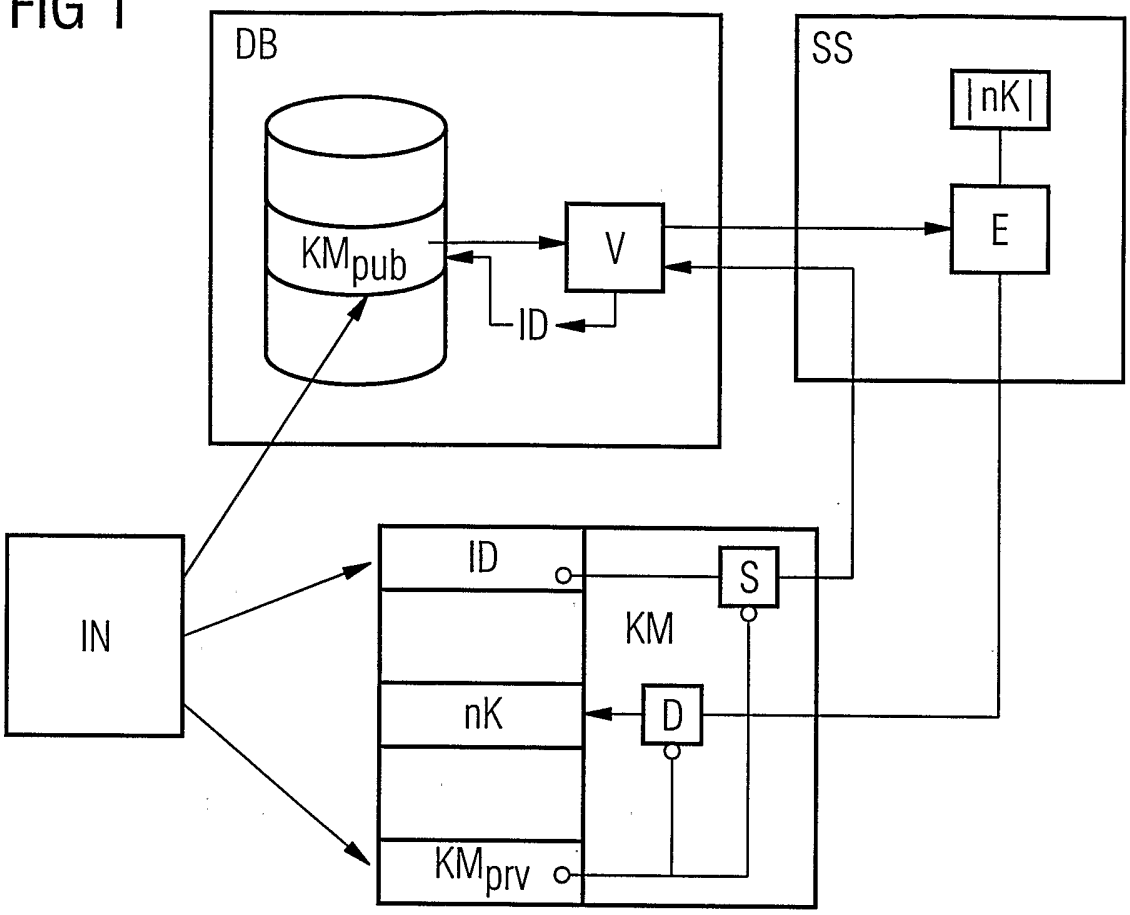

DB
SS
|nK|
E
KMpub
V
ID
IN
ID
S
KM
nK
D
KMprv

FIG 2

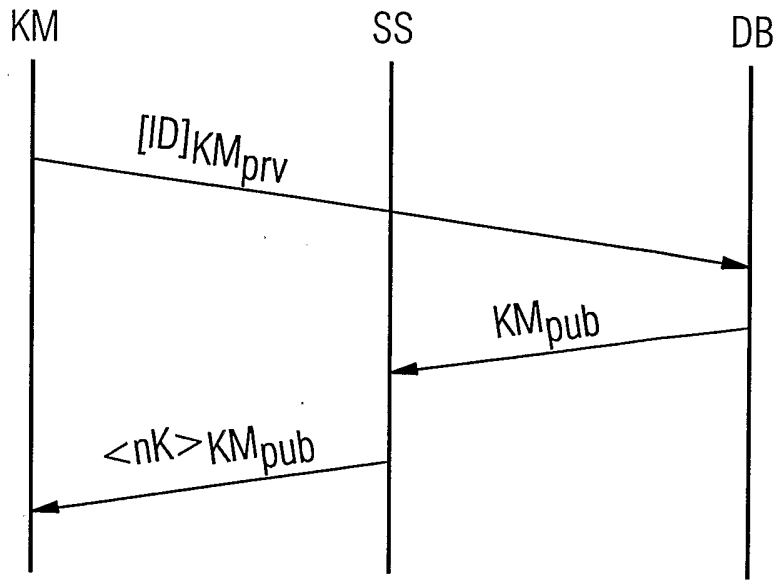

KM
SS
DB
[ID]KMprv
KMpub
<nK>KMpub

FIG 3

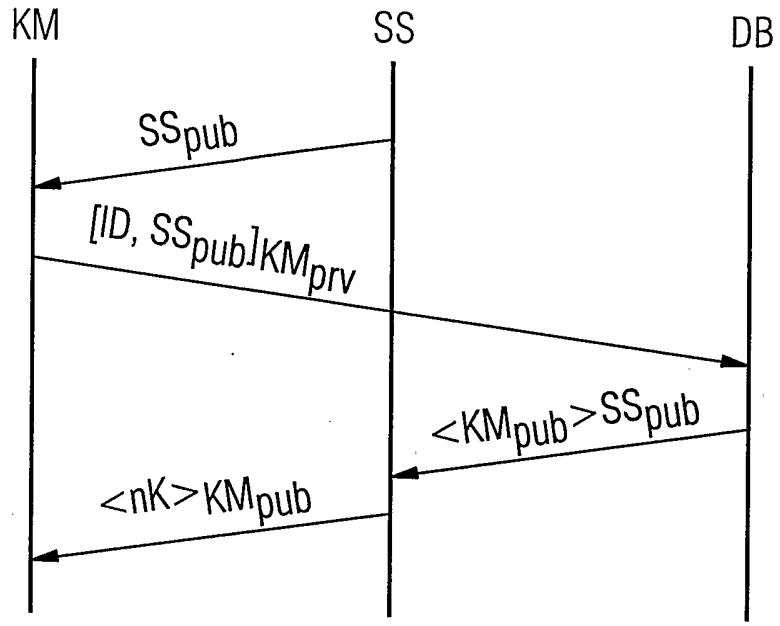
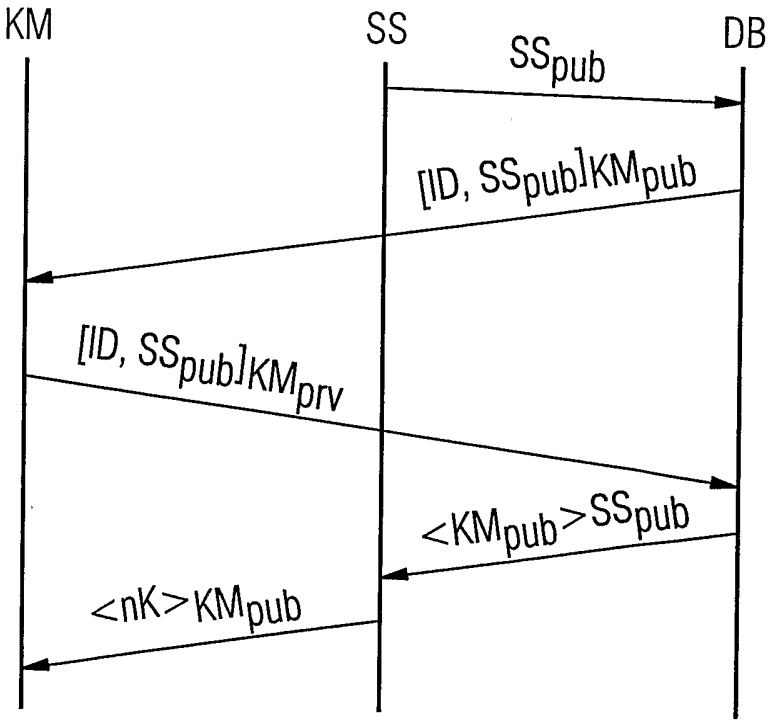

KM
SS
DB
SSpub
[ID, SSpub]KMprv
<KMpub>SSpub
<nK>KMpub

FIG 4


KM
SS
DB
SSpub
[ID, SSpub]KMpub
[ID, SSpub]KMprv
<KMpub>SSpub
<nK>KMpub

INTERNATIONAL SEARCH REPORT

International application No
PCT/DE2006/000655

A. CLASSIFICATION OF SUBJECT MATTER
INV. H04L9/08
ADD. G07F19/00

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)
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)
EPO-Internal, WPI Data, PAJ, INSPEC

C. DOCUMENTS CONSIDERED TO BE RELEVANT

Category*	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
A	US 5 745 576 A (ABRAHAM ET AL) 28 April 1998 (1998-04-28) cited in the application column 1, line 10 - column 2, line 27 column 6, line 57 - column 8, line 56	1-14
A	US 5 761 306 A (LEWIS ET AL) 2 June 1998 (1998-06-02) cited in the application column 1, line 6 - column 2, line 29 column 5, line 15 - column 13, line 5	1-14
A	EP 1 096 446 A (CITICORP DEVELOPMENT CENTER, INC) 2 May 2001 (2001-05-02) abstract paragraph [0015] - paragraph [0016] paragraph [0032] - paragraph [0039]	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	Date of mailing of the international search report
7 August 2006	16/08/2006

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	Liebhardt, I

INTERNATIONAL SEARCH REPORT

Information on patent family members

International application No
PCT/DE2006/000655

Patent document cited in search report	Publication date	Patent family member(s)	Publication date
US 5745576 A	28-04-1998	AU 4228197 A	05-01-1998
		WO 9745979 A2	04-12-1997
US 5761306 A	02-06-1998	AU 723946 B2	07-09-2000
		AU 2137797 A	10-09-1997
		GB 2324449 A	21-10-1998
		US 6240187 B1	29-05-2001
		WO 9731450 A1	28-08-1997
EP 1096446 A	02-05-2001	CN 1305159 A	25-07-2001

INTERNATIONALER RECHERCHENBERICHT

Internationales Aktenzeichen
PCT/DE2006/000655

A. KLASSIFIZIERUNG DES ANMELDUNGSGEGENSTANDES
INV. H04L9/08
ADD. G07F19/00

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

B. RECHERCHIERTE GEBIETE

Recherchierter Mindestprüfstoff (Klassifikationssystem und Klassifikationssymbole)
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)
EPO-Internal, WPI Data, PAJ, INSPEC

C. ALS WESENTLICH ANGESEHENE UNTERLAGEN

Kategorie*	Bezeichnung der Veröffentlichung, soweit erforderlich unter Angabe der in Betracht kommenden Teile	Betr. Anspruch Nr.
A	US 5 745 576 A (ABRAHAM ET AL) 28. April 1998 (1998-04-28) in der Anmeldung erwähnt Spalte 1, Zeile 10 - Spalte 2, Zeile 27 Spalte 6, Zeile 57 - Spalte 8, Zeile 56	1-14
A	US 5 761 306 A (LEWIS ET AL) 2. Juni 1998 (1998-06-02) in der Anmeldung erwähnt Spalte 1, Zeile 6 - Spalte 2, Zeile 29 Spalte 5, Zeile 15 - Spalte 13, Zeile 5	1-14
A	EP 1 096 446 A (CITICORP DEVELOPMENT CENTER, INC) 2. Mai 2001 (2001-05-02) Zusammenfassung Absatz [0015] - Absatz [0016] Absatz [0032] - Absatz [0039]	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	Absendedatum des internationalen Recherchenberichts
7. August 2006	16/08/2006

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	Liebhardt, I

INTERNATIONALER RECHERCHENBERICHT

Angaben zu Veröffentlichungen, die zur selben Patentfamilie gehören

Internationales Aktenzeichen
PCT/DE2006/000655

Im Recherchenbericht angeführtes Patentdokument	Datum der Veröffentlichung	Mitglied(er) der Patentfamilie	Datum der Veröffentlichung
US 5745576 A	28-04-1998	AU 4228197 A	05-01-1998
		WO 9745979 A2	04-12-1997
US 5761306 A	02-06-1998	AU 723946 B2	07-09-2000
		AU 2137797 A	10-09-1997
		GB 2324449 A	21-10-1998
		US 6240187 B1	29-05-2001
		WO 9731450 A1	28-08-1997
EP 1096446 A	02-05-2001	CN 1305159 A	25-07-2001