

(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  
1. Juli 2004 (01.07.2004)

PCT

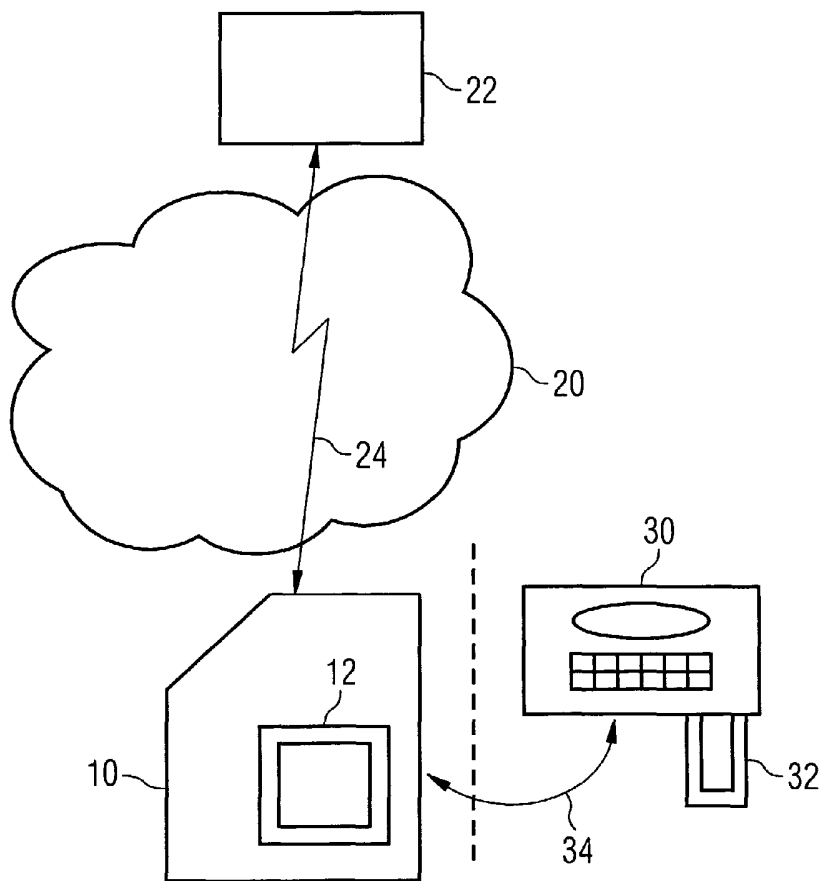
(10) Internationale Veröffentlichungsnummer  
**WO 2004/056030 A3**

- (51) Internationale Patentklassifikation<sup>7</sup>: **G07F 7/10**, 19/00, H04L 9/00
- (21) Internationales Aktenzeichen: PCT/DE2003/003853
- (22) Internationales Anmeldedatum:  
20. November 2003 (20.11.2003)
- (25) Einreichungssprache: Deutsch
- (26) Veröffentlichungssprache: Deutsch
- (30) Angaben zur Priorität:  
102 59 270.5 17. Dezember 2002 (17.12.2002) 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) Bestimmungsstaat (national): US.

[Fortsetzung auf der nächsten Seite]

(54) Title: PERSONALISATION OF SECURITY MODULES

(54) Bezeichnung: PERSONALISIERUNG VON SICHERHEITSMODULN



(57) Abstract: The invention relates to a security module, personalising unit and to a method for their use. According to said method, the security module contains a secret key of a key pair for asymmetric encryption, the personalising unit generates a certificate using the public key of the key pair and transmits said certificate, together with the public key of a central system, to the security module. The latter uses the certificate and the public key to secure the communication with a central system, in particular in the field of banking.

(57) Zusammenfassung:

Sicherheitsmodul, Personalisierer und Verfahren zu deren Benutzung, wobei der Sicherheitsmodul einen geheimen Schlüssel eines Schlüsselpaares für asymmetrische Verschlüsselung enthält, der Personalisierer ein Zertifikat über den öffentlichen Schlüssel des Schlüsselpaares erzeugt und zusammen mit dem öffentlichen Schlüssel eines Zentralsystems an den Sicherheitsmodul sendet. Der Sicherheitsmodul verwendet dieses Zertifikat und den öffentlichen

Schlüssel zur Sicherung der Kommunikation mit einem Zentralsystem, insbesondere im Bankenbereich.

WO 2004/056030 A3



(84) **Bestimmungsstaaten** (*regional*): europäisches Patent (AT, BE, BG, CH, CY, CZ, DE, DK, EE, ES, FI, FR, GB, GR, HU, IE, IT, LU, MC, NL, PT, RO, SE, SI, SK, TR).

*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.*

**Veröffentlicht:**

- *mit internationalem Recherchenbericht*
- *vor Ablauf der für Änderungen der Ansprüche geltenden Frist; Veröffentlichung wird wiederholt, falls Änderungen eintreffen*

(88) **Veröffentlichungsdatum des internationalen**

**Recherchenberichts:** 26. August 2004

# INTERNATIONAL SEARCH REPORT

International Application No  
PCT/DE 03/03853

**A. CLASSIFICATION OF SUBJECT MATTER**

IPC 7 G07F7/10 G07F19/00 H04L9/00

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)  
IPC 7 G07F H04L

Documentation searched other than minimum documentation to the extent that such documents are included in the fields searched

Electronic data base consulted during the international search (name of data base and, where practical, search terms used)

EPO-Internal

**C. DOCUMENTS CONSIDERED TO BE RELEVANT**

Category °	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
X	EP 0 784 256 A (INTEL CORP) 16 July 1997 (1997-07-16)  abstract column 3, line 32 - line 59 column 4, line 9 - line 19 column 4, line 59 - column 5, line 9 column 6, line 7 - line 38 column 6, line 56 - column 8, line 7 column 8, line 18 - column 9, line 10 figures 4-8	1-3, 9-11, 13, 16-21
A	----- -/--	4-8

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

14 June 2004

Date of mailing of the international search report

21/06/2004

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

Bassanini, A

## INTERNATIONAL SEARCH REPORT

International Application No  
PCT/DE 03/03853

C.(Continuation) DOCUMENTS CONSIDERED TO BE RELEVANT		
Category *	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
X	EP 1 096 446 A (CITICORP DEV CT INC) 2 May 2001 (2001-05-02) abstract paragraph '0017! - paragraph '0022! paragraph '0024! - paragraph '0026! paragraph '0032! - paragraph '0036! paragraph '0049! - paragraph '0053! figures 1,4,5	1-3
A	-----	4-21
P,X	US 2003/088772 A1 (HAARTSEN JACOBUS ET AL) 8 May 2003 (2003-05-08) abstract paragraph '0006! paragraph '0013! - paragraph '0021! figures 1-3	1-3,12
P,A	-----	14,15
X	US 5 781 723 A (BENALOH JOSH ET AL) 14 July 1998 (1998-07-14) the whole document	1-3
A	US 2002/053022 A1 (SPENCE JOHN R ET AL) 2 May 2002 (2002-05-02) paragraph '0009! - paragraph '0013! paragraph '0018! - paragraph '0023! paragraph '0028! -----	1-21

# INTERNATIONAL SEARCH REPORT

Information on patent family members

International Application No  
PCT/DE 03/03853

Patent document cited in search report	Publication date	Patent family member(s)	Publication date
EP 0784256	A	EP 0784256 A1	16-07-1997
EP 1096446	A	CN 1305159 A EP 1096446 A2	25-07-2001 02-05-2001
US 2003088772	A1	NONE	
US 5781723	A	NONE	
US 2002053022	A1	CA 2324772 A1	30-04-2002

# INTERNATIONALER RECHERCHENBERICHT

Internationales Aktenzeichen  
PCT/DE 03/03853

**A. KLASSIFIZIERUNG DES ANMELDUNGSGEGENSTANDES**  
IPK 7 G07F7/10 G07F19/00 H04L9/00

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

**B. RECHERCHIERTE GEBIETE**

Recherchierter Mindestprüfstoff (Klassifikationssystem und Klassifikationssymbole)  
IPK 7 G07F H04L

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 <sup>o</sup>	Bezeichnung der Veröffentlichung, soweit erforderlich unter Angabe der in Betracht kommenden Teile	Betr. Anspruch Nr.
X	EP 0 784 256 A (INTEL CORP) 16. Juli 1997 (1997-07-16)  Zusammenfassung Spalte 3, Zeile 32 - Zeile 59 Spalte 4, Zeile 9 - Zeile 19 Spalte 4, Zeile 59 - Spalte 5, Zeile 9 Spalte 6, Zeile 7 - Zeile 38 Spalte 6, Zeile 56 - Spalte 8, Zeile 7 Spalte 8, Zeile 18 - Spalte 9, Zeile 10 Abbildungen 4-8	1-3, 9-11, 13, 16-21
A	----- -/--	4-8

Weitere Veröffentlichungen sind der Fortsetzung von Feld C zu entnehmen

Siehe Anhang Patentfamilie

<sup>o</sup> 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

\*Z\* Veröffentlichung, die Mitglied derselben Patentfamilie ist

Datum des Abschlusses der internationalen Recherche

14. Juni 2004

Absendedatum des internationalen Recherchenberichts

21/06/2004

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

Bassanini, A

C.(Fortsetzung) ALS WESENTLICH ANGESEHENE UNTERLAGEN		
Kategorie°	Bezeichnung der Veröffentlichung, soweit erforderlich unter Angabe der in Betracht kommenden Teile	Betr. Anspruch Nr.
X	EP 1 096 446 A (CITICORP DEV CT INC) 2. Mai 2001 (2001-05-02) Zusammenfassung Absatz '0017! - Absatz '0022! Absatz '0024! - Absatz '0026! Absatz '0032! - Absatz '0036! Absatz '0049! - Absatz '0053! Abbildungen 1,4,5	1-3
A	-----	4-21
P,X	US 2003/088772 A1 (HAARTSEN JACOBUS ET AL) 8. Mai 2003 (2003-05-08) Zusammenfassung Absatz '0006! Absatz '0013! - Absatz '0021! Abbildungen 1-3	1-3,12
P,A	-----	14,15
X	US 5 781 723 A (BENALOH JOSH ET AL) 14. Juli 1998 (1998-07-14) das ganze Dokument	1-3
A	-----	1-21
	US 2002/053022 A1 (SPENCE JOHN R ET AL) 2. Mai 2002 (2002-05-02) Absatz '0009! - Absatz '0013! Absatz '0018! - Absatz '0023! Absatz '0028! -----	

# INTERNATIONALER RECHERCHENBERICHT

Angaben zu Veröffentlichungen, die zur selben Patentfamilie gehören

Internationales Aktenzeichen  
PCT/DE 03/03853

Im Recherchenbericht angeführtes Patentdokument		Datum der Veröffentlichung	Mitglied(er) der Patentfamilie		Datum der Veröffentlichung
EP 0784256	A	16-07-1997	EP	0784256 A1	16-07-1997
EP 1096446	A	02-05-2001	CN	1305159 A	25-07-2001
			EP	1096446 A2	02-05-2001
US 2003088772	A1	08-05-2003	KEINE		
US 5781723	A	14-07-1998	KEINE		
US 2002053022	A1	02-05-2002	CA	2324772 A1	30-04-2002