

(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. November 2007 (01.11.2007)

PCT

(10) Internationale Veröffentlichungsnummer
WO 2007/122266 A3

(51) Internationale Patentklassifikation:
H04L 29/06 (2006.01) *G06F 21/00* (2006.01)
G06F 9/46 (2006.01)

PERFORMANCE MICROELECTRONICS / INSTITUT FÜR INNOVATIVE MIKROELEKTRONIK [DE/DE]; Im Technologiepark 25, 15236 Frankfurt (Oder) (DE).

(21) Internationales Aktenzeichen: PCT/EP2007/054117

(72) Erfinder; und

(22) Internationales Anmeldedatum:
26. April 2007 (26.04.2007)

(75) Erfinder/Anmelder (*nur für US*): LANDGENDÖRFER, Peter [DE/DE]; Kiliansberg 3, 15230 Frankfurt (Oder) (DE). MAASER, Michael [DE/DE]; Briesener Str. 4, 15517 Fürstenwalde/Spree (DE).

(25) Einreichungssprache: Deutsch

(26) Veröffentlichungssprache: Deutsch

(74) Anwalt: EISENFÜHR, SPEISER & PARTNER; Anna-Louisa-Karsch-Strasse 2, 10178 Berlin (DE).

(30) Angaben zur Priorität:
10 2006 020 093.4 26. April 2006 (26.04.2006) DE

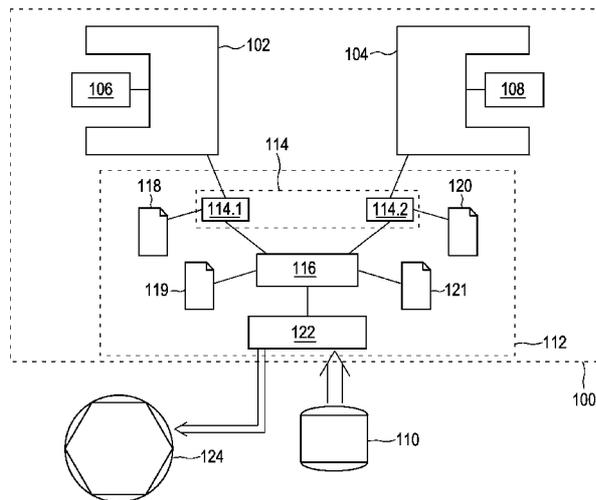
(81) Bestimmungsstaaten (*soweit nicht anders angegeben, für jede verfügbare nationale Schutzrechtsart*): AE, AG, AL, AM, AT, AU, AZ, BA, BB, BG, BH, BR, BW, BY, BZ, CA, CH, CN, CO, CR, CU, CZ, DE, DK, DM, DZ, EC, EE, EG,

(71) Anmelder (*für alle Bestimmungsstaaten mit Ausnahme von US*): IHP GMBH - INNOVATIONS FOR HIGH

[Fortsetzung auf der nächsten Seite]

(54) Title: PROTECTED EXECUTION OF A SERVICE PROVIDER'S DATA PROCESSING APPLICATION FOR A USER BY MEANS OF A TRUSTWORTHY EXECUTION ENVIRONMENT

(54) Bezeichnung: GESCHÜTZTES AUSFÜHREN EINER DATENVERARBEITUNGSANWENDUNG EINES DIENSTANBIETERS FÜR EINEN NUTZER DURCH EINE VERTRAUENSWÜRDIGE AUSFÜHRUNGSUMGEBUNG



(57) Abstract: The invention relates to an execution container for a service provider's data processing application. Said execution container comprises at least one execution environment, a communication interface that is connected to the execution environment, and a security control unit which is connected to the communication interface and is configured so as to prevent the data processing application from communicating data with any communication terminal external to the execution environment if the data communication path circumvents the execution environment. An access control unit is also provided which is connected to the communication interface and is configured so as to prevent the execution environment from communicating data with any communication terminal which is external to the execution container and is not defined as authorized through a first security agreement.

(57) Zusammenfassung: Die Erfindung betrifft einen Ausführungscontainer für eine Datenverarbeitungsanwendung eines Diensteanbieters. Neben mindestens einer Ausführungsumgebung und einer mit der Ausführungsumgebung verbundenen Kommunikationsschnittstelle enthält der Ausführungscontainer

[Fortsetzung auf der nächsten Seite]



WO 2007/122266 A3



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, MG, MK, MN, MW, MX, MY, MZ, NA, NG, NI, NO, NZ, OM, PG, PH, PL, PT, RO, RS, RU, SC, SD, SE, SG, SK, SL, SM, SV, SY, 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, 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, MT, 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).

Erklärung gemäß Regel 4.17:

— *Erfindererklärung (Regel 4.17 Ziffer iv)*

Veröffentlicht:

— *mit internationalem Recherchenbericht*

(88) Veröffentlichungsdatum des internationalen

Recherchenberichts:

17. Januar 2008

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.

eine mit der Kommunikationsschnittstelle verbundene Sicherheitssteuerungseinheit, die ausgebildet ist, solche Datenkommunikation der Datenverarbeitungsanwendung mit jeglichem relativ zur Ausführungsumgebung externen Kommunikationsendpunkt zu verhindern, deren Kommunikationspfad die Ausführungsumgebung umgeht. Weiterhin ist eine mit der Kommunikationsschnittstelle verbundene Zugriffssteuerungseinheit vorhanden, die ausgebildet ist, solche Datenkommunikation der Ausführungsumgebung mit jeglichem relativ zum Ausführungscontainer externen Kommunikationsendpunkt zu verhindern, der nicht durch eine erste Sicherheitsvereinbarung als zulässig definiert ist.

INTERNATIONAL SEARCH REPORT

International application No
PCT/EP2007/054117

A. CLASSIFICATION OF SUBJECT MATTER
INV. H04L29/06 G06F9/46 G06F21/00

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 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.
X	US 2004/268356 A1 (WHITE PETER DUNCAN [US] ET AL) 30 December 2004 (2004-12-30)	1-3,6, 10,11, 15-18
Y	abstract; figure 14 paragraph [0009] paragraph [0051] - paragraph [0059] paragraph [0067]	4,5
Y	US 2003/158960 A1 (ENGBERG STEPHAN J [US]) 21 August 2003 (2003-08-21) cited in the application paragraph [0018]; figure 5	4,5
X	US 2004/025016 A1 (FOCKE MICHEL W [US] ET AL FOCKE MICHAEL W [US] ET AL) 5 February 2004 (2004-02-05) paragraph [0009] - paragraph [0015] paragraph [0070] - paragraph [0077] paragraph [0102] - paragraph [0116]	1,18

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	"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
"E" earlier document but published on or after the international filing date	"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
"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)	"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.
"O" document referring to an oral disclosure, use, exhibition or other means	"&" document member of the same patent family
"P" document published prior to the international filing date but later than the priority date claimed	

Date of the actual completion of the international search 8 August 2007	Date of mailing of the international search report 02. 11. 07
---	---

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 Figiel, Barbara
---	--

Box No. II Observations where certain claims were found unsearchable (Continuation of item 2 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 No. III Observations where unity of invention is lacking (Continuation of item 3 of first sheet)

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

See additional 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 additional fees, this Authority did not invite payment of additional fees.
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.:

1-6,10-11,15-18

Remark on Protest

- The additional search fees were accompanied by the applicant's protest and, where applicable, the payment of a protest fee.
- The additional search fees were accompanied by the applicant's protest but the applicable protest fee was not paid within the time limit specified in the invitation.
- No protest accompanied the payment of additional search fees.

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

1. Claims 1-6, 10-11, 15-18

A negotiation unit for negotiating the first security agreement between an execution container and a service user via the negotiation interface according to a predefined negotiation protocole [claim 4].

2. Claims 7-9

Causing the erasure of user input data and user output data of the data processing application, which are stored in the memoy, on completion of the execution of the data processing application [claim 7].

3. Claims 12-13

Sending a literal selected from a set of predefined literals to a communication terminal external to the execution container via the communication interface and on a command received by the data processing application [claim 12].

4. Claim 14

Varying a processor load in accordance with a random time pattern which is independent from the actual load by the data processing application [claim 4].

INTERNATIONAL SEARCH REPORT

Information on patent family members

International application No

PCT/EP2007/054117

Patent document cited in search report	Publication date	Patent family member(s)	Publication date
US 2004268356 A1	30-12-2004	AU 773730 B2	03-06-2004
		AU 1654901 A	30-05-2001
		EP 1232436 A2	21-08-2002
		GB 2372358 A	21-08-2002
		JP 2003524829 T	19-08-2003
		WO 0137086 A2	25-05-2001
		US 6772416 B1	03-08-2004

US 2003158960 A1	21-08-2003	NONE	

US 2004025016 A1	05-02-2004	US 2007130458 A1	07-06-2007
		US 2007056036 A1	08-03-2007
		US 2007056037 A1	08-03-2007
		US 2007118900 A1	24-05-2007
		US 2007118901 A1	24-05-2007
		US 2007118902 A1	24-05-2007

INTERNATIONALER RECHERCHENBERICHT

Internationales Aktenzeichen

PCT/EP2007/054117

A. KLASSIFIZIERUNG DES ANMELDUNGSGEGENSTANDES
 INV. H04L29/06 G06F9/46 G06F21/00

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

B. RECHERCHIERTE GEBIETE

Recherchierter Mindestprüfstoff (Klassifikationssystem und Klassifikationssymbole)
 H04L 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.
X	US 2004/268356 A1 (WHITE PETER DUNCAN [US] ET AL) 30. Dezember 2004 (2004-12-30)	1-3,6, 10,11, 15-18
Y	Zusammenfassung; Abbildung 14 Absatz [0009] Absatz [0051] - Absatz [0059] Absatz [0067]	4,5
Y	US 2003/158960 A1 (ENGBERG STEPHAN J [US]) 21. August 2003 (2003-08-21) in der Anmeldung erwähnt Absatz [0018]; Abbildung 5	4,5
X	US 2004/025016 A1 (FOCKE MICHEL W [US] ET AL FOCKE MICHAEL W [US] ET AL) 5. Februar 2004 (2004-02-05) Absatz [0009] - Absatz [0015] Absatz [0070] - Absatz [0077] Absatz [0102] - Absatz [0116]	1,18

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	Absenddatum des internationalen Recherchenberichts
8. August 2007	02. 11. 07

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 Figiel, Barbara
---	--

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 Recherchegebühren 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 Recherchegebühr gerechtfertigt hätte, hat die Behörde nicht zur Zahlung einer solchen Gebühr aufgefordert.

3. Da der Anmelder nur einige der erforderlichen zusätzlichen Recherchegebühren 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 Recherchegebühren nicht rechtzeitig entrichtet. Der internationale Recherchenbericht beschränkt sich daher auf die in den Ansprüchen zuerst erwähnte Erfindung; diese ist in folgenden Ansprüchen erfaßt:
1-6,10-11,15-18

Bemerkungen hinsichtlich eines Widerspruchs

- Die zusätzlichen Gebühren wurden vom Anmelder unter Widerspruch gezahlt.
- Die Zahlung zusätzlicher Recherchegebühren 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: 1-6, 10-11, 15-18

eine Verhandlungseinheit um über die Verhandlungsschnittstelle entsprechend einem vordefinierten Verhandlungsprotokoll die erste Sicherheitsvereinbarung zwischen einem dem Ausführungscontainer und einem Dienstanutzer auszuhandeln [Anspruch 4]

2. Ansprüche: 7-9

nach Abschluss der Ausführung der Datenverarbeitungsanwendung eine Löschung im Speicher abgelegter Nutzereingabedaten und Nutzerausgabedaten der Datenverarbeitungsanwendung zu veranlassen [Anspruch 7]

3. Ansprüche: 12-13

auf ein von der Datenverarbeitungsanwendung her empfangenes Kommando hin über die Kommunikationsschnittstelle ein im Kommando angegebenes, aus einem Satz vordefinierter Literale ausgewähltes Literal an einen relativ zum Ausführungscontainer externen Kommunikationsendpunkt zu senden [Anspruch 12]

4. Anspruch: 14

eine Prozessorlast nach einem zufälligen Zeitmuster zu variieren, das unabhängig von einer tatsächlichen Belastung durch die Datenverarbeitungsanwendung ist [Anspruch 14]

INTERNATIONALER RECHERCHENBERICHT

Angaben zu Veröffentlichungen, die zur selben Patentfamilie gehören

Internationales Aktenzeichen

PCT/EP2007/054117

Im Recherchenbericht angeführtes Patentdokument	Datum der Veröffentlichung	Mitglied(er) der Patentfamilie	Datum der Veröffentlichung
US 2004268356 A1	30-12-2004	AU 773730 B2	03-06-2004
		AU 1654901 A	30-05-2001
		EP 1232436 A2	21-08-2002
		GB 2372358 A	21-08-2002
		JP 2003524829 T	19-08-2003
		WO 0137086 A2	25-05-2001
		US 6772416 B1	03-08-2004

US 2003158960 A1	21-08-2003	KEINE	

US 2004025016 A1	05-02-2004	US 2007130458 A1	07-06-2007
		US 2007056036 A1	08-03-2007
		US 2007056037 A1	08-03-2007
		US 2007118900 A1	24-05-2007
		US 2007118901 A1	24-05-2007
		US 2007118902 A1	24-05-2007
