

(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  
25. März 2010 (25.03.2010)

PCT

(10) Internationale Veröffentlichungsnummer  
WO 2010/031700 A3

- (51) Internationale Patentklassifikation:  
H04L 12/22 (2006.01) H04L 29/06 (2006.01)
- (21) Internationales Aktenzeichen: PCT/EP2009/061476
- (22) Internationales Anmeldedatum:  
4. September 2009 (04.09.2009)
- (25) Einreichungssprache: Deutsch
- (26) Veröffentlichungssprache: Deutsch
- (30) Angaben zur Priorität:  
10 2008 042 262.2  
22. September 2008 (22.09.2008) DE  
10 2008 042 582.6  
2. Oktober 2008 (02.10.2008) DE
- (71) Anmelder (für alle Bestimmungsstaaten mit Ausnahme von US): **BUNDESDRUCKEREI GMBH** [DE/DE]; Oranienstraße 91, 10958 Berlin (DE).
- (72) Erfinder; und
- (75) Erfinder/Anmelder (nur für US): **DIETRICH, Frank** [DE/DE]; Berberitzenweg 25, 12437 Berlin (DE). **PAESCHKE, Manfred** [DE/DE]; An der Wildbahn 61, 16348 Wandlitz (DE). **FIEDLER, Robert** [DE/DE]; Herbert-Baum-Straße 8, 13088 Berlin (DE).
- (74) Anwalt: **RICHARDT, Markus**; Leergasse 11, 65343 Eltville am Rhein (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, 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, HR, HU, IE, IS, IT, LT, LU, LV, MC, MK, MT, NL, NO, PL, PT, RO, SE, SI, SK, SM, TR), OAPI (BF, BJ, CF, CG, CI, CM, GA, GN, GQ, GW, ML, MR, NE, SN, TD, TG).

[Fortsetzung auf der nächsten Seite]

(54) Title: METHOD COMPUTER PROGRAMME PRODUCT AND SYSTEM FOR AUTHENTICATING A USER OF A TELECOMMUNICATION NETWORK

(54) Bezeichnung : VERFAHREN, COMPUTERPROGRAMMPRODUKT UND SYSTEM ZUR AUTHENTIFIZIERUNG EINES BENUTZERS EINES TELEKOMMUNIKATIONSNETZWERKES

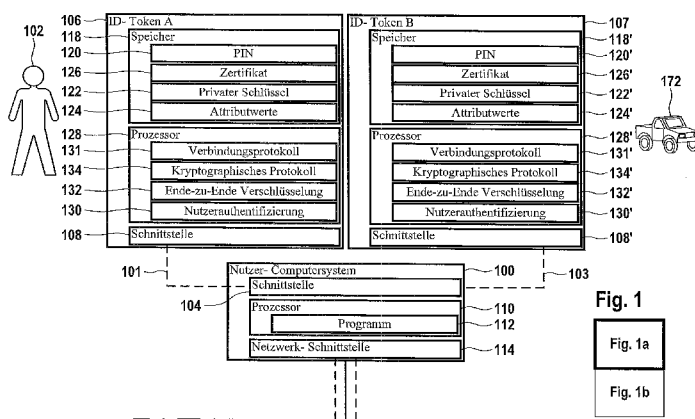


Fig. 1

Fig. 1a

Fig. 1b

- 106, 107 ID-token A, B
- 118 Memory
- 120 PIN
- 126 Certificate
- 122 Private key
- 124 Attribute values
- 110, 128 Processor
- 131 Connection protocol
- 134 Cryptographic protocol
- 132 End-to-end encoding
- 130 User authentication
- 101, 108 Interface
- 100 User computer system
- 112 Programme
- 114 Network interface

(57) Abstract: The invention relates to a telecommunication method with the following steps: establishing a first connection (101) between a first ID-token (106) and a first computer system (136) via a second computer system (100) for reading out at least a first attribute from the first ID-token, generating a first soft-token, wherein the first Soft-Token comprises at least a first attribute and a time stamp and the first soft-token is signed by the first computer system, transmitting the first soft-token from the first computer system to a third computer system (150), wherein the first connection is a connection with end-to-end encoding.

(57) Zusammenfassung: Die Erfindung betrifft ein Telekommunikationsverfahren mit folgenden Schritten: Aufbau einer ersten Verbindung (101) zwischen einem ersten ID-Token (106) und einem ersten Computersystem (136) über ein zweites Computersystem (100) zum Auslesen zumindest eines ersten Attributs aus dem ersten ID-Token, Generierung eines ersten Soft-Tokens, wobei der erste Soft-Token das zumindest eine erste Attribut und eine Zeitangabe beinhaltet, und wobei der erste Soft-Token von dem ersten Computersystem signiert ist, Senden des ersten Soft-Tokens von dem ersten Computersystem an ein drittes Computersystem (150), wobei es sich bei der ersten

Verbindung um eine Verbindung mit Ende-zu-Ende-Verschlüsselung handelt.



**Veröffentlicht:**

- *mit internationalem Recherchenbericht (Artikel 21 Absatz 3)*
- *vor Ablauf der für Änderungen der Ansprüche geltenden Frist; Veröffentlichung wird wiederholt, falls Änderungen eingehen (Regel 48 Absatz 2 Buchstabe h)*

**(88) Veröffentlichungsdatum des internationalen Recherchenberichts:**

1. Juli 2010

**INTERNATIONAL SEARCH REPORT**

International application No <b>PCT/EP2009/061476</b>
--

**A. CLASSIFICATION OF SUBJECT MATTER**  
 INV. H04L12/22 H04L29/06  
 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**

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 1 802 155 A1 (CRONTO LTD [GB]) 27 June 2007 (2007-06-27) paragraphs [0009], [0042] - [0046]	1-26
A	DE 103 06 338 A1 (KAPPE GABRIELE [DE]) 26 August 2004 (2004-08-26) paragraphs [0001] - [0015]; claims 1-9	1-26

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 <b>8 April 2010</b>	Date of mailing of the international search report <b>16/04/2010</b>
--	---

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  <b>Veen, Gerardus</b>
--	---

# INTERNATIONAL SEARCH REPORT

Information on patent family members

International application No

PCT/EP2009/061476

Patent document cited in search report	Publication date	Patent family member(s)	Publication date	
EP 1802155	A1	27-06-2007	EP 1969880 A1	17-09-2008
			WO 2007072001 A1	28-06-2007
			US 2008307515 A1	11-12-2008
-----				
DE 10306338	A1	26-08-2004	NONE	
-----				

**INTERNATIONALER RECHERCHENBERICHT**

Internationales Aktenzeichen

PCT/EP2009/061476

**A. KLASSIFIZIERUNG DES ANMELDUNGSGEGENSTANDES**  
 INV. H04L12/22 H04L29/06  
 ADD.

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

**B. RECHERCHIERTE GEBIETE**

Recherchierter Mindestprüfstoff (Klassifikationssystem und Klassifikationssymbole)  
 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*	Bezeichnung der Veröffentlichung, soweit erforderlich unter Angabe der in Betracht kommenden Teile	Betr. Anspruch Nr.
X	EP 1 802 155 A1 (CRONTO LTD [GB]) 27. Juni 2007 (2007-06-27) Absätze [0009], [0042] - [0046]	1-26
A	DE 103 06 338 A1 (KAPPE GABRIELE [DE]) 26. August 2004 (2004-08-26) Absätze [0001] - [0015]; Ansprüche 1-9	1-26

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. April 2010	16/04/2010

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  Veen, Gerardus
--	---

**INTERNATIONALER RECHERCHENBERICHT**

Angaben zu Veröffentlichungen, die zur selben Patentfamilie gehören

Internationales Aktenzeichen

**PCT/EP2009/061476**

Im Recherchenbericht angeführtes Patentdokument	Datum der Veröffentlichung	Mitglied(er) der Patentfamilie	Datum der Veröffentlichung	
EP 1802155	A1	27-06-2007	EP 1969880 A1	17-09-2008
			WO 2007072001 A1	28-06-2007
			US 2008307515 A1	11-12-2008
-----				
DE 10306338	A1	26-08-2004	KEINE	
-----				