(12) DEMANDE INTERNATIONALE PUBLIÉE EN VERTU DU TRAITÉ DE COOPÉRATION EN MATIÈRE DE BREVETS (PCT)

(19) Organisation Mondiale de la Propriété Intellectuelle
Bureau international

(43) Date de la publication internationale
30 septembre 2010 (30.09.2010)

PCT

(10) Numéro de publication internationale
WO 2010/108994 A3

(51) Classification internationale des brevets :
H04L 9/08 (2006.01)

(21) Numéro de la demande internationale :
PCT/EP2010/053953

(22) Date de dépôt international :
25 mars 2010 (25.03.2010)

(25) Langue de dépôt : français

(26) Langue de publication : français

(30) Données relatives à la priorité :
09 01441 26 mars 2009 (26.03.2009) FR
09 01442 26 mars 2009 (26.03.2009) FR

(71) Déposant *(pour tous les États désignés sauf US)* : **TRUSTSEED** [FR/FR]; 23, avenue du Lieutel, F-78490 Galluis (FR).

(72) Inventeur; et

(75) Inventeur/Déposant *(pour US seulement)* : **BLOT-LEFEVRE, Eric** [FR/FR]; 53, Boulevard Victor Hugo, F-92200 Neuilly-sur-seine (FR).

(74) Mandataire : **NGUYEN-VAN-YEN, Christian**; Immeuble "Visium", 22, avenue Aristide Briand, F-94117 Arcueil Cedex (FR).

(81) États désignés *(sauf indication contraire, pour tout titre de protection nationale disponible)* : 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.

[Suite sur la page suivante]

(54) Title : METHOD AND DEVICE FOR ARCHIVING A DOCUMENT

(54) Titre : PROCEDE ET DISPOSTIF D'ARCHIVAGE D'UN DOCUMENT

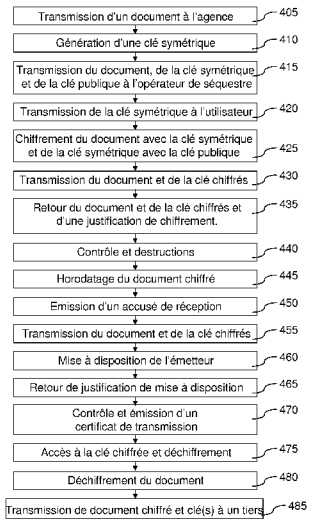

Figure 5

405 Send a document to the agency
410 Generate a symmetric key
415 Send the document, the symmetric key, and the public key to the receiving operator
420 Send the symmetric key to the user
425 Encrypt the document with a symmetric key, and encrypt the symmetric key with the public key
430 Send encrypted document and encrypted key
435 Return encrypted document and encrypted key and confirmation of the encryption
440 Check and destroy
445 Timestamp the encrypted document
450 Send confirmation of receipt
455 Send the encrypted document and encrypted key
460 Make available by sender
465 Return confirmation of making available
470 Check and send a transmission certificate
475 Access and decrypt the encrypted key
480 Decrypt the document
485 Send encrypted document and key(s) to a third party

(57) Abstract : The invention relates to a method for archiving a document, including: a step (225, 325, 425, 525) of encrypting the document with a symmetric key; a step (230, 330, 430, 530) of sending said encrypted document to an archiving operator; and a step of sending the symmetric key for encrypting said document to a receiving operator separate from the archiving operator. In certain embodiments, the method comprises a step (425, 525) of encrypting the symmetric key with a key consisting of a dual key comprising asymmetric keys. During the step of encrypting with the asymmetric key, the asymmetric key is that of the user having sent said document or that of the recipient of the document, depending on whether the method is used for personal archiving or for document transmission.

(57) Abrégé : Le procédé d'archivage d'un document comprend : - une étape (225, 325, 425, 525) de chiffrement du document avec une clé symétrique, - une étape (230, 330, 430, 530) de transmission dudit document chiffré à un opérateur d'archivage, - une étape de transmission de la clé symétrique de chiffrement dudit document à un opérateur de séquestre distinct de l'opérateur d'archivage. Dans des modes de réalisation, le procédé comporte une étape (425, 525) de chiffrement de la clé symétrique avec une clé d'un bi-clés de clés asymétriques. Selon qu'il est appliqué à l'archivage personnel ou à la transmission de document, au cours de l'étape de chiffrement avec la clé asymétrique, la clé asymétrique est celle de l'utilisateur ayant transmis ledit document ou celle du destinataire du document.

WO 2010/108994 A3

(84) États désignés *(sauf indication contraire, pour tout titre de protection régionale disponible)* : ARIPO (BW, GH, GM, KE, LR, LS, MW, MZ, NA, SD, SL, SZ, TZ, UG, ZM, ZW), eurasien (AM, AZ, BY, KG, KZ, MD, RU, TJ, TM), européen (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).

Publiée :

— *avec rapport de recherche internationale (Art. 21(3))*

— *avant l'expiration du délai prévu pour la modification des revendications, sera republiée si des modifications sont reçues (règle 48.2.h))*

(88) Date de publication du rapport de recherche internationale :

25 novembre 2010

INTERNATIONAL SEARCH REPORT

International application No
PCT/EP2010/053953

A. CLASSIFICATION OF SUBJECT MATTER
INV. H04L9/08
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, PAJ, 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	ERIC GAUTRIN: "VISON : Vers un Intranet Sécurisé Ouvert au Nomadisme" 20060131, [Online] 31 January 2006 (2006-01-31), pages 1-10, XP007914709 Retrieved from the Internet: URL:http://hal.archives-ouvertes.fr/docs/00/05/71/96/PDF/papierJRES05-V7.pdf> [retrieved on 2010-09-01]	1,3,4, 10,12,13
Y	paragraph [0006]	2,5-7,11
A		8,9,14, 15

Y	FR 2 804 561 A (FRANCE TELECOM [FR]) 3 August 2001 (2001-08-03)	2,5-7,11
A	* abstract page 5, line 21 - page 8, line 14 page 11, line 16 - page 15, line 19	3,4,8,9, 12-15

	-/--	

[X] Further documents are listed in the continuation of Box C.

[X] 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
8 September 2010	15/09/2010

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, Fax: (+31-70) 340-3016	Bec, Thierry

INTERNATIONAL SEARCH REPORT

International application No
PCT/EP2010/053953

C(Continuation). DOCUMENTS CONSIDERED TO BE RELEVANT

Category*	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
A	VICTOR SHOUP: "A Proposal for an ISO Standard for Public Key Encryption (version 2.1)" INTERNET CITATION, [Online] 20 December 2001 (2001-12-20), page COMPLETE, XP007910787 Retrieved from the Internet: URL:http://eprint.iacr.org/2001/112.pdf> [retrieved on 2009-12-04] paragraph [0003] - paragraph [0005]	1-15
A	WO 02/093849 A (KASTEN CHASE APPLIED RES LTD [CA]; MULDER DAVID G [CA]; MISKIMMIN ROBE) 21 November 2002 (2002-11-21) * abstract page 5, line 1 - page 8, line 2 claim 1	1-15
A	FR 2 786 049 A (LEFEVRE JEAN PIERRE ROLAND PAU [FR]) 19 May 2000 (2000-05-19) page 4, line 5 - page 5, line 34 page 16, line 8 - page 20, line 27	1-10

INTERNATIONAL SEARCH REPORT

Information on patent family members

International application No
PCT/EP2010/053953

Patent document cited in search report	Publication date	Patent family member(s)	Publication date
FR 2804561 A	03-08-2001	EP 1254534 A1	06-11-2002
		WO 0156222 A1	02-08-2001
		JP 2003521197 T	08-07-2003
		US 2003012387 A1	16-01-2003
WO 02093849 A	21-11-2002	CA 2386491 A1	16-11-2002
FR 2786049 A	19-05-2000	NONE	

RAPPORT DE RECHERCHE INTERNATIONALE

Demande internationale n° PCT/EP2010/053953

A. CLASSEMENT DE L'OBJET DE LA DEMANDE

INV. H04L9/08
ADD.

Selon la classification internationale des brevets (CIB) ou à la fois selon la classification nationale et la CIB

B. DOMAINES SUR LESQUELS LA RECHERCHE A PORTE

Documentation minimale consultée (système de classification suivi des symboles de classement)
H04L

Documentation consultée autre que la documentation minimale dans la mesure où ces documents relèvent des domaines sur lesquels a porté la recherche

Base de données électronique consultée au cours de la recherche internationale (nom de la base de données, et si cela est réalisable, termes de recherche utilisés)
EPO-Internal, PAJ, WPI Data

C. DOCUMENTS CONSIDERES COMME PERTINENTS

Catégorie*	Identification des documents cités, avec, le cas échéant, l'indication des passages pertinents	no. des revendications visées
X	ERIC GAUTRIN: "VISON : Vers un Intranet Sécurisé Ouvert au Nomadisme" 20060131, [Online] 31 janvier 2006 (2006-01-31), pages 1-10, XP007914709 Extrait de l'Internet: URL:http://hal.archives-ouvertes.fr/docs/00/05/71/96/PDF/papierJRES05-V7.pdf> [extrait le 2010-09-01]	1,3,4, 10,12,13
Y	alinéa [0006]	2,5-7,11
A		8,9,14, 15

Y	FR 2 804 561 A (FRANCE TELECOM [FR]) 3 août 2001 (2001-08-03)	2,5-7,11
A	* abrégé page 5, ligne 21 - page 8, ligne 14 page 11, ligne 16 - page 15, ligne 19	3,4,8,9, 12-15

	-/--	

[X] Voir la suite du cadre C pour la fin de la liste des documents

[X] Les documents de familles de brevets sont indiqués en annexe

* Catégories spéciales de documents cités:

"A" document définissant l'état général de la technique, non considéré comme particulièrement pertinent

"E" document antérieur, mais publié à la date de dépôt international ou après cette date

"L" document pouvant jeter un doute sur une revendication de priorité ou cité pour déterminer la date de publication d'une autre citation ou pour une raison spéciale (telle qu'indiquée)

"O" document se référant à une divulgation orale, à un usage, à une exposition ou tous autres moyens

"P" document publié avant la date de dépôt international, mais postérieurement à la date de priorité revendiquée

"T" document ultérieur publié après la date de dépôt international ou la date de priorité et n'appartenant pas à l'état de la technique pertinent, mais cité pour comprendre le principe ou la théorie constituant la base de l'invention

"X" document particulièrement pertinent; l'invention revendiquée ne peut être considérée comme nouvelle ou comme impliquant une activité inventive par rapport au document considéré isolément

"Y" document particulièrement pertinent; l'invention revendiquée ne peut être considérée comme impliquant une activité inventive lorsque le document est associé à un ou plusieurs autres documents de même nature, cette combinaison étant évidente pour une personne du métier

"&" document qui fait partie de la même famille de brevets

Date à laquelle la recherche internationale a été effectivement achevée	Date d'expédition du présent rapport de recherche internationale
8 septembre 2010	15/09/2010

Nom et adresse postale de l'administration chargée de la recherche internationale	Fonctionnaire autorisé
Office Européen des Brevets, P.B. 5818 Patentlaan 2 NL - 2280 HV Rijswijk Tel. (+31-70) 340-2040, Fax: (+31-70) 340-3016	Bec, Thierry

RAPPORT DE RECHERCHE INTERNATIONALE

Demande internationale n° PCT/EP2010/053953

C(suite). DOCUMENTS CONSIDERES COMME PERTINENTS

Catégorie*	Identification des documents cités, avec, le cas échéant, l'indication des passages pertinents	no. des revendications visées
A	VICTOR SHOUP: "A Proposal for an ISO Standard for Public Key Encryption (version 2.1)" INTERNET CITATION, [Online] 20 décembre 2001 (2001-12-20), page COMPLETE, XP007910787 Extrait de l'Internet: URL:http://eprint.iacr.org/2001/112.pdf> [extrait le 2009-12-04] alinéa [0003] - alinéa [0005]	1-15
A	WO 02/093849 A (KASTEN CHASE APPLIED RES LTD [CA]; MULDER DAVID G [CA]; MISKIMMIN ROBE) 21 novembre 2002 (2002-11-21) * abrégé page 5, ligne 1 - page 8, ligne 2 revendication 1	1-15
A	FR 2 786 049 A (LEFEVRE JEAN PIERRE ROLAND PAU [FR]) 19 mai 2000 (2000-05-19) page 4, ligne 5 - page 5, ligne 34 page 16, ligne 8 - page 20, ligne 27	1-10

RAPPORT DE RECHERCHE INTERNATIONALE

Renseignements relatifs aux membres de familles de brevets

Demande internationale n°
PCT/EP2010/053953

Document brevet cité au rapport de recherche		Date de publication	Membre(s) de la famille de brevet(s)		Date de publication
FR 2804561	A	03-08-2001	EP	1254534 A1	06-11-2002
			WO	0156222 A1	02-08-2001
			JP	2003521197 T	08-07-2003
			US	2003012387 A1	16-01-2003
WO 02093849	A	21-11-2002	CA	2386491 A1	16-11-2002
FR 2786049	A	19-05-2000	AUCUN		