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

(19) Organisation Mondiale de la Propriété Intellectuelle
Bureau international

PCT

(43) Date de la publication internationale
19 janvier 2006 (19.01.2006)

(10) Numéro de publication internationale
WO 2006/005685 A1

(51) Classification internationale des brevets[7] : G06F 1/00

(21) Numéro de la demande internationale :
PCT/EP2005/053084

(22) Date de dépôt international : 29 juin 2005 (29.06.2005)

(25) Langue de dépôt : français

(26) Langue de publication : français

(30) Données relatives à la priorité :
0407761 12 juillet 2004 (12.07.2004) FR

(71) Déposant *(pour tous les États désignés sauf US)* : **GEMPLUS** [FR/FR]; Avenue du Pic de Bertagne Parc, d'activité de Gémenos, F-13420 GEMENOS (FR).

(72) Inventeurs; et

(75) Inventeurs/Déposants *(pour US seulement)* : **COULIER, Charles** [FR/FR]; 19 avenue Frédéric Mistral Le Cannet, F-13360 ROQUEVAIRE (FR). **MORVAN, Olwehn** [FR/FR]; Villa Céliandre Chemin Saint Eloi, F-13600 LA CIOTAT (FR).

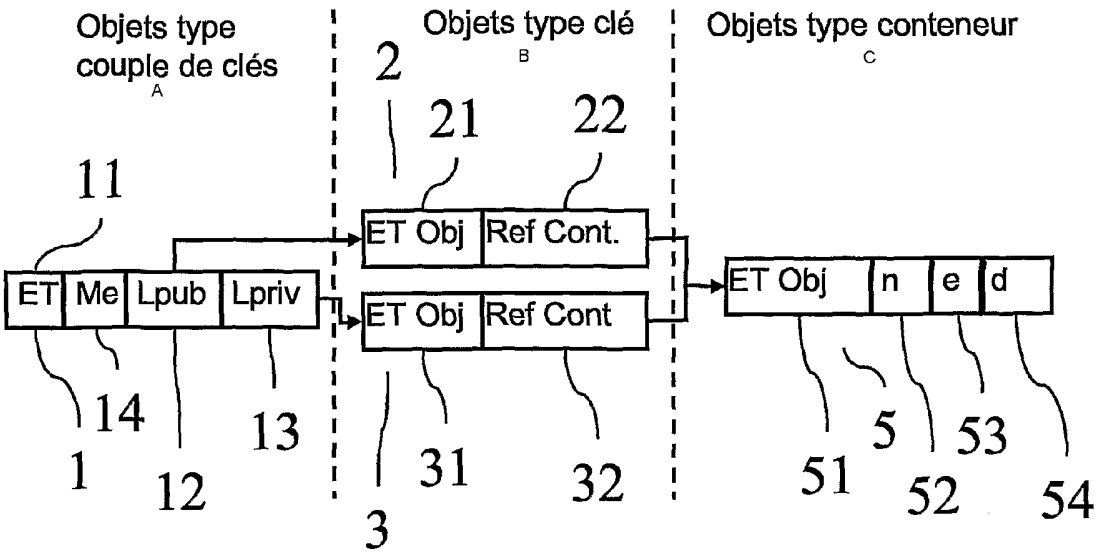
(81) États désignés *(sauf indication contraire, pour tout titre de protection nationale disponible)* : AE, AG, AL, AM, AT, AU, AZ, BA, BB, BG, BR, BW, BY, BZ, CA, CH, CN, CO, CR, CU, CZ, DE, DK, DM, DZ, EC, EE, EG, ES, FI, GB, GD, GE, GH, GM, HR, HU, ID, IL, IN, IS, JP, KE, KG, KM, KP, KR, KZ, LC, LK, LR, LS, LT, LU, LV, 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) États désignés *(sauf indication contraire, pour tout titre de protection régionale disponible)* : ARIPO (BW, GH, GM, KE, 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, HU, IE, IS, IT, LT, LU, MC, 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).

[Suite sur la page suivante]

(54) **Title:** STORAGE OF KEYS OF A PUBLIC KEY ALGORITHM IN AN INTEGRATED ENVIRONMENT

(54) **Titre :** STOCKAGE DE CLES D'UN ALGORITHME A CLE PUBLIQUE DANS UN ENVIRONNEMENT EMBARQUE



A PAIR OF KEYS TYPE OBJECT
B KEY TYPE OBJECT
C CONTAINER TYPE OBJECT

(57) **Abstract:** The invention concerns a method for storing a key of a public key algorithm in a portable apparatus provided with a programme interpreter written in an object-oriented language, said method comprising the following steps: creating in the apparatus at least one container object (5), storing the elements of a private key (54, 72) and at least one element (53, 73) of an associated public key; creating in the apparatus at least one key object (3) not containing any element of the private key or of the associated public key; associating the key object with at least one method for accessing the stored elements in the container object. The invention enables the space occupied by the elements of the keys to be reduced.

[Suite sur la page suivante]

WO 2006/005685 A1

Publiée :

— *avec rapport de recherche internationale*

— *avant l'expiration du délai prévu pour la modification des revendications, sera republiée si des modifications sont reçues*

En ce qui concerne les codes à deux lettres et autres abréviations, se référer aux "Notes explicatives relatives aux codes et abréviations" figurant au début de chaque numéro ordinaire de la Gazette du PCT.

(57) Abrégé : L'invention porte sur un procédé de stockage d'une clé d'un algorithme à clé publique dans un appareil portatif muni d'un interpréteur de programme écrit dans un langage orienté objet, ce procédé comprenant les étapes consistant à : -créer dans l'appareil au moins un objet conteneur (5), mémorisant les éléments d'une clé privée (54, 72) et au moins un élément (53, 73) d'une clé publique associée ; -créer dans l'appareil au moins un objet clé (3) ne contenant aucun élément de la clé privée ou de la clé publique associée ; -associer l'objet clé à au moins une méthode d'accès aux éléments mémorisés dans l'objet conteneur. L'invention permet de réduire l'espace occupé par les éléments des clés.

STOCKAGE DE CLES D'UN ALGORITHME A CLE PUBLIQUE DANS UN ENVIRONNEMENT EMBARQUE

L'invention concerne le stockage de clés pour des algorithmes à clé publique et en particulier le stockage de clés dans des environnements embarqués, par exemple dans des cartes à puce.

Les algorithmes à clé publique nécessitent la mise en œuvre d'une clé publique et d'une clé privée. Ces clés sont mathématiquement liées pour former une paire. Alors que la clé publique est destinée à être diffusée sans aucune restriction, la clé privée doit rester confidentielle pour assurer la sécurité de l'algorithme. Ces clés sont donc en général cloisonnées de façon assez stricte.

Certaines cartes à puce ou appareils portatifs embarquent une machine virtuelle par exemple de type JavaCard (marque déposée), ainsi que des applications faisant appel à des algorithmes à clé publique, tels le RSA (cryptage, signature électronique). Pour ce type de machine virtuelle, il est imposé un accès exclusif très strict respectivement entre la clé publique et la clé privée. Un objet clé publique contient par exemple les éléments n et e (module et exposant public). Les méthodes associées à cet objet clé permettent la lecture de ses éléments par l'utilisateur. Un objet clé privée contient soit les éléments d et n si la clé est stockée au format standard (d étant l'exposant privé et n le module), soit les éléments p, q, dp, dq et iq si la clé est stockée au format CRT. En outre, une classe appelée KeyPair en prenant l'exemple JavaCard est prévue dans le but d'associer une clé publique et une clé privée et de générer ainsi des paires de clés mathématiquement liées.

Le stockage et l'utilisation de telles clés posent problème dans les appareils embarqués et en particulier dans les cartes à puce.

Les clés mémorisées occupent un espace important dans la mémoire de l'appareil, au détriment d'autres applications. Cet espace occupé peut représenter une proportion relativement importante de la mémoire disponible. En outre, pour répondre à la contrainte de l'indépendance stricte entre les clés publiques et les clés privées, le module est dupliqué dans chacune de ces clés. A titre d'exemple, le module d'une clé RSA 2048 occupe au moins 256 octets.

Certaines méthodes d'attaque consistent à forcer la carte à puce à générer des signatures erronées, en la soumettant par exemple à des perturbations de l'alimentation électrique. Une exploitation mathématique d'une signature erronée permet de

déterminer des éléments privés. Certaines cartes mettent en œuvre des algorithmes de vérification de la signature électronique générée. En principe, la vérification de la signature devrait être effectuée au moyen de l'exposant public. Cependant, du fait de l'indépendance stricte entre les clés publique et privée, ni l'exposant public ni les autres éléments publics ne sont mémorisés dans l'objet clé privée. Le niveau de sécurité de la vérification des signatures générées n'est alors pas optimal.

Il existe donc un besoin pour un procédé de stockage d'une clé d'un algorithme à clé publique dans un appareil portatif muni d'un interpréteur de programme écrit dans un langage orienté objet, comprenant les étapes consistant à :

- créer dans l'appareil au moins un objet conteneur (5), mémorisant au moins un élément d'une clé privée (54, 72) et au moins un élément (53, 73) d'une clé publique associée ;

- créer dans l'appareil au moins un objet clé (3) ne contenant aucun élément de la clé privée et de la clé publique associée ;

- associer l'objet clé à au moins une méthode d'accès aux éléments mémorisés dans l'objet conteneur.

Selon une variante, l'étape d'association de l'objet clé à une méthode d'accès consiste à associer à l'objet, dit objet clé publique, une méthode d'accès aux seuls éléments de la clé publique mémorisés dans l'objet conteneur.

Selon une autre variante, l'étape d'association de l'objet clé à une méthode d'accès consiste à associer à l'objet, dit objet clé privée, une méthode d'accès aux seuls éléments de la clé privée mémorisés dans l'objet conteneur.

On peut alors prévoir que le procédé comprenne en outre les étapes consistant à:

- créer dans l'appareil au moins un autre objet clé (3) ne contenant aucun élément de la clé privée ou de la clé publique associée ;

- associer l'autre objet clé, dit objet clé publique, à au moins une méthode d'accès aux seuls éléments de la clé publique mémorisés dans l'objet conteneur.

Selon encore une variante :

- la clé privée et la clé publique sont associées à un algorithme de cryptage RSA en mode standard ;

- l'objet conteneur mémorise les éléments n, e et d, n étant le module RSA, e étant l'exposant public, et d étant l'exposant privé ;

- la méthode d'accès associée à l'objet clé privée fournit en outre un accès à n et d ;

- la méthode d'accès associée à l'objet clé publique fournit un accès uniquement aux éléments n et e.

Selon encore une autre variante :

- la clé privée et la clé publique sont associées à un algorithme de cryptage RSA en mode CRT ;

- l'objet conteneur mémorise les éléments n, e, p, q, dp, dq et iq, tels que dp= d modulo (p-1), dq= d modulo (q-1) et iq = q^{-1} modulo p, n étant le module RSA, p et q étant les nombres premiers distincts, n étant le module RSA et e étant l'exposant public ;

- la méthode d'accès associée à l'objet clé privée fournit en outre un accès à p, q, dp, dq et iq ;

- la méthode d'accès associée à l'objet clé publique fournit un accès uniquement aux éléments n et e.

On peut encore prévoir que l'appareil portatif soit contrôlé par un interpréteur du type Java ou Javacard.

L'invention porte également sur un procédé de signature dans lequel la clé privée et la clé publique sont associées à un algorithme de cryptage RSA, ce procédé comprenant les étapes des procédés de stockage ci-dessus et les étapes suivantes :

- générer une signature électronique associée à la clé privée ;

- lire l'exposant public e par une méthode associée à l'objet conteneur;

- vérifier la signature électronique générée au moyen de l'exposant public e;

- fournir la signature électronique vérifiée sur une sortie de l'appareil électronique.

L'invention porte encore sur un appareil électronique portatif présentant une mémoire mémorisant une application mettant en œuvre un algorithme à clé publique, une clé privée stockée dans la mémoire par l'un quelconque des procédés ci-dessus, et un organe de calcul susceptible d'exécuter ladite application.

Selon une variante, l'appareil électronique portatif est une carte à puce.

D'autres caractéristiques et avantages de l'invention ressortiront clairement de la description qui en est faite ci-après, à titre indicatif et nullement limitatif, en référence aux dessins annexés, dans lesquels :

-la figure 1 illustre des objets mémorisés dans une carte à puce selon une première variante de l'invention ;

-la figure 2 illustre des objets mémorisés dans une carte à puce selon une seconde variante de l'invention.

L'invention propose de créer un objet associé à une clé d'un algorithme à clé publique. Cet objet ne contient aucun élément de la clé publique ou de la clé privée. Un objet conteneur est créé pour mémoriser les éléments de la clé privée et certains éléments de la clé publique. Une méthode d'accès est associée à l'objet clé pour accéder aux éléments mémorisés dans l'objet conteneur.

Le stockage des différents éléments dans un même objet conteneur permet notamment de réduire l'espace mémoire occupé par ces éléments, du fait de la mise en commun de certains d'entre eux (par exemple le module).

L'invention s'applique à un appareil numérique portatif (non représenté), qui embarque au moins une application utilisant un algorithme à clé publique. Cet appareil embarque également un interpréteur de programme écrit en langage orienté objet, tel que Java ou JavaCard (marque déposée). L'interpréteur et l'application sont par exemple mémorisés dans une mémoire non volatile incluse dans l'appareil portatif numérique, telle qu'une EEPROM. L'appareil est également muni de moyens d'exécution de l'application à clé publique.

La figure 1 illustre une première variante de l'invention. Selon cette variante, on crée dans un premier temps un objet « couple de clés » 1 dans la mémoire non volatile de l'appareil. Cet objet 1 présente un entête 11 et est associé à au moins une méthode de génération d'un couple de clés par le champ 14. Cette méthode est appelée et génère de façon connue en soi un couple de clés liées mathématiquement, comprenant une clé publique et une clé privée. On peut également envisager que les clés soient créées au préalable et mémorisées lors d'un chargement dans l'appareil.

Un objet 2 est créé pour la clé publique et un objet 3 est créé pour la clé privée. L'objet 1 présente des champs 12 et 13 comprenant chacun une référence vers

respectivement l'objet clé publique 2 et vers l'objet clé privée 3. Les objets 2 et 3 présentent respectivement les entêtes 21 et 31. Les objets de type clé 2 et 3 sont mémorisés dans une mémoire non volatile de l'appareil. On notera que ces objets 2 et 3 ne contiennent aucun élément du couple de clés créé.

La méthode de génération du couple de clés comprend également la création d'un objet conteneur 5, commun à la clé publique et à la clé privée. Les objets 2 et 3 présentent respectivement des champs 22 et 32 contenant des références à l'objet conteneur 5. Au sein des méthodes de chaque objet clé, on peut accéder à des éléments prédéfinis de l'objet conteneur 5.

Cet objet conteneur 5 comprend un entête 51 et l'ensemble des éléments répartis dans plusieurs champs 52 à 54. L'objet conteneur 5 est également mémorisé dans une mémoire non volatile de l'appareil. Les éléments du couple de clés ne sont pas stockés dans les objets clés mais dans l'objet conteneur 5. Ainsi, les accès à un élément dans l'objet conteneur 5 peuvent être gérés simplement en fonction des méthodes associées aux objets clés 2 et 3. Le cloisonnement entre l'objet clé publique et l'objet clé privée est ainsi réalisé par les méthodes d'accès respectives des objets 2 et 3 aux éléments de l'objet conteneur 5.

Dans l'exemple de la figure 1, les éléments mémorisés dans l'objet conteneur 5 sont associés à un algorithme RSA standard. L'objet clé publique 2 est associé à une méthode d'accès aux éléments publics de l'objet conteneur 5. Ces éléments sont en l'occurrence n (le module) et e (l'exposant public) et sont stockés respectivement dans les champs 52 et 53. L'objet clé publique 2 est également associé à une méthode d'accès aux éléments publics de l'objet conteneur 5. L'objet clé publique 2 n'est en revanche pas associé à une méthode d'accès à un élément privé de l'objet conteneur 5. Ainsi, aucune méthode associée à l'objet clé publique 2 ne permet d'accéder aux éléments de la clé privée.

L'objet clé privée 3 est associé à une méthode d'accès uniquement aux éléments privés de l'objet conteneur 5. Le champ 54 contient les éléments privés (en l'occurrence d correspondant à l'exposant privé). Aucune méthode d'accès associée à l'objet clé privée ne permet de récupérer des éléments de la clé publique.

Selon la variante illustrée à la figure 2, l'appareil mémorise seulement un objet de clé privée 6 et pas d'objet de clé publique. L'objet 6 présente un entête 61 et un

champ 62 contenant une référence à l'objet conteneur 7. L'objet 6 est associé à une méthode d'accès uniquement aux éléments privés (p, q, dp, dq et iq).

L'objet conteneur 7 comprend un entête 71 et des champs d'éléments 72 et 73. Le champ 72 comprend les éléments privés p, q, dp, dq et iq (éléments pour un cryptage RSA en mode CRT, avec dp = d modulo (p-1), dq = d modulo (q-1) et iq = q^{-1} modulo p) et le champ 73 comprend l'élément public e.

Dans ces deux exemples, l'objet conteneur 5 ou 7 peut stocker une méthode de récupération d'éléments publics et en particulier de l'exposant public e. Cette méthode est rendue utilisable uniquement par une fonction de vérification qui utilise l'exposant public e pour tester la validité de signatures générées à partir des éléments privés. Une signature non valide ne sera pas appliquée sur la sortie de l'appareil électronique. Une attaque par injection de faute lors de la génération de la signature sera donc inopérante.

Cette fonction de vérification cryptographique peut être incluse sans accroître excessivement l'espace occupé dans la mémoire non volatile de l'appareil numérique. En effet, un unique exemplaire de l'exposant e est accessible par une méthode d'accès de l'objet clé publique et est utilisable par la fonction de vérification.

REVENDICATIONS

1. Procédé de stockage d'une clé d'un algorithme à clé publique dans un appareil portatif muni d'un interpréteur de programme écrit dans un langage orienté objet, caractérisé en ce qu'il comprend les étapes consistant à :

   - créer dans l'appareil au moins un objet conteneur (5), mémorisant au moins un élément d'une clé privée (54, 72) et au moins un élément (53, 73) d'une clé publique associée ;
   - créer dans l'appareil au moins un objet clé (3), dit objet clé privée, ne contenant aucun élément de la clé privée et de la clé publique associée ;
   - associer l'objet clé privée à au moins une méthode d'accès aux seuls éléments de la clé privée mémorisés dans l'objet conteneur ;
   - créer dans l'appareil au moins un autre objet clé (3), dit objet clé publique, ne contenant aucun élément de la clé privée ou de la clé publique associée ;
   - associer l'objet clé publique, à au moins une méthode d'accès aux seuls éléments de la clé publique mémorisés dans l'objet conteneur.

2. Procédé de stockage selon la revendication 1, caractérisé en ce que :

   - la clé privée et la clé publique sont associées à un algorithme de cryptage RSA en mode standard ;
   - l'objet conteneur mémorise les éléments n, e et d, n étant le module RSA, e étant l'exposant public, et d étant l'exposant privé ;
   - la méthode d'accès associée à l'objet clé privée fournit en outre un accès à n et d ;
   - la méthode d'accès associée à l'objet clé publique fournit un accès uniquement aux éléments n et e.

3. Procédé de stockage selon la revendication 1, caractérisé en ce que :

   - la clé privée et la clé publique sont associées à un algorithme de cryptage RSA en mode CRT ;
   - l'objet conteneur mémorise les éléments n, e, p, q, dp, dq et iq, tels que dp= d modulo (p-1), dq= d modulo (q-1) et $iq = q^{-1}$ modulo p, n étant le module RSA,

p et q étant les nombres premiers distincts, n étant le module RSA et e étant l'exposant public ;

- la méthode d'accès associée à l'objet clé privée fournit en outre un accès à p, q, dp, dq et iq ;
- la méthode d'accès associée à l'objet clé publique fournit un accès uniquement aux éléments n et e.

4. Procédé de stockage selon l'une quelconque des revendications précédentes, caractérisé en ce que l'appareil portatif est contrôlé par un interpréteur du type Java ou Javacard.

5. Procédé de signature dans lequel la clé privée et la clé publique sont associées à un algorithme de cryptage RSA, ce procédé comprenant les étapes du procédé de stockage selon l'une quelconque des revendications précédentes et les étapes suivantes :
   - générer une signature électronique associée à la clé privée ;
   - lire l'exposant public e par une méthode associée à l'objet conteneur;
   - vérifier la signature électronique générée au moyen de l'exposant public e;
   - fournir la signature électronique vérifiée sur une sortie de l'appareil électronique.

6. Appareil électronique portatif, caractérisé en ce qu'il présente une mémoire mémorisant une application mettant en œuvre un algorithme à clé publique, une clé privée stockée dans la mémoire par le procédé selon l'une quelconque des revendications 1 à 5 et un organe de calcul susceptible d'exécuter ladite application.

7. Appareil électronique portatif selon la revendication 6, caractérisé en ce qu'il s'agit d'une carte à puce.

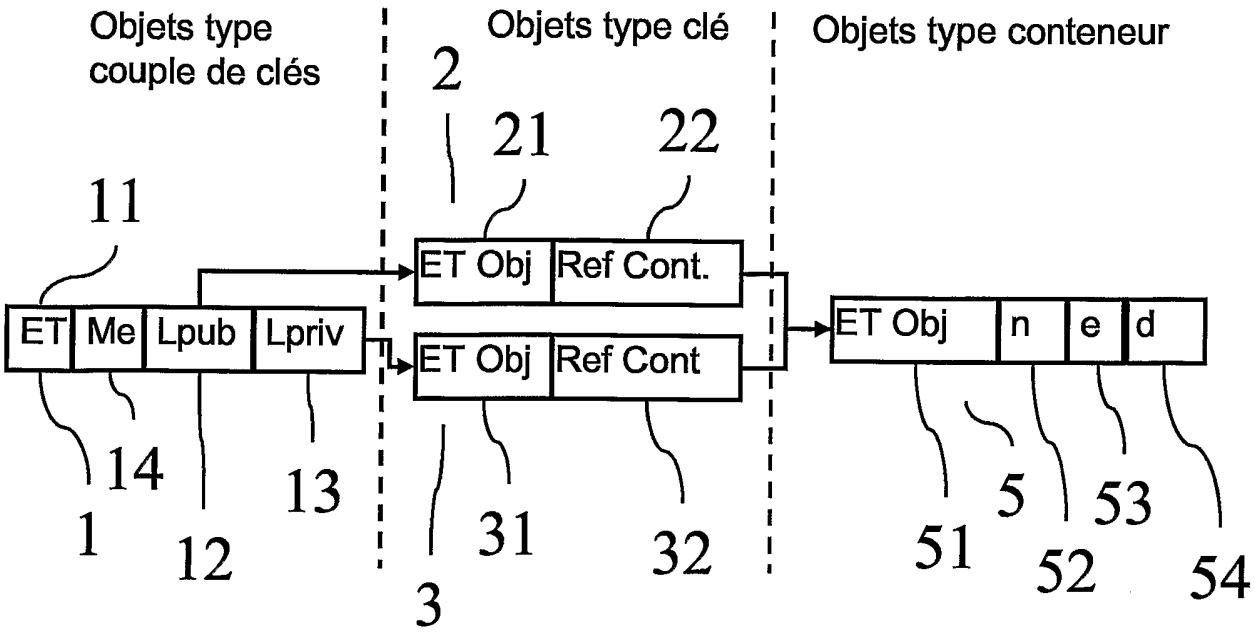

Objets type couple de clés
Objets type clé
Objets type conteneur
2
21
22
11
ET Obj
Ref Cont.
ET
Me
Lpub
Lpriv
ET Obj
Ref Cont
ET Obj
n
e
d
14
13
1
12
3
31
32
51
5
53
52
54

Fig. 1

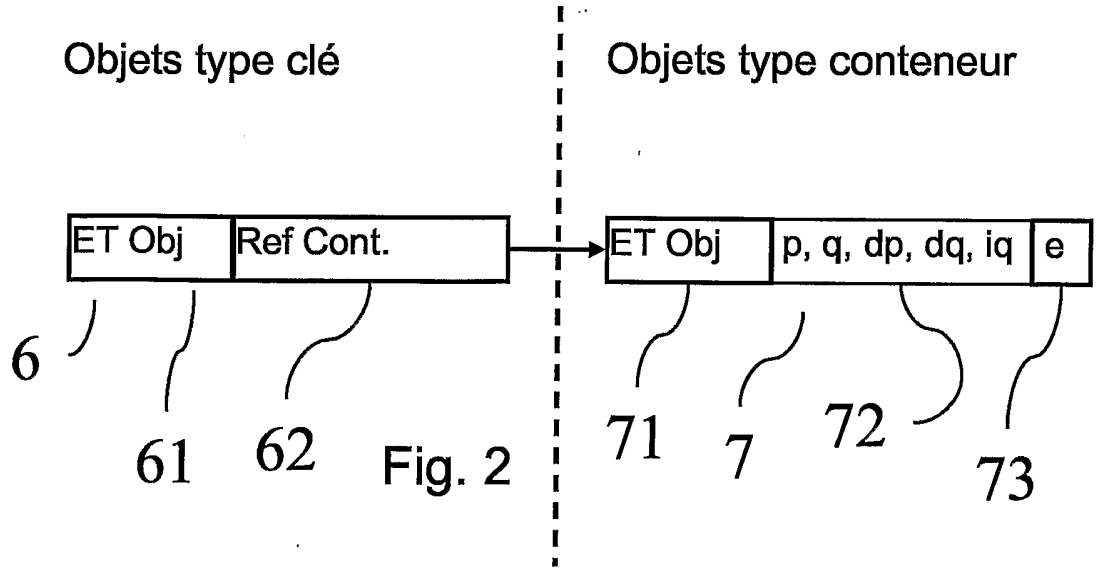

Objets type clé
Objets type conteneur
ET Obj
Ref Cont.
ET Obj
p, q, dp, dq, iq
e
6
61
62
71
7
72
73

Fig. 2

INTERNATIONAL SEARCH REPORT

PCT/EP2005/053084

A. CLASSIFICATION OF SUBJECT MATTER
G06F1/00

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)
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, INSPEC, IBM-TDB

C. DOCUMENTS CONSIDERED TO BE RELEVANT

Category °	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
X	SCHEIBELHOFER K.: "Using Opencard in combination with the java cryptographic architecture for digital signing"" PROCEEDINGS OF GEMPLUS DEVELOPER CONFERENCE GDC'200, 'Online! 20 June 2000 (2000-06-20), XP002321069 MONTPELLIER Retrieved from the Internet: URL:http://www.iaik.tu-graz.ac.at/research /publications/2000/gdc2000.pdf> 'retrieved on 2005-03-10!	1,3,4,6, 7
Y	Paragraphe 2.2.2 Key Handling	5
	-/--	

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

[X] 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	Date of mailing of the international search report
15 November 2005	28/11/2005

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	Veillas, E

C.(Continuation) DOCUMENTS CONSIDERED TO BE RELEVANT

Category °	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
Y	BURTON S. KALISKI, MATTHEW J.B. ROBSHAW: "Comments on Some New Attacks on Cryptographic Devices" RSA LABORATORIES BULLETIN, 'Online! no. 5, 1997, XP002321070 Retrieved from the Internet: URL:http://www.comms.scitech.susx.ac.uk/fft/crypto/RSAbulletin/bulletn5.pdf> 'retrieved on 2005-03-04! Whole document, in particular Section "Overcoming These Basic Attacks"	5
A	JAVA CRYPTOGRAPHY ARCHITECTURE, 'Online! 4 August 2002 (2002-08-04), XP002321071 API SPECIFICATION AND REFERENCE Retrieved from the Internet: URL:http://java.sun.com/j2se/1.4.2/docs/guide/security/CryptoSpec.html#KeystoreLocation> 'retrieved on 2005-03-10! page 26 - page 31 page 34 - page 36	1-7
A	US 2002/120842 A1 (BRAGSTAD HELGE ET AL) 29 August 2002 (2002-08-29) paragraphs '0021! - '0023!; figures 2-4 paragraphs '0031!, '0034!, '0038!	1-7

INTERNATIONAL SEARCH REPORT

PCT/EP2005/053084

Patent document cited in search report	Publication date	Patent family member(s)	Publication date
US 2002120842 A1	29-08-2002	AU 2703902 A	11-06-2002
		WO 0244874 A2	06-06-2002

RAPPORT DE RECHERCHE INTERNATIONALE

PCT/EP2005/053084

A. CLASSEMENT DE L'OBJET DE LA DEMANDE

G06F1/00

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)

G06F

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 réalisable, termes de recherche utilisés)

EPO-Internal, INSPEC, IBM-TDB

C. DOCUMENTS CONSIDERES COMME PERTINENTS

Catégorie °	Identification des documents cités, avec, le cas échéant, l'indication des passages pertinents	no. des revendications visées
X	SCHEIBELHOFER K.: "Using Opencard in combination with the java cryptographic architecture for digital signing"" PROCEEDINGS OF GEMPLUS DEVELOPER CONFERENCE GDC'200, 'Online! 20 juin 2000 (2000-06-20), XP002321069 MONTPELLIER Extrait de l'Internet: URL:http://www.iaik.tu-graz.ac.at/research /publications/2000/gdc2000.pdf> 'extrait le 2005-03-10!	1,3,4,6, 7
Y	Paragraphe 2.2.2 Key Handling	5
	-/--	

[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'appartenenant 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'inven tion revendiquée ne peut être considérée comme nouvelle ou comme impliquant une activité inventive par rapport au document considéré isolément

"Y" document particulièrement pertinent; l'inven tion 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
15 novembre 2005	28/11/2005

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, Tx. 31 651 epo nl, Fax: (+31–70) 340–3016	Veillas, E

RAPPORT DE RECHERCHE INTERNATIONALE

PCT/EP2005/053084

C.(suite) DOCUMENTS CONSIDERES COMME PERTINENTS

Catégorie °	Identification des documents cités, avec, le cas échéant, l'indication des passages pertinents	no. des revendications visées
Y	BURTON S. KALISKI, MATTHEW J.B. ROBSHAW: "Comments on Some New Attacks on Cryptographic Devices" RSA LABORATORIES BULLETIN, 'Online! no. 5, 1997, XP002321070 Extrait de l'Internet: URL:http://www.comms.scitech.susx.ac.uk/fft/crypto/RSAbulletin/bulletn5.pdf> 'extrait le 2005-03-04! Whole document, in particular Section "Overcoming These Basic Attacks"	5
A	JAVA CRYPTOGRAPHY ARCHITECTURE, 'Online! 4 août 2002 (2002-08-04), XP002321071 API SPECIFICATION AND REFERENCE Extrait de l'Internet: URL:http://java.sun.com/j2se/1.4.2/docs/guide/security/CryptoSpec.html#KeystoreLocation> 'extrait le 2005-03-10! page 26 - page 31 page 34 - page 36	1-7
A	US 2002/120842 A1 (BRAGSTAD HELGE ET AL) 29 août 2002 (2002-08-29) alinéas '0021! - '0023!; figures 2-4 alinéas '0031!, '0034!, '0038!	1-7

RAPPORT DE RECHERCHE INTERNATIONALE

PCT/EP2005/053084

Document brevet cité au rapport de recherche	Date de publication	Membre(s) de la famille de brevet(s)	Date de publication
US 2002120842 A1	29-08-2002	AU 2703902 A	11-06-2002
		WO 0244874 A2	06-06-2002