(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
21 août 2003 (21.08.2003)

PCT

(10) Numéro de publication internationale
WO 03/069450 A2

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

(21) Numéro de la demande internationale :
PCT/IB03/00436

(22) Date de dépôt international : 7 février 2003 (07.02.2003)

(25) Langue de dépôt : français

(26) Langue de publication : français

(30) Données relatives à la priorité :
0233/02 12 février 2002 (12.02.2002) CH
0698/02 24 avril 2002 (24.04.2002) CH

(71) Déposant *(pour tous les États désignés sauf US)* : **NAGRACARD SA** [CH/CH]; Route de Genève 22, CH-1033 Cheseaux-sur-Lausanne (CH).

(72) Inventeurs; et

(75) Inventeurs/Déposants *(pour US seulement)* : **BRIQUE, Olivier** [CH/CH]; Chemin de la Perrause 39, CH-1052 Le Mont-sur-Lausanne (CH). **HILL, Michael, John** [CH/CH]; Route de Commugny 10, CH-1296 Coppet (CH). **JOLY, Stéphane** [CH/CH]; Port Roulant 10, CH-2000 Neuchâtel (CH). **COCHARD, Jimmy** [CH/CH]; Chemin d'En-Quettolla 41, CH-1616 Attalens (CH).

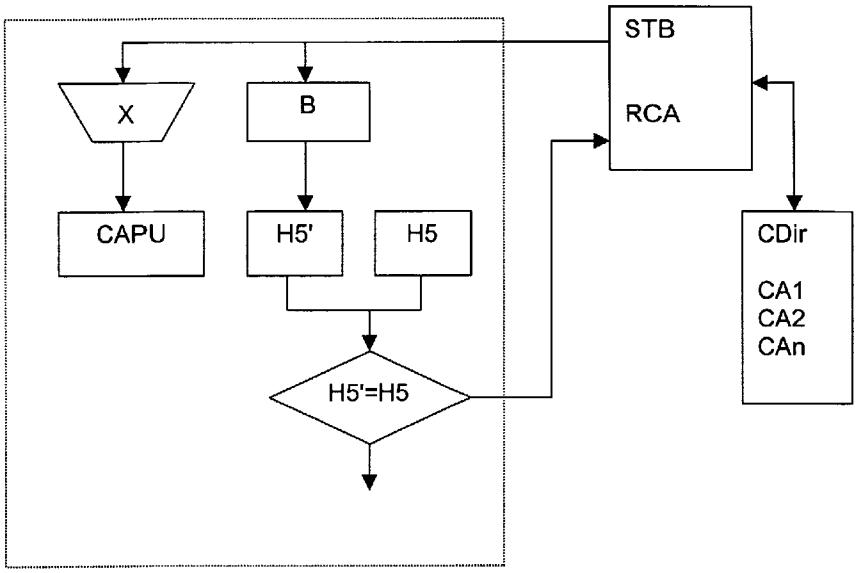
(74) Mandataire : **LEMAN CONSULTING SA**; Route de Clémenty 62, CH-1260 Nyon (CH).

(81) États désignés *(national)* : AE, AG, AL, AM, AT, AU, AZ, BA, BB, BG, BR, BY, BZ, CA, CH, CN, CO, CR, CU, CZ, DE, DK, DM, DZ, EC, EE, ES, FI, GB, GD, GE, GH, GM, HR, HU, ID, IL, IN, IS, JP, KE, KG, KP, KR, KZ, LC, LK, LR, LS, LT, LU, LV, MA, MD, MG, MK, MN, MW, MX, MZ, NO, NZ, OM, PH, PL, PT, RO, RU, SC, SD, SE, SG,

[Suite sur la page suivante]

(54) **Title:** METHOD FOR STORAGE AND TRANSPORT OF AN ELECTRONIC CERTIFICATE

(54) **Titre :** METHODE DE STOCKAGE ET DE TRANSPORT D'UN CERTIFICAT ELECTRONIQUE



(57) **Abstract:** The aim of the invention is to ensure the transportability of an electronic certificate and the security of the private key which forms part of a certificate of type X509, wherein it is important that said certificate is not used for unauthorised purposes by the bearer, such as assuming identity, authorisation of undesired transactions and the reproduction of transactions (replay). Said aim is achieved by means of a method for storage and transport of an electronic certificate, said certificate comprising an authorisation section dedicated to the issuing authority, a bearer section dedicated to the bearer of the certificate and a signature section fixed by the issuing authority, characterised in that all or part of the bearer section is contained in a detachable security module and that at least the authorisation section is contained in a host computer.

[Suite sur la page suivante]

WO 03/069450 A2

SK, SL, TJ, TM, TN, TR, TT, TZ, UA, UG, US, UZ, VC, VN, YU, ZA, ZM, ZW.

(84) États désignés *(régional)* **:** brevet ARIPO (GH, GM, KE, LS, MW, MZ, SD, SL, SZ, TZ, UG, ZM, ZW), brevet eurasien (AM, AZ, BY, KG, KZ, MD, RU, TJ, TM), brevet européen (AT, BE, BG, CH, CY, CZ, DE, DK, EE, ES, FI, FR, GB, GR, HU, IE, IT, LU, MC, NL, PT, SE, SI, SK, TR), brevet OAPI (BF, BJ, CF, CG, CI, CM, GA, GN, GQ, GW, ML, MR, NE, SN, TD, TG).

Publiée :

— *sans rapport de recherche internationale, sera republiée dès réception de ce rapport*

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 : Le but de la présente invention est d'assurer la transportabilité d'un certificat électronique et la sécurité de la clé privée faisant partie d'un certificat du type X509.En effet, il est important que ce certificat ne soit pas utilisé ô des fins non contrôlées par le titulaire, telles que l'usurpation d'identité, l'autorisation de transactions non souhaitées ou la reproduction de transactions (replay).Ce but est atteint par une méthode de stockage et de transport d'un certificat électronique, ledit certificat comprenant une section autorité propre ô l'autorité émettrice, une section titulaire propre au titulaire du certificat et une section signature déterminée par l'autorité émettrice, caractérisée en ce que tout ou partie de la section titulaire est contenue dans un module de sécurité amovible et ce qu'au moins la section autorité est contenue dans un ordinateur hôte.