

(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
29 décembre 2005 (29.12.2005)

PCT

(10) Numéro de publication internationale
WO 2005/124502 A1

(51) Classification internationale des brevets⁷ : **G06F 1/00**,
9/445, H04N 7/24

(74) Mandataire : **WENGER, Joel**; Leman Consulting S.A.,
Route de Clémenty 62, CH-1260 Nyon (CH).

(21) Numéro de la demande internationale :
PCT/EP2005/052797

(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.

(22) Date de dépôt international : 16 juin 2005 (16.06.2005)

(25) Langue de dépôt : français

(26) Langue de publication : français

(30) Données relatives à la priorité :
04102768.1 17 juin 2004 (17.06.2004) EP

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

(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), eurasién (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).

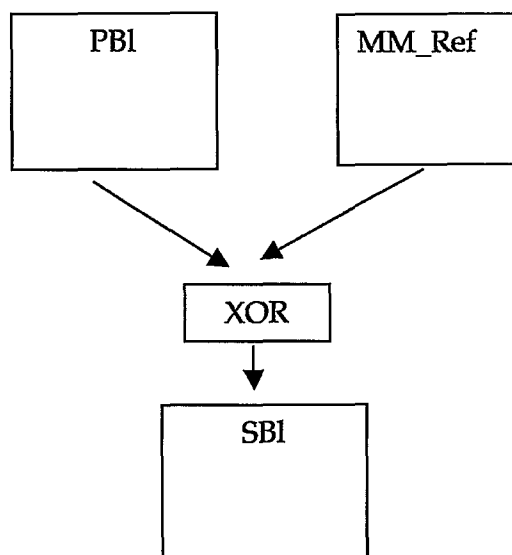
(72) Inventeur; et

(75) Inventeur/Déposant (pour US seulement) : **OSEN, Karl**
[CH/CH]; Route du Mandement 453, CH-1282 Dardagny
(CH).

[Suite sur la page suivante]

(54) Title: METHOD FOR SECURELY UPDATING A PROGRAM BLOCK LOADED IN A SECURITY MODULE

(54) Titre : METHODE DE MISE A JOUR SECURISEE DE LOGICIEL EMBARQUE DANS UN MODULE DE SECURITE



(57) Abstract: The aim of the invention is to offer a method for transmitting a program block-containing message enabling to avoid the consequences of a possible malicious decryption thereof. The inventive method for securely updating a program block loaded in a security module consists in forming a first updating program block (PBI), in determining the target memory area of said security module, in determining a content (MM_Ref) pre-recorded in said target memory area for the module, in forming a second program block (SBI) by mixing entirely or partially said pre-recorded content with the first program block (PBI), in transmitting the second program block (SBI) to the security module, in receiving the second block by the security module, in reading the target memory area (MEM) and in obtaining and writing entirely or partially the first block in the target memory area by the inversely mixing the entire second block or the part thereof with the content of the target memory area.

(57) Abrégé : Le but de la présente invention est de proposer une méthode de transmission d'un message contenant un bloc de programme permettant d'éviter les conséquences d'une éventuelle décryption malveillante de ce message. Ce but est atteint par une méthode de mise à jour sécurisée de

logiciel embarqué dans un module de sécurité, cette méthode comprenant des étapes suivantes: formation d'un premier bloc de programme (PBI) de mise à jour, détermination d'une zone de mémoire cible dudit module de sécurité, détermination pour ledit module de sécurité, d'un contenu préenregistré (MM_Ref) dans ladite zone de mémoire cible, formation d'un second bloc de programme (SBI) obtenu par le mélange de tout ou partie du contenu préenregistré et du premier bloc de programme (PBI), transmission du second bloc de programme (SBI) au module de sécurité, réception du second bloc par le module de sécurité, lecture de la zone de mémoire cible (MEM), obtention et écriture dans la zone de mémoire cible du premier bloc par le mélange inverse de tout ou partie du second bloc et du contenu de la zone de mémoire cible.

WO 2005/124502 A1



Publiée :

— avec rapport de recherche internationale

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.