

(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  
15 décembre 2005 (15.12.2005)

PCT

(10) Numéro de publication internationale  
**WO 2005/119583 A2**

(51) Classification internationale des brevets<sup>7</sup> :

**G06K 19/00**

(72) Inventeur; et

(75) Inventeur/Déposant (pour US seulement) : **KUDELSKI, André** [CH/CH]; Chemin de Bellingard, CH-1095 Lutry (CH).

(21) Numéro de la demande internationale :

PCT/EP2005/052519

(22) Date de dépôt international : 2 juin 2005 (02.06.2005)

(25) Langue de dépôt : français

(26) Langue de publication : français

(30) Données relatives à la priorité :

04102505.7 3 juin 2004 (03.06.2004) 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).

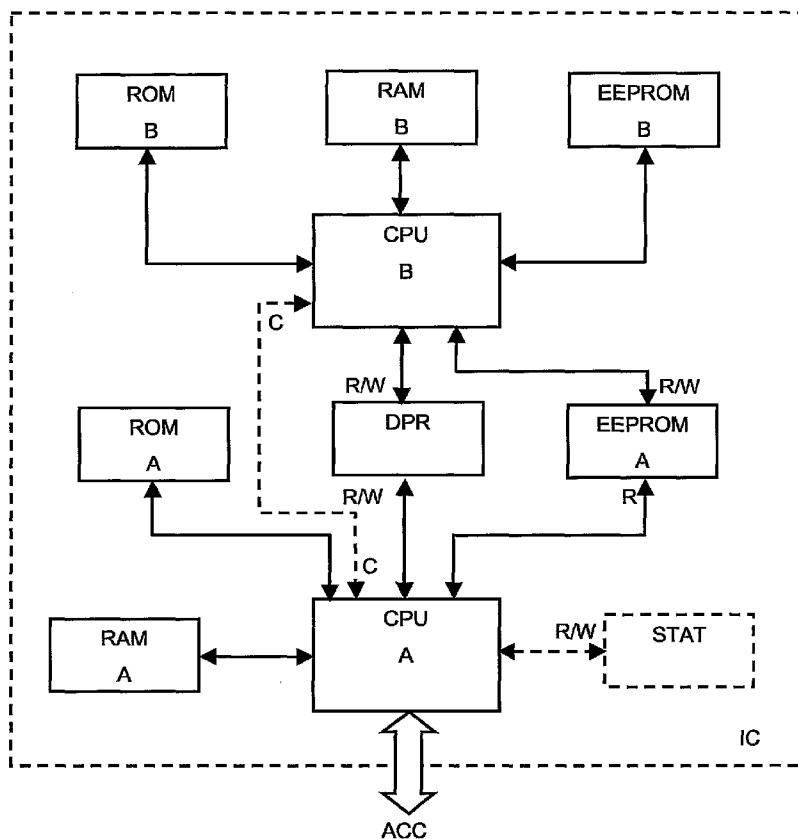
(74) Mandataire : **WENGER, Joel**; Leman Consulting S.A., Route de Clémenty 62, CH-1260 Nyon (CH).

(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,

[Suite sur la page suivante]

(54) Title: SECURITY MODULE COMPONENT

(54) Titre : COMPOSANT POUR MODULE DE SÉCURITÉ



(57) Abstract: The aim of said invention is to optimally improve chipboard security by preventing fraudulent controls by a cryptographic processor or processors which use external signals for disturbing the normal operation of a processor or processors. The inventive security module IC component comprises at least two CPU A and CPU B processors, each of which is connected to ROM A and ROM B program memories, to programmable non-volatile and erasable data-containing memories (EEPROM) EEPROM A and EEPROM B and to random access memories (RAM) RAM A, RAM B for temporary storing data during processing, wherein the first CPU A processor comprises a bus for interfacing with the external of the IC component, the second CPU B processor is connected to the first CPU processor by means of a forwarding memory DPR, the non-volatile programmable and erasable memory EEPROM A of the first CPU A processor has a read access R only thereto and the second CPU B processor is provided with a read/write R/W access to said

non-volatile programmable and erasable memory EEPROM A of the first CPU A processor.

[Suite sur la page suivante]

WO 2005/119583 A2



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), 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).

**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'améliorer de manière optimale la sécurité des cartes à puces en empêchant le contrôle frauduleux du ou des processeurs cryptographiques au moyen de signaux externes venant perturber le déroulement normal des tâches du ou des processeurs. Ce but est atteint par un composant IC de module de sécurité comprenant au moins deux processeurs CPU A, CPU B connectés chacun à des mémoires programme ROM A, ROM B, à des mémoires non-volatiles programmables et effaçables (EEPROM) EEPROM A, EEPROM B contenant des données et à des mémoires vives (RAM) RAM A, RAM B servant au stockage temporaire de données en cours de traitement, le premier processeur CPU A ayant un bus d'interfaçage avec l'extérieur du composant IC, caractérisé en ce que le second processeur CPU B est connecté au premier processeur CPU A par l'intermédiaire d'une mémoire d'échange DPR, la mémoire non-volatile programmable et effaçable EEPROM A du premier processeur CPU A étant uniquement en accès lecture R pour ledit premier processeur CPU A, le second processeur CPU B disposant d'un accès en lecture et écriture R/W sur ladite mémoire non-volatile programmable et effaçable EEPROM A du premier processeur CPU A.