

(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
18 janvier 2007 (18.01.2007)

PCT

(10) Numéro de publication internationale
WO 2007/006735 A1

(51) Classification internationale des brevets :
H04N 7/167 (2006.01) **G07F 7/10** (2006.01)
H04N 5/00 (2006.01)

[CH/CH]; Chemin d'En-Quettolla 41, CH-1616 Attal-
ens (CH).

(21) Numéro de la demande internationale :
PCT/EP2006/063988

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

(22) Date de dépôt international : 6 juillet 2006 (06.07.2006)

(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, HN, HR, HU, ID, IL, IN, IS, JP, KE,
KG, KM, KN, KP, KR, KZ, LA, LC, LK, LR, LS, LT, LU,
LV, LY, MA, MD, MG, MK, MN, MW, MX, MZ, NA, NG,
NI, NO, NZ, OM, PG, PH, PL, PT, RO, RS, RU, SC, SD,
SE, SG, SK, SL, SM, SY, TJ, TM, TN, TR, TT, TZ, UA,
UG, US, UZ, VC, VN, ZA, ZM, ZW.

(25) Langue de dépôt : français

(26) Langue de publication : français

(30) Données relatives à la priorité :
05106185.1 7 juillet 2005 (07.07.2005) EP

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

(72) Inventeurs; et

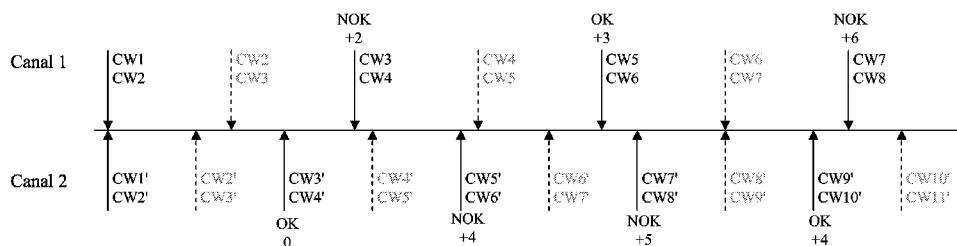
(84) États désignés (sauf indication contraire, pour tout titre
de protection régionale disponible) : ARIPO (BW, GH,
GM, KE, LS, MW, MZ, NA, SD, SL, SZ, TZ, UG, ZM,
ZW), eurasien (AM, AZ, BY, KG, KZ, MD, RU, TJ, TM),

(75) Inventeurs/Déposants (pour US seulement) : **KUDEL-
SKI, Henri** [CH/CH]; Chemin de Sous-Gourze 1,
CH-1091 Grandvaux (CH). **COCHARD, Jimmy**

[Suite sur la page suivante]

(54) Title: METHOD AND DEVICE FOR CONTROLLING ACCESS TO ENCRYPTED DATA

(54) Titre : METHODE ET DISPOSITIF DE CONTROLE D'ACCES A DES DONNEES CHIFFREES



(57) Abstract: The invention concerns a method for controlling access to encrypted data by control words (CW), said control words being received by a security module in control messages (ECM) and returned to a unit operating on (STB) the encrypted data. The method includes the following steps: receiving a first control message (ECM) comprising at least one control word (CW) and a time stamp (TS), receiving a second control message (ECM2) consecutive to the first control message (ECM1), said second message comprising at least one control word (CW) and a time stamp (TS), determining a duration corresponding to the difference between the time stamps (TS) of the two consecutive control messages (ECM1, ECM2), if said duration is less than a predefined duration (CP), incrementing an error counter (CE), and if said duration is not less than said predefined duration, decrementing said error counter (CE), returning the control word (CW) to the operating unit (STB) after a waiting time depending on the value of the error counter (CE).

(57) Abrégé : L'invention concerne une méthode et un dispositif de contrôle d'accès à des données chiffrées par des mots de contrôle (CW), ces mots de contrôle étant reçus par un module de sécurité dans des messages de contrôle (ECM) et retournés à une unité d'exploitation (STB) des données chiffrées. La méthode comprend les étapes suivantes: réception d'un premier message de contrôle (ECM1) comprenant au moins un mot de contrôle (CW) et une marque temporelle (TS), réception d'un second message de contrôle (ECM2) consécutif au premier message de contrôle (ECM1), ce second message comprenant au moins un mot de contrôle (CW) et une marque temporelle (TS), détermination d'une durée correspondant à la différence entre les marques temporelles (TS) des deux messages de contrôle consécutifs (ECM1, ECM2), si cette durée est inférieure à durée pré-définie (CP), incrémentation d'un compteur d'erreurs (CE), si cette durée est égale ou supérieure à ladite durée pré-définie, décrémentation dudit compteur d'erreurs (CE), renvoi du mot de contrôle (CW) à l'unité d'exploitation (STB) après un temps d'attente dépendant de la valeur du compteur d'erreurs (CE).

WO 2007/006735 A1



européen (AT, BE, BG, CH, CY, CZ, DE, DK, EE, ES, FI, FR, GB, GR, HU, IE, IS, IT, LT, LU, LV, 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).

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.

Publiée :

— avec rapport de recherche internationale