

(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 octobre 2012 (18.10.2012)

WIPO | PCT

(10) Numéro de publication internationale
WO 2012/140077 A1

(51) Classification internationale des brevets :
H04L 9/00 (2006.01) H04L 9/08 (2006.01)
G09C 1/10 (2006.01)

THALES, 110 avenue Leclerc, BP 70945, F-49309 Cholet (FR).

(21) Numéro de la demande internationale :
PCT/EP2012/056571

(74) Mandataires : **BLOT, Philippe** et al.; 2, place d'Estienne d'Orves, F-75009 Paris (FR).

(22) Date de dépôt international :
11 avril 2012 (11.04.2012)

(81) États désignés (sauf indication contraire, pour tout titre de protection nationale disponible) : AE, AG, AL, AM, AO, AT, AU, AZ, BA, BB, BG, BH, BR, BW, BY, BZ, CA, CH, CL, CN, CO, CR, CU, CZ, DE, DK, DM, DO, DZ, EC, EE, EG, ES, FI, GB, GD, GE, GH, GM, GT, HN, HR, HU, ID, IL, IN, IS, JP, KE, KG, KM, KN, KP, KR, KZ, LA, LC, LK, LR, LS, LT, LU, LY, MA, MD, ME, MG, MK, MN, MW, MX, MY, MZ, NA, NG, NI, NO, NZ, OM, PE, PG, PH, PL, PT, QA, RO, RS, RU, RW, SC, SD, SE, SG, SK, SL, SM, ST, SV, SY, TH, 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 :
1101105 11 avril 2011 (11.04.2011) FR

(71) Déposant (pour tous les États désignés sauf US) :
THALES [FR/FR]; 45 rue de Villiers, F-92200 Neuilly sur Seine (FR).

(72) Inventeurs; et

(75) Inventeurs/Déposants (pour US seulement) : **BINESSE, Dominique** [FR/FR]; c/o THALES, 110 avenue Leclerc, BP 70945, F-49309 Cholet (FR). **DUPUTZ, Patrick** [FR/FR]; c/o THALES, 160 boulevard de Valmy, BP 82, F-92704 Colombes Cedex (FR). **MACE, Gaël** [FR/FR]; c/o THALES, 110 avenue Leclerc, BP 70945, F-49309 Cholet (FR). **MAILLARD, Romaric** [FR/FR]; c/o

(84) États désignés (sauf indication contraire, pour tout titre de protection régionale disponible) : ARIPO (BW, GH, GM, KE, LR, LS, MW, MZ, NA, RW, SD, SL, SZ, TZ, UG, ZM, ZW), eurasien (AM, AZ, BY, KG, KZ, MD, RU, TJ, TM), européen (AL, AT, BE, BG, CH, CY, CZ, DE, DK, EE, ES, FI, FR, GB, GR, HR, HU, IE, IS, IT, LT, LU, LV, MC, MK, MT, NL, NO, PL, PT, RO, RS, SE, SI, SK, SM, 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 : CRYPTOGRAPHIC EQUIPMENT IMPLEMENTING RED/BLACK COMMUNICATION MODES

(54) Titre : EQUIPEMENT CRYPTOGRAPHIQUE METTANT EN ŒUVRE LES MODES ROUGES ET NOIR DE COMMUNICATION

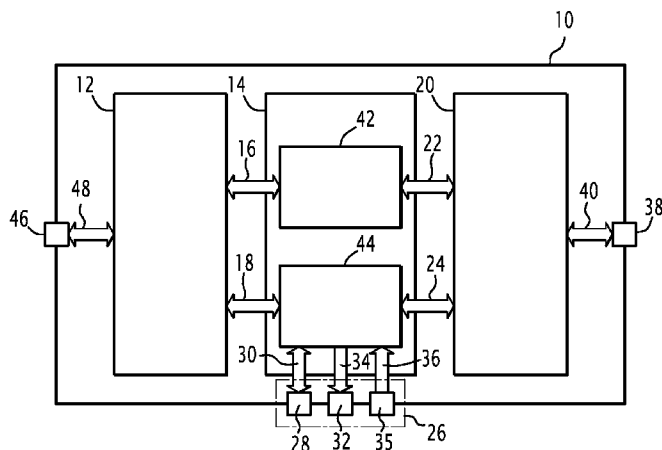


FIG.1

(57) Abstract : The invention relates to cryptographic equipment which includes an input interface, a red module, a cryptographic module, a black module, and an output module. The cryptographic module comprises a cryptographic unit, which interacts with the red module and with the black module, and a management device, which interacts with the input interface and with either the red module or the black module but not with both simultaneously. The cryptographic unit and the management device are physically and logically separate from one another and independent, and have identical protection means capable of protecting the integrity of the management device so as to detect any attempt at tampering.

(57) Abrégé :

[Suite sur la page suivante]



WO 2012/140077 A1



Publiée :

— avec rapport de recherche internationale (Art. 21(3))

L'équipement cryptographique comprend une interface d'entrée, un module rouge, un module cryptographique, un module noir, et une interface de sortie. Le module cryptographique comporte un bloc cryptographique interagissant d'une part avec le module rouge, et d'autre part avec le module noir, et un dispositif de gestion, interagissant avec l'interface d'entrée et avec soit le module rouge, soit le module noir à l'exclusion des deux simultanément. Le bloc cryptographique et le dispositif de gestion sont physiquement et logiquement distincts l'un de l'autre et autonomes, et disposent de moyen de protection identiques, propres à protéger en intégrité le dispositif de gestion afin de détecter toute tentative d'altération.