(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
30 septembre 2004 (30.09.2004)

PCT

(10) Numéro de publication internationale
WO 2004/084049 A1

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

(21) Numéro de la demande internationale :
PCT/FR2004/000601

(22) Date de dépôt international : 12 mars 2004 (12.03.2004)

(25) Langue de dépôt : français

(26) Langue de publication : français

(30) Données relatives à la priorité :
03/03036 12 mars 2003 (12.03.2003) FR

(71) Déposant et
(72) Inventeur : DEBIEZ, Jacques [FR/FR]; 229, chemin de Tucaut/Saint Simon, F-31270 Cugnaux (FR).

(74) Mandataire : MORELLE, Guy; Cabinet Morelle & Bardou, SC, 9 avenue de l'Europe, BP 53, F-31527 Ramonville Cedex (FR).

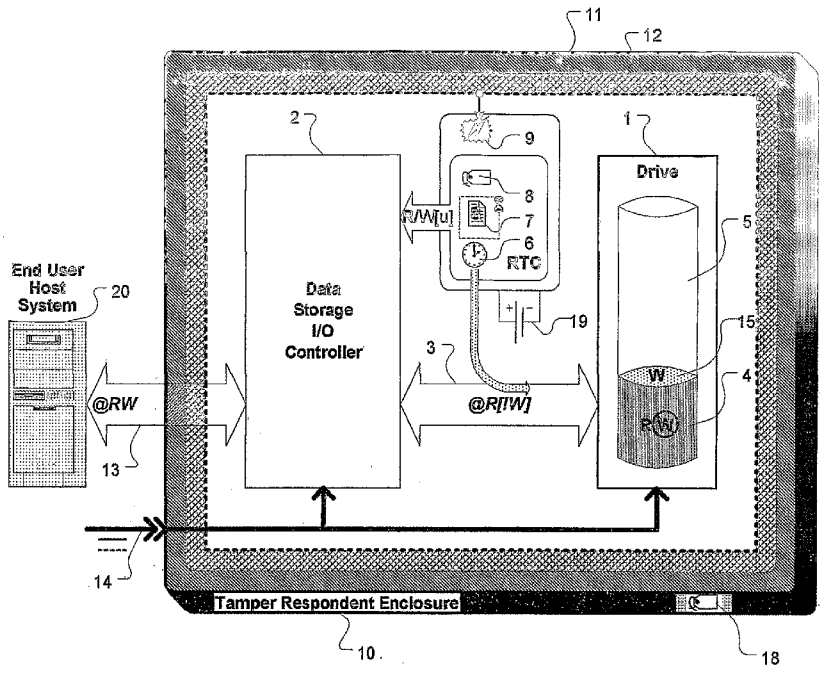
(81) États désignés *(sauf indication contraire, pour tout titre de protection nationale disponible)* : AE, AG, AL, AM, AT, AU, AZ, BA, BB, BG, BR, BW, BY, BZ, CA, CH, CN, CO, CR, CU, CZ, DE, DK, DM, DZ, EC, EE, EG, ES, FI, GB, GD, GE, GH, GM, HR, HU, ID, IL, IN, IS, JP, KE, KG, KP, KR, KZ, LC, LK, LR,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

[Suite sur la page suivante]

(54) Title: SECURE COMPUTER DATA STORAGE METHOD AND DEVICE

(54) Titre : PROCEDE ET DISPOSITIF DE STOCKAGE DE DONNEES INFORMATIQUES SECURISE



(57) Abstract: The invention relates to a secure, tamper- and forgery-proof peripheral for the storage of authenticated, dated computer data with an evidential value. The invention is based on an optionally-rewritable, fully-integrated storage peripheral which is functionally protected by an electronic system which only authorises the addition of data in the unused free space and prohibits the deletion, alteration or overwriting of pre-recorded data. At the end of each file-write operation, the date, which is provided by a non-modifiable internal clock that is calibrated only at the time of production, is associated therewith. Each device comprises a unique integrated secret internal digital identifier which is associated with a unique public identifier and said identifiers are used to personalise the device and render same unreproducible. The aforementioned association can be verified using several third methods which never divulge the secret internal identifier. According to the invention, a physical and electronic peripheral protection system activates, incorporates and protects the assembly of above-mentioned internal elements and destroys the unique internal identifiers in the event of an attempted intrusion, compromise, corruption or internal analysis. For said purpose, the authenticity of the equipment assembly is invalidated and, consequently, so too are the stored data which nonetheless remain readable. The inventive device is particularly suitable for the private storage and archiving of computer data having an authentic, juridical and/or legal weight of evidence in respect of official authorities. Moreover, said device uses no heavy cryptography methods.

[Suite sur la page suivante]

WO 2004/084049 A1

KE, LS, MW, MZ, SD, SL, SZ, TZ, UG, ZM, ZW), eurasien (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, IT, 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).

Déclaration en vertu de la règle 4.17 :

— *relative au droit du déposant de demander et d'obtenir un brevet (règle 4.17.ii)) pour toutes les désignations*

Publiée :

— *avec rapport de recherche internationale*

— *avant l'expiration du délai prévu pour la modification des revendications, sera republiée si des modifications sont reçues*

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 : L'invention concerne un périphérique sécurisé, inviolable et infalsifiable pour le stockage de données informatiques authentifiées et datées à valeur probante. Il est constitué autour d'un périphérique de stockage éventuellement réinscriptible, entièrement intégré, protégé fonctionnellement par une électronique qui autorise uniquement l'ajout de données dans l'espace libre inutilisé et interdit l'effacement, la modification, ou la réécriture des données enregistrées antérieurement. A chaque fin d'écriture de fichier, on associe l'enregistrement de la date fournie par une horloge interne non modifiable calibrée uniquement en fabrication. Chaque dispositif intègre une identification numérique unique secrète interne, associée à une identification unique publique, qui personnalisent le dispositif et le rendent irreproductible. La correspondance est vérifiable par plusieurs méthodes tierces qui ne divulguent jamais l'identification secrète interne. Une protection périmétrique physique et électronique active, englobe et protège l'ensemble des éléments internes précités et assure la destruction des identifiants uniques internes en cas de tentative d'intrusion, de compromission, de corruption, ou d'analyse interne.