04 SEP 2003

20030478800

(12) DEMANDE INTERNATIONALE PUBLIÉE EN VERTU DU TRAITÉ DE COOPÉRATION EN MATIÈRE DE BREVETS (PCT)

(19) Organisation Mondiale de la Propriété Intellectuelle
Bureau international

162162

(43) Date de la publication internationale
19 septembre 2002 (19.09.2002)

PCT

(10) Numéro de publication internationale
WO 02/073876 A3

(51) Classification internationale des brevets[7] : H04L 9/32

(21) Numéro de la demande internationale :
PCT/FR02/00884

(22) Date de dépôt international : 12 mars 2002 (12.03.2002)

(25) Langue de dépôt : français

(26) Langue de publication : français

(30) Données relatives à la priorité :
01/03313 12 mars 2001 (12.03.2001) FR

(71) Déposants *(pour tous les États désignés sauf US)* : **FRANCE TELECOM** [FR/FR]; 6, place d'Alleray, F-75015 Paris (FR). **TELEDIFFUSION DE FRANCE** [FR/FR]; 10, rue d'Oradour-sur-Glane, F-75732 Paris Cedex 15 (FR).

(72) Inventeur; et

(75) Inventeur/Déposant *(pour US seulement)* : **GUILLOU, Louis** [FR/FR]; 16, rue de l'Ise, F-35230 Bourgbarre (FR).

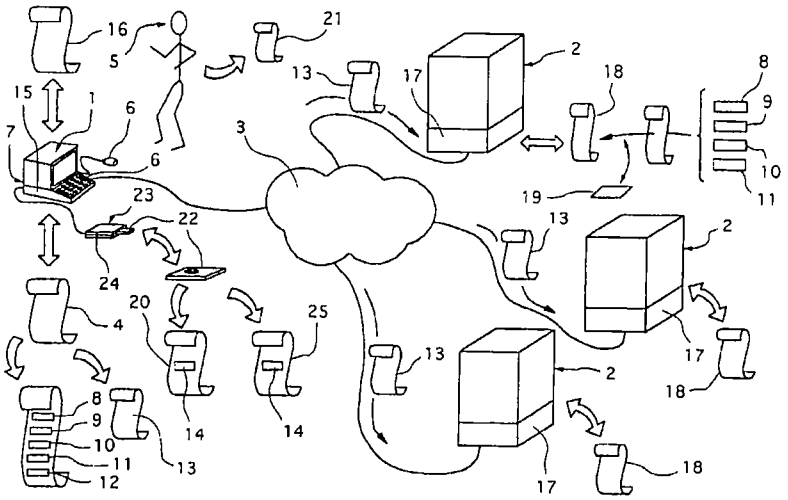
(74) Mandataire : **VIDON, Patrice**; Le Nobel, 2, allée Antoine Becquerel, BP 90333, F-35703 Rennes Cedex 7 (FR).

(81) États désignés *(national)* : AE, AG, AL, AM, AT, AU, AZ, BA, BB, BG, BR, BY, BZ, CA, CH, CN, CO, CR, CU, CZ, DE, DK, DM, DZ, EC, EE, ES, FI, GB, GD, GE, GH, GM, HR, HU, ID, IL, IN, IS, JP, KE, KG, KP, KR, KZ, LC, LK,

[Suite sur la page suivante]

(54) Title: CRYPTOGRAPHIC AUTHENTICATION WITH EPHEMERAL MODULES

(54) Titre : AUTHENTIFICATION CRYPTOGRAPHIQUE PAR MODULES EPHEMERES



(57) **Abstract:** The invention concerns a method enabling a personal computer (1) to be authenticated by a server (2). The method comprises the step, which consists for the user in launching the execution of a log-on procedure software, by introducing personal identifiers (21) providing access to a signature private key (14) for long-term use relative to the duration of the session. The log-on procedure software produces: identification data of the session Id, a public ephemeral module n (9), a public exponent v and at least a pair of ephemeral public numbers G (11) and ephemeral private numbers Q (12) related by a generic equation of the type: $G \equiv Q^v \pmod n$ or $GxQ^v \equiv 1 \pmod n$, an ephemeral certificate (13) linking, by means of said signature private key (14), Id (8) and n (9). The public ephemeral module n (9) is of reduced size relative to the signature private key (14). The method comprises the step which consists for said user (5) to launch the execution of an evidence software, the step which consists for the server (2) in launching the execution of a control software.

(57) **Abrégé :** La présente invention concerne un procédé permettant à un ordinateur personnel (1), d'être authentifié par un serveur (2). Le procédé comprend l'étape, pour un utilisateur (5), de lancer l'exécution d'un logiciel d'ouverture de session, en introduisant des identifiants personnels (21)

[Suite sur la page suivante]

WO 02/073876 A3

ACTION