(19) RÉPUBLIQUE FRANÇAISE

INSTITUT NATIONAL
DE LA PROPRIÉTÉ INDUSTRIELLE

COURBEVOIE

(11) **N° de publication :** **2 904 169**
(à n'utiliser que pour les commandes de reproduction)

(21) **N° d'enregistrement national :** **07 56146**

(51) Int Cl[8] : ***H 04 L 9/28*** *(2007.10), G 06 F 21/00, H 04 L 9/30, H 04 L 9/32*

(12) **BREVET D'INVENTION** **B1**

(54) PROCEDE ET APPLICATION D'ASSOCIATION INTERSYSTEME BASES SUR UNE UNITE DE SECURITE LOGICIELLE.

(22) **Date de dépôt :** 29.06.07.

(30) **Priorité :** 03.07.06 CN 200610100538.5.

(43) **Date de mise à la disposition du public de la demande :** 25.01.08 Bulletin 08/04.

(45) **Date de la mise à disposition du public du brevet d'invention :** 17.06.22 Bulletin 22/24.

(56) **Liste des documents cités dans le rapport de recherche :**

Se reporter à la fin du présent fascicule

(60) **Références à d'autres documents nationaux apparentés :**

◯ **Demande(s) d'extension :**

(71) **Demandeur(s) :** *LENOVO (BEIJING) LIMITED* — CN.

(72) **Inventeur(s) :** LI XIZHE, WANG XU et CHENG SONG.

(73) **Titulaire(s) :** LENOVO (BEIJING) LIMITED.

(74) **Mandataire(s) :** CASALONGA.

FR 2 904 169 - B1

B 07-2407 FR

Au nom de : **LENOVO (BEIJING) LIMITED**

Procédé et application d'association intersystème basés sur une unité de sécurité logicielle

Invention de : **LI Xizhe**
WANG Xu
CHEN Song

Priorité d'une demande de brevet déposée en République Populaire de Chine le 3 juillet 2006 **sous le** n° 200610100538.5

Procédé et application d'association intersystème basés sur une unité de sécurité logicielle

La présente invention concerne la technologie du calcul sécurisé, et plus particulièrement, un procédé et une application d'association intersystème basés sur une unité de sécurité matérielle.

Une unité de sécurité matérielle, telle que le « Trusted Platform Module » (TPM) possède généralement les fonctionnalités pour sécuriser le caractère unique de l'identité d'un utilisateur, l'état complet et le caractère secret de l'espace de travail de l'utilisateur ; la sécurisation de la confidentialité/l'état complet des informations mémorisées, traitées et transmises ; et la sécurisation de l'état complet des réglages de l'environnement matériel, du noyau d'exploitation du système, des programmes utilitaires et applicatifs. En tant que base d'un système sécurisé, l'unité de sécurité matérielle sécurise le système de manière à avoir une immunité telle à bloquer les attaques d'un virus et d'un logiciel de piratage. De plus, en tant que module de clé électronique, l'unité de sécurité matérielle sauvegarde à l'intérieur de la puce les clés utilisées pour le chiffrement, ou chiffre et mémorise les clés dans un espace externe, au lieu de sauvegarder les clés sur un disque dur ou un autre support, sous forme de texte en clair comme habituellement, et fournit un service de cryptographie fiable à la plate-forme du système et aux programmes d'application par l'intermédiaire d'un intergiciel de l'unité de sécurité matérielle. Dans cette procédure, la gestion des clés, l'encapsulation/désencapsulation de sécurisation des données et le calcul de signature numérique ont une très haute sécurité.

Un dispositif équipé d'une unité de sécurité matérielle peut être appelé système de calcul sécurisé. Dans les spécifications et les techniques antérieures, les fonctionnalités de l'unité de sécurité matérielle ne sont efficaces que dans le dispositif où elle est située, il n'existe aucune approche pour établir une relation sécurisée entre différents dispositifs comportant des unités de sécurité matérielles, en se basant sur l'unité de sécurité matérielle. Il existe en conséquence un besoin pour étendre les fonctions de calcul sécurisées à d'autres systèmes de calcul sécurisés.

Par exemple, un utilisateur possède deux dispositifs électroniques, un ordinateur personnel (PC) et un téléphone portable, tous deux comportant des unités de sécurité matérielles montées sur ceux-ci. L'utilisateur mémorise certains fichiers secrets sur le PC, et utilise une clé de l'unité de sécurité matérielle sur le PC pour le chiffrement et la mémorisation. Si l'utilisateur souhaite transmettre ces fichiers au téléphone portable pour un autre traitement, alors il est nécessaire d'exécuter une

procédure dans laquelle les fichiers sont d'abord déchiffrés en entrant une clé de déchiffrement sur le PC. Après cela, les fichiers déchiffrés sont transmis au téléphone portable. Enfin, le téléphone portable utilise son unité de sécurité matérielle pour chiffrer les fichiers reçus pour mémorisation. Dans la procédure ci-dessus, il n'existe aucun mécanisme pour prendre en compte un problème tel que le système de calcul sécurisé d'homologue est ou non de confiance ; d'autre part, puisque la transmission est effectuée sous forme de texte en clair, il y existe un risque potentiel pour la sécurité ; et on demande à l'utilisateur d'entrer les clés et mot de passe durant le chiffrement et le déchiffrement, et ainsi, la procédure est pénible.

Il existe un grand nombre d'autres besoins pour des extensions de calcul sécurisées, par exemple, un ordinateur portable avec un PC, un téléphone portable avec un PC, un téléphone portable avec un ordinateur portable, un PC avec un PC, des associations de dispositifs sans fil, et ainsi de suite. Toutefois, dans les techniques antérieures, il n'existe aucune approche pour accorder les confiances entre systèmes, basée sur une unité de sécurité matérielle.

Un objectif de la présente invention est de fournir un procédé d'association de systèmes de calcul inter-sécurisés, basé sur une unité de sécurité matérielle, capable de fournir une approche pour octroyer des confiances entre des systèmes de calcul sécurisés, basée sur l'unité de sécurité matérielle.

Selon un aspect de la présente invention, il est fourni un procédé d'association de systèmes de calcul inter-sécurisés, basé sur une unité de sécurité matérielle, comprenant :

Étape 11, la configuration des conditions nécessaires d'association pour des unités de sécurité matérielles de systèmes de calcul sécurisés ;

Étape 12, l'échange d'informations d'unités de sécurité matérielles entre les unités de sécurité matérielles des systèmes de calcul sécurisés à associer, et le contrôle des validités des dispositifs de l'unité de sécurité matérielle d'homologue ; et si le contrôle de validation réussit, il se poursuit par les étapes suivantes ; sinon, la sortie de la procédure d'association ;

Étape 13, la vérification respective du fait que l'association satisfait leurs conditions nécessaires d'association respectives par les unités de sécurité matérielles des systèmes de calcul sécurisés à associer ; et si la vérification réussit, il se poursuit par les étapes suivantes ; sinon, la sortie de la procédure d'association ; et

Étape 14, la mémorisation respective des informations de la plate-forme d'homologue et des informations d'association des unités de sécurité matérielles par les unités de sécurité matérielles des systèmes de calcul sécurisés.

De préférence, avant l'étape 12 d'échange mutuel des informations des unités de sécurité matérielles, le procédé comprend en outre, une étape consistant à :

générer respectivement une paire de clés asymétriques en tant que clé publique, et échanger la clé publique générée par les unités de sécurité matérielles des systèmes de calcul sécurisés à associer de façon à établir un tube chiffré entre les systèmes de calcul sécurisés à associer.

De préférence, entre les étapes 13 et 14, le procédé comprend en outre, une étape consistant à :

respectivement générer une clé et remplacer la clé par les unités de sécurité matérielles des systèmes de calcul sécurisés à associer de façon à établir un tube chiffré entre les systèmes de calcul sécurisés à associer.

Dans un mode de réalisation, la clé générée à l'étape 13b est une clé asymétrique, et la clé échangée est une clé publique ; ou la clé générée et échangée à l'étape 13b est une clé symétrique.

Dans un mode de réalisation, entre les étapes 13 et 14, le procédé comprend en outre, une étape consistant à :

Étape 13b, respectivement générer une clé et remplacer la clé par les unités de sécurité matérielles des systèmes de calcul sécurisés à associer de façon à établir un tube chiffré entre les systèmes de calcul sécurisés à associer.

Dans un mode de réalisation, la clé générée à l'étape 13b est une clé asymétrique, et la clé échangée est une clé publique ; ou la clé générée et échangée à l'étape 13b est une clé symétrique.

Dans un mode de réalisation, lesdites conditions nécessaires d'association comportent le fait que l'association est autorisée ou non, et/ou le type d'unité de sécurité matérielle qu'il est permis d'associer, et/ou les numéros de série des unités de sécurité matérielles qu'il est permis d'associer, et/ou les identifiants des dispositifs où sont situées les unités de sécurité matérielles qu'il est permis d'associer, et et/ou les modes d'association autorisés, et/ou le fait qu'il puisse initialiser activement une association ou non, et/ou le fait qu'il puisse accepter une demande d'association ou non, et/ou des algorithmes de cryptographie pouvant être sélectionnés pour une association, et/ou des ressources et services matériels et logiciels configurables.

Dans un mode de réalisation, lesdites conditions nécessaires d'association comportent en outre, un nombre maximum de liaisons d'association respectivement pour déterminer le nombre maximum de liaisons d'association satisfaisant les conditions nécessaires d'association respectives.

Dans un mode de réalisation, lesdites conditions nécessaires d'association comportent en outre, un niveau de sécurité pour indiquer une plage dans laquelle l'unité de sécurité matérielle peut utiliser les fonctions, droits et services de l'unité de sécurité matérielle associée d'homologue.

Dans un mode de réalisation, lesdites conditions nécessaires d'association comportent en outre, la détermination de la vérification d'association.

Dans un mode de réalisation, lesdites conditions nécessaires d'association comportent en outre, la durée de l'association, et/ou le temps maximum disponible pour l'association, et/ou les clés ou variables ou bits de nombres indiqués ou informations de plate-forme selon lesquelles l'association peut exister.

Dans un mode de réalisation, lesdites conditions nécessaires d'association comportent en outre, la détermination du fait que les informations d'association mémorisées par l'unité de sécurité matérielle sont autorisées ou non à être distribuées à d'autres unités de sécurité matérielles ou à d'autres systèmes.

Dans un mode de réalisation, lesdites conditions nécessaires d'association comportent en outre, le fait que l'association est autorisée ou non, et/ou le type d'unité de sécurité matérielle qu'il est autorisé d'associer, et/ou les numéros de série des unités de sécurité matérielles qu'il est permis d'associer, et/ou les identifiants des dispositifs où sont situées les unités de sécurité matérielles qu'il est permis d'associer, et/ou les modes d'association autorisés, et/ou le fait qu'il puisse ou non initialiser activement une association, et/ou le fait qu'il puisse ou non accepter une demande d'association, et/ou les algorithmes de cryptographie pouvant être sélectionnés pour une association, et/ou les ressources et services logiciels et matériels configurables.

Dans un mode de réalisation, lesdites conditions nécessaires d'association comportent en outre, un nombre maximum de liaisons d'association respectivement pour déterminer le nombre maximum de liaisons d'association satisfaisant les conditions nécessaires d'association respectives.

Dans un mode de réalisation, lesdites conditions nécessaires d'association comportent en outre, un niveau de sécurité pour indiquer une plage dans laquelle l'unité de sécurité matérielle peut utiliser les fonctions, droits et services de l'unité de sécurité matérielle associée d'homologue.

Dans un mode de réalisation, lesdites conditions nécessaires d'association comportent en outre, la détermination de la vérification d'association.

Dans un mode de réalisation, lesdites conditions nécessaires d'association comportent en outre, la durée de l'association, et/ou le temps maximum disponible

pour l'association, et/ou les clés ou variables ou bits de nombres indiqués ou informations de plate-forme selon lesquelles l'association peut exister.

Dans un mode de réalisation, lesdites conditions nécessaires d'association comportent en outre, la détermination du fait que les informations d'association mémorisées par l'unité de sécurité matérielle sont autorisées ou non à être distribuées à d'autres unités de sécurité matérielles ou à d'autres systèmes.

Selon la description ci-dessus, la présente invention fournit le procédé d'association de systèmes de calcul inter-sécurisés basé sur une unité de sécurité matérielle, dans lequel, après les contrôles de validation du dispositif et que les vérifications des conditions nécessaires d'association des unités de sécurité matérielles entre les systèmes de calcul sécurisés sont satisfaites, les informations des unités de sécurité matérielles et les informations de plate-forme des homologues sont respectivement mémorisées, de telle sorte à établir une relation sécurisée entre les systèmes de calcul sécurisés. L'échange des clés et l'établissement du tube chiffré évitent le risque de sécurité potentielle dû aux transmissions de texte en clair, de telle sorte à encore améliorer la sécurité des transmissions d'informations entre les systèmes de calcul sécurisés.

Les objectifs, avantages et caractéristiques ci-dessus de la présente invention apparaîtront d'après la description détaillée qui suit des modes de réalisation préférés, effectuée conjointement avec les dessins, dans lesquels :

la figure 1 est un organigramme d'un procédé d'association de systèmes de calcul inter-sécurisés, basé sur une unité de sécurité matérielle selon un mode de réalisation de la présente invention ;

la figure 2 représente les gestions de l'unité de sécurité matérielle vers les associations de systèmes de calcul inter-sécurisés selon le mode de réalisation de la présente invention ; et

la figure 3 représente les fonctionnalités étendues obtenues par l'unité de sécurités matérielles associée selon le mode de réalisation de la présente invention.

Les modes de réalisation de la présente invention vont être décrits en détail ci-après en référence aux figures, et les détails et les fonctions inutiles pour l'invention sont omis dans la description pour ne pas compliquer la compréhension de l'invention.

Le procédé d'association de systèmes de calcul inter-sécurisés basé sur l'unité de sécurité matérielle selon le mode de réalisation de la présente invention va être décrit en détail conjointement avec les dessins. Dans le procédé, les propriétaires des unités de sécurité matérielles configurent d'abord les conditions nécessaires

d'association ; puis, le contrôle de validation de dispositifs pour l'unité de sécurité matérielle et la vérification du fait que les conditions nécessaires d'association sont satisfaites sont effectués entre les systèmes de calcul sécurisés à associer. Si le contrôle de validation et la vérification des conditions nécessaires d'association pour les deux homologues réussissent tous, les systèmes de calcul sécurisés mémorisent alors respectivement les informations de liaison des homologues et les informations de plate-forme dans leurs propres unités de sécurité matérielles. Les systèmes de calcul sécurisés ont établi les relations d'association en considérant que les homologues sont sécurisés. En se basant sur ces sécurisations, les gestions et les services de sécurité correspondants peuvent être fournis.

Comme représenté sur la figure 1, le procédé d'association de systèmes de calcul inter-sécurisés basé sur l'unité de sécurité matérielle selon le mode de réalisation de la présente invention comprend les étapes suivantes.

Étape 11, les propriétaires des unités de sécurité matérielles des systèmes de calcul sécurisés configurent les conditions nécessaires d'association.

Les propriétaires des unités de sécurité matérielles peuvent configurer et gérer les conditions nécessaires d'association pouvant inclure le fait que l'association est autorisée ou non, le type d'unité de sécurité matérielle qu'il est permis d'associer, et d'autres conditions devant être satisfaites par l'association. Comme autres conditions devant être satisfaites par les associations, il peut y avoir les numéros de série des unités de sécurité matérielles qu'il est permis d'associer, ou les identifiants des dispositifs où sont situés les unités de sécurité matérielles qu'il est permis d'associer. Les conditions nécessaires d'association peuvent inclure en outre, les modes d'association autorisés, le fait de pouvoir ou non initialiser activement une association, le fait qu'elle puisse accepter une demande d'association ou non, des algorithmes de cryptographie pouvant être sélectionnés pour une association, les ressources et services logiciels et matériels configurables, et analogue.

Étape 12, les informations d'unités de sécurité matérielles sont échangées entre les unités de sécurité matérielles des systèmes de calcul sécurisés à associer, et les validités des dispositifs de l'unité de sécurité matérielle d'homologue sont contrôlées.

Les systèmes de calcul sécurisés à associer sont reliés par l'intermédiaire d'interfaces de communication telles que des ports série, une « General-Purpose Input Output Interface » (GPIO), un « Universal Serial Bus » (USB), infrarouge et sans fil et analogue. Les informations de l'unité de sécurités matérielles échangées comportent un numéro d'identification (ID), un descripteur du fabricant et une

signature de l'unité de sécurité matérielle. L'unité de sécurité matérielle vérifie la validation du dispositif de l'unité de sécurité matérielle d'homologue au moyen d'algorithmes de contrôle d'état complet. Si le contrôle réussit, il passe alors à l'étape suivante ; et sinon, la procédure d'association se termine.

Étape 13, les unités de sécurité matérielles des systèmes de calcul sécurisés à associer vérifient si l'association satisfait leurs conditions nécessaires d'association.

Les unités de sécurité matérielles des systèmes de calcul sécurisés à associer échangent des informations d'utilisateur, des informations d'unité de sécurité matérielle et des informations de plate-forme. Les informations d'utilisateur comportent la signature, le mot de passe de l'utilisateur ou du propriétaire, et analogue. Les informations d'unité de sécurité matérielle comportent le type d'interface, le descripteur du fabricant et l'algorithme de cryptographie d'association de l'unité de sécurité matérielle. Les informations de plate-forme peuvent comporter des informations matérielles et des informations logicielles des systèmes de calcul sécurisés. Comme exemple, pour un ordinateur monté avec une unité de sécurité matérielle, ses informations matérielles comportent des informations de « Basic Input Output System » (BIOS), des informations de CPU, des informations de carte, des informations de disque dur et analogue. En outre, ses informations logicielles comportent des informations de secteur d'amorçage, des informations de système d'exploitation et analogue. D'autre part, pour un téléphone portable monté avec une unité de sécurité matérielle, ses informations matérielles concernent généralement les informations de mémoire à lecture seule (ROM), de CPU, de « Subscriber Identity Module » (SIM) et d'autres dispositifs associés montés dans les systèmes de calcul sécurisés. L'unité de sécurité matérielle vérifie si l'association satisfait les conditions nécessaires de ses propres conditions nécessaires d'association, en fonction des informations échangées ci-dessus. Si les conditions nécessaires ne sont pas satisfaites, alors la procédure d'association se termine ; et si les conditions nécessaires d'association sont satisfaites, elle passe à l'étape suivante.

Étape 14, l'association de systèmes de calcul inter-sécurisés basée sur l'unité de sécurité matérielle est confirmée, les informations de plate-forme et les informations d'association d'unité de sécurité matérielle de l'homologue d'association sont mémorisées, et les droits et leurs plages d'application sont déterminés entre les unités de sécurité matérielles associées.

Pour améliorer la sécurité des transmissions de données durant la procédure d'association et empêcher l'interception des données transmises durant la procédure d'association, dans les systèmes de calcul sécurisés mutuellement associés, chacune

des unités de sécurité matérielles génère d'abord une paire de clés asymétriques en tant que clé publique et échange la clé publique générée de manière à créer un tube chiffré entre les systèmes de calcul sécurisés à associer, et les échanges de données qui suivent sont tous effectués au travers du tube chiffré. Après échange des clés publiques, les systèmes de calcul sécurisés chiffrent les données par les unités de sécurité matérielles respectives en utilisant les clés publiques échangées ci-dessus avant la transmission des données. Les données chiffrées par la clé publique ne peuvent être déchiffrées que par la clé privée correspondant à la clé publique, de façon à éviter à des tiers d'obtenir des données échangées durant la procédure d'association, et ainsi, la sécurité de la procédure d'association est améliorée.

Dans les conditions nécessaires d'association, on peut déterminer en outre, si les unités de sécurités matérielles associées sont dans une relation d'égal à égal ou ne sont pas dans une relation d'égal à égal. La relation d'égal à égal définit une relation coopérative d'égal à égal entre les unités de sécurité matérielles, dans laquelle l'une des unités de sécurité matérielles n'a pas de droit de contrôle et de droit de configuration sur l'autre des unités de sécurité matérielles. Les unités de sécurités matérielles associées d'égal à égal peuvent effectuer des migrations de clés et de services. La relation qui n'est pas d'égal à égal définit une relation maître-esclave entre les unités de sécurité matérielles, et désigne l'une des unités de sécurité matérielles comme maître et l'autre des unités de sécurité matérielles comme esclave. L'unité de sécurité matérielle maître peut configurer les fonctions, services, caractéristiques, ressources matérielles et logicielles disponibles, de l'unité de sécurité matérielle esclave, ou obliger l'exécution d'opérations telles que l'effacement, la copie et l'arrêt. Les unités de sécurités matérielles qui ne sont pas d'égal à égal peuvent également effectuer des migrations de clés et de services.

Dans une condition nécessaire d'association, on peut prévoir un nombre maximum de liaisons d'association pour indiquer le nombre de liaisons d'association satisfaisant la condition nécessaire d'association et qui sont acceptables par l'unité de sécurité matérielle. Si par exemple, le nombre maximum de liaisons d'association est fixé à 1, alors l'unité de sécurité matérielle peut établir une liaison d'association avec une seule autre unité de sécurité matérielle satisfaisant la condition nécessaire d'association. Si le nombre maximum de liaisons d'association est plus grand que 1, alors l'unité de sécurité matérielle peut établir des liaisons d'association avec une pluralité d'autres unités de sécurité matérielles satisfaisant la condition nécessaire d'association.

De plus, dans une condition nécessaire d'association, on peut déterminer la vérification sur une association. On peut vérifier la relation d'association entre les systèmes informatiques sécurisés durant la période au cours de laquelle la relation existe. Le contenu à vérifier comporte les informations de vérification de dispositifs, les informations de conditions nécessaires d'association, le temps de vérification et analogue. S'il n'est pas vérifié avant l'expiration de la temporisation de la vérification, alors l'opération d'association est terminée. Les unités de sécurités matérielles d'association peuvent négocier et déterminer l'intervalle de temps de vérification, les temps de vérification et la durée totale de vérification.

Dans une condition nécessaire d'association, on peut déterminer le niveau de sécurité d'une association. Pour différentes associations établies selon les conditions nécessaires d'association de niveaux de sécurité différents, les plages dans lesquelles l'unité de sécurité matérielle peut utiliser les fonctions, les droits et les services de l'unité de sécurité matérielle d'homologue sont également différentes.

Dans une condition nécessaire d'association, on peut déterminer qu'il n'est pas permis de distribuer à d'autres unités de sécurité matérielles les signatures, certificats, informations d'association et informations de plate-forme, mémorisées par la présente unité de sécurité matérielle. Cependant, on peut également déterminer dans une condition nécessaire d'association qu'il est permis de distribuer certaines informations appropriées à l'association mémorisée par la présente unité de sécurité matérielle, à d'autres unités de sécurité matérielles ayant des relations d'association avec la présente unité de sécurité matérielle. Si par exemple, le propriétaire espère que ces relations d'association basées sur une condition nécessaire d'association ont une transitivité, c'est-à-dire selon une seule et même condition nécessaire d'association, si une unité de sécurité matérielle A est associée à une unité de sécurité matérielle B, et que l'unité de sécurité matérielle B est également associée à une unité de sécurité matérielle C, alors la relation d'association basée sur la seule et même condition nécessaire d'association entre l'unité de sécurité matérielle A et l'unité de sécurité matérielle C est également vérifiée, ainsi, lorsque les unités de sécurité matérielles A et C établissent l'association, l'unité de sécurité matérielle C peut fournir des informations de signature, certificat ou association de l'unité de sécurité matérielle B à l'unité de sécurité matérielle A pour vérification. Si la vérification réussit, alors les systèmes de calcul sécurisés où sont respectivement situées les unités de sécurité matérielles A et C peuvent être associés, de façon à simplifier la procédure de vérification entre l'unité de sécurité matérielle A et l'unité de sécurité matérielle C.

Il existe un grand nombre de façons pour terminer les relations d'association entre les systèmes de calcul sécurisés. Premièrement, le propriétaire de l'unité de sécurité matérielle est autorisé à mettre à jour ou à effacer les conditions nécessaires d'association. Lorsque les conditions nécessaires d'association d'une unité de sécurité matérielle sont modifiées, les relations d'association précédemment établies sont contrôlées conformément aux nouvelles conditions nécessaires d'association, et celles qui ne satisfont pas aux nouvelles conditions nécessaires d'association sont gelées ou effacées. Deuxièmement, certaines contraintes devant être satisfaites par les associations peuvent être configurées dans les conditions nécessaires d'association, telles que la durée d'association, les temps disponibles pour l'association et d'autres conditions devant être satisfaites par l'existence de l'association, par exemple, des clés, des variables, des bits de nombres indiqués, des informations de plate-forme ou des informations externes. Dans une seule et même condition nécessaire d'association, on peut configurer une ou plusieurs contraintes ci-dessus. Seulement lorsque toutes les contraintes configurées sont satisfaites, la liaison correspondante peut exister. Sinon, la liaison entre les systèmes de calcul sécurisés est terminée.

Comme représenté sur la figure 2, les gestions de l'unité de sécurité matérielle vers les associations du système de calcul inter-sécurisé comportent un contrôle de liaison, une mise à jour de liaison, une mise à jour de tube chiffré et un effacement de liaison.

Le contrôle d'association signifie qu'un tiers d'association demande à l'autre tiers d'envoyer des informations de l'unité de sécurité matérielle et des informations d'association, à jour, et les compare à ses informations d'unité de sécurité matérielle et information d'association de l'autre tiers, mémorisées. S'il existe certaines différences, l'association se termine et les informations résiduelles sont effacées.

La mise à jour d'association signifie qu'une partie du contenu des conditions nécessaires d'association peut être modifiée entre les unités de sécurité matérielles associées. Par exemple, dans la relation qui n'est pas d'égal à égal, l'unité de sécurité matérielle maître peut modifier les conditions nécessaires d'association de l'unité de sécurité matérielle esclave.

La mise à jour de tube chiffré signifie que les unités de sécurités matérielles associées peuvent nouvellement générer de nouvelles clés et les échanger entre elles, et toutes les données à transmettre après cela sont chiffrées avec les nouvelles clés, de façon à générer un nouveau tube chiffré. À ce moment, les clés générées peuvent être des clés symétriques ou des clés asymétriques. L'algorithme pour générer les clés peut également être reconçu dans les conditions nécessaires d'association.

L'effacement de liaison signifie que le propriétaire de l'unité de sécurité matérielle peut effacer les informations concernant les enregistrements de liaisons, de façon à effacer la liaison entre les systèmes de calcul sécurisés.

Comme représenté sur la figure 3, les fonctionnalités étendues obtenues par l'unité de sécurité matérielle associée comportent la vérification de l'état complet de plate-forme, la gestion de configuration, la gestion de journal, la gestion de mémorisation des clés, et la migration et la gestion des services de cryptographie tels que les clés et certificats. Le procédé d'association de systèmes informatiques inter-sécurisés basé sur l'unité de sécurité matérielle proposée dans la présente invention constitue la base des confiances entre les systèmes de calcul sécurisés associés, de telle sorte que la sécurité pour réaliser les fonctionnalités étendues de ces unités de sécurité matérielles est améliorée.

Le moyen de vérification de l'état complet de plate-forme signifie que l'unité de sécurité matérielle vérifie l'état complet du système où est située l'unité de sécurité matérielle d'homologue. Dans la procédure d'association susmentionnée, les unités de sécurité matérielles enregistrent respectivement des informations de mesure d'état complet de plate-forme ou leur résumé, mémorisées dans le « Platform Control Register » (PCR) des unités de sécurité matérielles d'homologue. Lorsqu'il est requis d'effectuer la vérification d'état complet de plate-forme, l'une des unités de sécurité matérielles envoie une demande à l'autre des unités de sécurité matérielles. L'autre des unités de sécurité matérielles effectue une mesure d'état complet de plate-forme après vérification de la fiabilité de la relation d'association, et renvoie le résultat correspondant ou le résumé au demandeur des unités de sécurité matérielles. Le demandeur des unités de sécurité matérielles compare les nouvelles informations de plate-forme reçues à ses informations mémorisées ; et s'il existe certaines différences, la plate-forme de l'homologue est considérée comme anormale, et des processus appropriés sont exécutés.

Le moyen de gestion de journal signifie que l'une des unités de sécurités matérielles associées sauvegarde ou effectue l'acquisition de journaux appropriés de l'autre et exécute des traitements appropriés. Par exemple, pour un journal d'opérations concernant l'association, les associations peuvent être gérées en analysant le journal des opérations concernant l'association.

Le moyen de gestion de mémorisation de clés signifie qu'avant de mémoriser une clé, une unité de sécurité matérielle associée A transmet d'abord la clé à l'autre unité de sécurité matérielle associée B pour le chiffrement, puis mémorise la clé renvoyée chiffrée par l'unité de sécurité matérielle B. Lorsque l'unité de sécurité

matérielle A a besoin d'utiliser la clé, l'unité de sécurité matérielle B effectue d'abord le déchiffrement de la clé, puis la clé renvoyée déchiffrée par l'unité de sécurité matérielle B est utilisée pour le déchiffrement. Ainsi, puisque cette clé est chiffrée par les deux tiers, en l'utilisant, elle doit être déchiffrée par les deux tiers, de telle sorte que la sécurité est améliorée.

La gestion de configuration signifie que lorsqu'une association de systèmes de calcul inter-sécurisés basée sur une unité de sécurité matérielle est la relation qui n'est pas d'égal à égal, le propriétaire de l'unité de sécurité matérielle maître peut configurer les fonctions, services, caractéristiques et les ressources logicielles et matérielles de l'unité de sécurité matérielle esclave comme un superutilisateur ou administrateur de l'unité de sécurité matérielle esclave, et peut commander des opérations telles que l'effacement, la copie et l'arrêt de l'unité de sécurité matérielle esclave.

La migration et la gestion des services de cryptographie tels que les clés et certificats se réfèrent au fait que les services de cryptographie tels que les clés et certificats peuvent migrer entre les unités de sécurité matérielles ayant établi la relation d'association. L'unité de sécurité matérielle enregistre les migrations des clés et certificats, incluant les chemins de migration, l'emplacement de migration, le propriétaire, le créateur, le cycle de vie, les temps d'utilisation, les droits et ainsi de suite, et gère les migrations des clés et certificats de façon à obtenir les services de migration et de gestion de cryptographie. Il peut également déterminer si les clés et certificats ayant migré sont ou non autorisés à être également distribués à d'autres unités de sécurité matérielles.

En résumé, la présente invention fournit un procédé d'association intersystème basé sur une unité de sécurité matérielle, pour fournir un mécanisme de traitement basé sur une unité de sécurité matérielle pour établir des confiances entre des systèmes de calcul sécurisés. Dans la procédure d'association, l'utilisation des clés, le contrôle de validation de dispositif de l'unité de sécurité matérielle et la vérification des conditions nécessaires de liaison améliorent encore la sécurité et la fiabilité de la totalité du procédé d'association. Par la détermination des conditions nécessaires de liaison, les relations de liaison satisfaisant différentes conditions nécessaires peuvent être établies entre les systèmes de calcul sécurisés et la gestion des relations d'association peut être réalisée. Selon le procédé d'association de la présente invention, les relations pouvant être sécurisées sont établies entre les systèmes de calcul sécurisés de façon à constituer la base et l'assurance des fonctions multiples étendues de l'unité de sécurité matérielle.

REVENDICATIONS

1. Procédé d'association de systèmes de calcul inter-sécurisés, basé sur une unité de sécurité matérielle, comprenant :

Étape 11, la configuration des conditions nécessaires d'association pour des unités de sécurité matérielles de systèmes de calcul sécurisés ;

Étape 12, l'échange d'informations d'unités de sécurité matérielles entre les unités de sécurité matérielles des systèmes de calcul sécurisés à associer, et le contrôle des validités des dispositifs de l'unité de sécurité matérielle d'homologue ; et si le contrôle de validation réussit, il se poursuit par les étapes suivantes ; sinon, la sortie de la procédure d'association ;

Étape 13, la vérification respective du fait que l'opération d'association satisfait leurs conditions nécessaires d'association respectives par les unités de sécurité matérielles des systèmes de calcul sécurisés à associer ; et si la vérification réussit, l'opération d'association se poursuit par les étapes suivantes ; sinon, la sortie de la procédure d'association ;

Étape 14, la mémorisation respective des informations de la plate-forme d'homologue et des informations d'association des unités de sécurité matérielles par les unités de sécurité matérielles des systèmes de calcul sécurisés ; et

lesdites conditions nécessaires d'association comportant en outre un niveau de sécurité pour indiquer une plage dans laquelle l'unité de sécurité matérielle peut utiliser les fonctions, droits et services de l'unité de sécurité matérielle associée d'homologue.

2. Procédé selon la revendication 1, dans lequel avant l'étape 12 d'échange mutuel des informations des unités de sécurité matérielles, le procédé comprend en outre, une étape consistant à :

Étape 12a, générer respectivement une paire de clés asymétriques en tant que clé publique, et échanger la clé publique générée par les unités de sécurité matérielles des systèmes de calcul sécurisés à associer de façon à établir un tube chiffré entre les systèmes de calcul sécurisés à associer.

3. Procédé selon la revendication 1 ou 2, dans lequel entre les étapes 13 et 14, le procédé comprend en outre, une étape consistant à :

Étape 13b, respectivement générer une clé et remplacer la clé par les unités de sécurité matérielles des systèmes de calcul sécurisés à associer de façon à établir un tube chiffré entre les systèmes de calcul sécurisés à associer.

4. Procédé selon la revendication 3, dans lequel la clé générée à l'étape 13b est une clé asymétrique, et la clé échangée est une clé publique ; ou la clé générée et échangée à l'étape 13b est une clé symétrique.

5. Procédé selon la revendication 3, dans lequel la clé générée à l'étape 13b est une clé asymétrique, et la clé échangée est une clé publique ; ou la clé générée et échangée à l'étape 13b est une clé symétrique.

6. Procédé selon la revendication 1 ou 2, dans lequel lesdites conditions nécessaires d'association comportent le fait que l'association est autorisée ou non, et/ou le type d'unité de sécurité matérielle qu'il est permis d'associer, et/ou les numéros de série des unités de sécurité matérielles qu'il est permis d'associer, et/ou les identifiants des dispositifs où sont situées les unités de sécurité matérielles qu'il est permis d'associer, et et/ou les modes d'association autorisés, et/ou le fait qu'il puisse initialiser activement une association ou non, et/ou le fait qu'il puisse accepter une demande d'association ou non, et/ou des algorithmes de cryptographie pouvant être sélectionnés pour une association, et/ou des ressources et services matériels et logiciels configurables.

7. Procédé selon la revendication 6, dans lequel lesdites conditions nécessaires d'association comportent en outre, un nombre maximum de liaisons d'association respectivement pour déterminer le nombre maximum de liaisons d'association satisfaisant les conditions nécessaires d'association respectives.

8. Procédé selon la revendication 6, dans lequel lesdites conditions nécessaires d'association comportent en outre, la détermination de la vérification d'association.

9. Procédé selon la revendication 6, dans lequel lesdites conditions nécessaires d'association comportent en outre, la durée de l'association, et/ou le temps maximum disponible pour l'association, et/ou les clés ou variables ou bits de nombres indiqués ou informations de plate-forme selon lesquelles l'association peut exister.

10. Procédé selon la revendication 6, dans lequel lesdites conditions nécessaires d'association comportent en outre, la détermination du fait que les informations d'association mémorisées par l'unité de sécurité matérielle sont

autorisées ou non à être distribuées à d'autres unités de sécurité matérielles ou à d'autres systèmes.

11. Procédé de vérification de l'état complet de plate-forme entre des unités de sécurité matérielle associées, comprenant les étapes suivantes :

l'une des unités de sécurité matérielles envoie une demande à l'autre des unités de sécurité matérielles ;

l'autre des unités de sécurité matérielles effectue une mesure d'état complet de plate-forme après vérification de la fiabilité de la relation d'association, et renvoie le résultat correspondant ou le résumé au demandeur des unités de sécurité matérielles ;

le demandeur des unités de sécurité matérielles compare les nouvelles informations de plate-forme reçues à ses informations mémorisées ;

s'il existe certaines différences, la plate-forme de l'homologue est considérée comme anormale, et des processus appropriés sont exécutés.

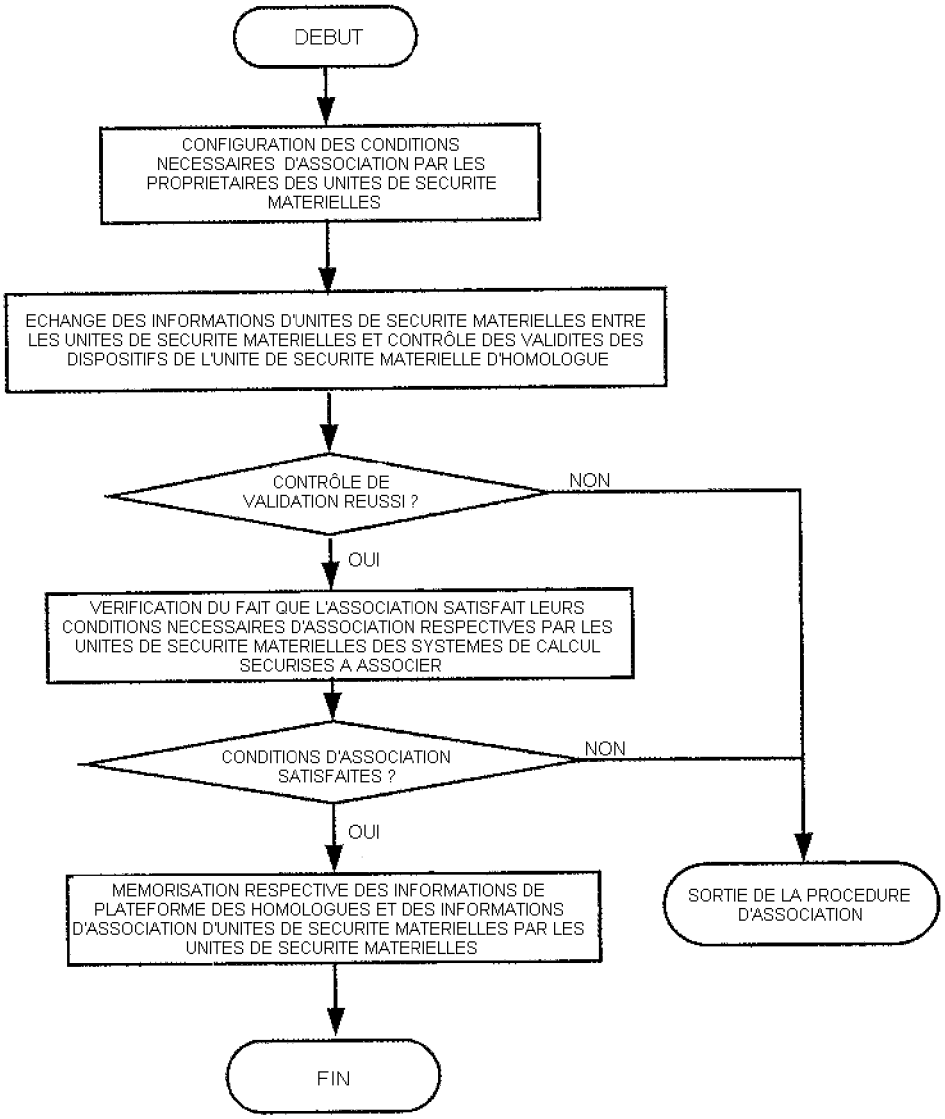
DEBUT
CONFIGURATION DES CONDITIONS NECESSAIRES D'ASSOCIATION PAR LES PROPRIETAIRES DES UNITES DE SECURITE MATERIELLES
ECHANGE DES INFORMATIONS D'UNITES DE SECURITE MATERIELLES ENTRE LES UNITES DE SECURITE MATERIELLES ET CONTRÔLE DES VALIDITES DES DISPOSITIFS DE L'UNITE DE SECURITE MATERIELLE D'HOMOLOGUE
CONTRÔLE DE VALIDATION REUSSI ?
NON
OUI
VERIFICATION DU FAIT QUE L'ASSOCIATION SATISFAIT LEURS CONDITIONS NECESSAIRES D'ASSOCIATION RESPECTIVES PAR LES UNITES DE SECURITE MATERIELLES DES SYSTEMES DE CALCUL SECURISES A ASSOCIER
CONDITIONS D'ASSOCIATION SATISFAITES ?
NON
OUI
MEMORISATION RESPECTIVE DES INFORMATIONS DE PLATEFORME DES HOMOLOGUES ET DES INFORMATIONS D'ASSOCIATION D'UNITES DE SECURITE MATERIELLES PAR LES UNITES DE SECURITE MATERIELLES
SORTIE DE LA PROCEDURE D'ASSOCIATION
FIN

Fig. 1

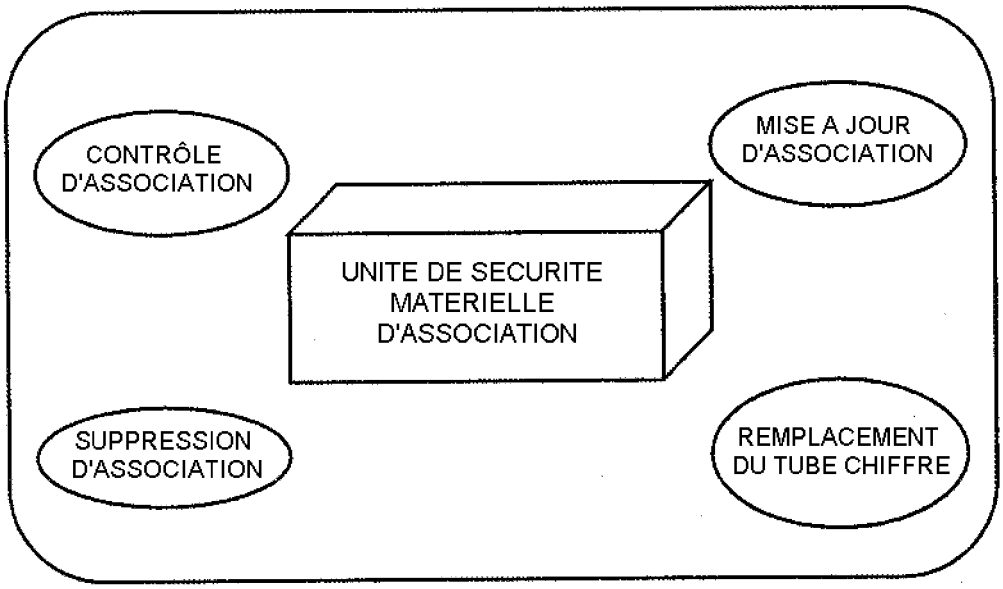
CONTRÔLE D'ASSOCIATION
MISE A JOUR D'ASSOCIATION
UNITE DE SECURITE MATERIELLE D'ASSOCIATION
SUPPRESSION D'ASSOCIATION
REMPLACEMENT DU TUBE CHIFFRE

Fig. 2

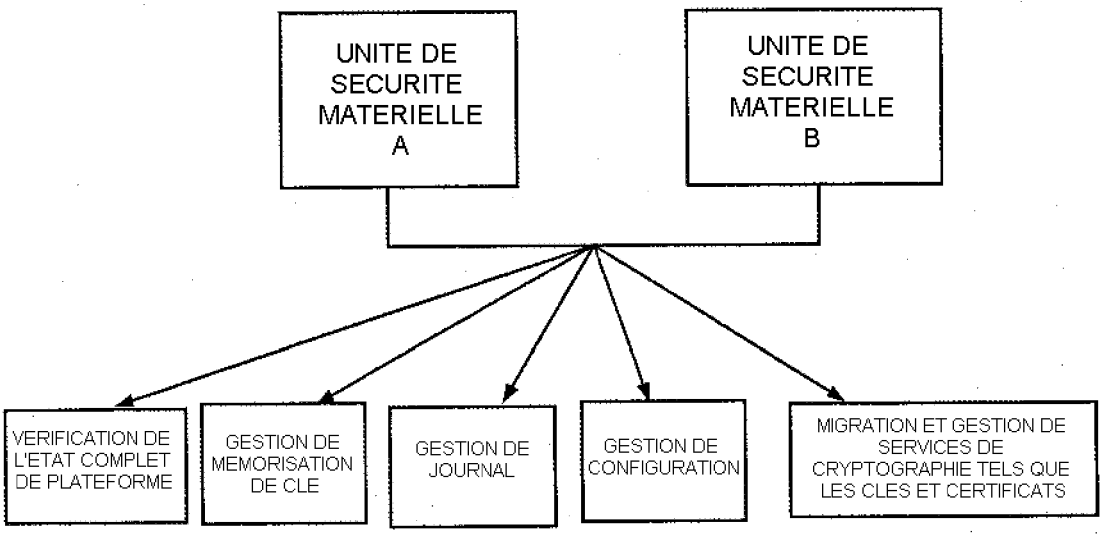
UNITE DE SECURITE MATERIELLE A
UNITE DE SECURITE MATERIELLE B
VERIFICATION DE L'ETAT COMPLET DE PLATEFORME
GESTION DE MEMORISATION DE CLE
GESTION DE JOURNAL
GESTION DE CONFIGURATION
MIGRATION ET GESTION DE SERVICES DE CRYPTOGRAPHIE TELS QUE LES CLES ET CERTIFICATS

Fig. 3

RAPPORT DE RECHERCHE

articles L.612-14, L.612-53 à 69 du code de la propriété intellectuelle

OBJET DU RAPPORT DE RECHERCHE

L'I.N.P.I. annexe à chaque brevet un "RAPPORT DE RECHERCHE" citant les éléments de l'état de la technique qui peuvent être pris en considération pour apprécier la brevetabilité de l'invention, au sens des articles L. 611-11 (nouveauté) et L. 611-14 (activité inventive) du code de la propriété intellectuelle. Ce rapport porte sur les revendications du brevet qui définissent l'objet de l'invention et délimitent l'étendue de la protection.
Après délivrance, l'I.N.P.I. peut, à la requête de toute personne intéressée, formuler un "AVIS DOCUMENTAIRE" sur la base des documents cités dans ce rapport de recherche et de tout autre document que le requérant souhaite voir prendre en considération.

CONDITIONS D'ETABLISSEMENT DU PRESENT RAPPORT DE RECHERCHE

[x] Le demandeur a présenté des observations en réponse au rapport de recherche préliminaire.

☐ Le demandeur a maintenu les revendications.

[x] Le demandeur a modifié les revendications.

☐ Le demandeur a modifié la description pour en éliminer les éléments qui n'étaient plus en concordance avec les nouvelles revendications.

☐ Les tiers ont présenté des observations après publication du rapport de recherche préliminaire.

☐ Un rapport de recherche préliminaire complémentaire a été établi.

DOCUMENTS CITES DANS LE PRESENT RAPPORT DE RECHERCHE

La répartition des documents entre les rubriques 1, 2 et 3 tient compte, le cas échéant, des revendications déposées en dernier lieu et/ou des observations présentées.

[x] Les documents énumérés à la rubrique 1 ci-après sont susceptibles d'être pris en considération pour apprécier la brevetabilité de l'invention.

[x] Les documents énumérés à la rubrique 2 ci-après illustrent l'arrière-plan technologique général.

☐ Les documents énumérés à la rubrique 3 ci-après ont été cités en cours de procédure, mais leur pertinence dépend de la validité des priorités revendiquées.

☐ Aucun document n'a été cité en cours de procédure.

1. ELEMENTS DE L'ETAT DE LA TECHNIQUE SUSCEPTIBLES D'ETRE PRIS EN CONSIDERATION POUR APPRECIER LA BREVETABILITE DE L'INVENTION
US 2005/289343 A1 (TAHAN THOMAS [US]) 29 décembre 2005 (2005-12-29) US 2006/101286 A1 (CATHERMAN RYAN C [US] ET AL) 11 mai 2006 (2006-05-11)
2. ELEMENTS DE L'ETAT DE LA TECHNIQUE ILLUSTRANT L'ARRIERE-PLAN TECHNOLOGIQUE GENERAL
"Trusted Computing Platform Alliance (TCPA). Main Specification, Version 1.0", TCPA MAIN SPECIFICATION, XX, XX, 25 janvier 2001 (2001-01-25), page 293pp, XP009098659,
3. ELEMENTS DE L'ETAT DE LA TECHNIQUE DONT LA PERTINENCE DEPEND DE LA VALIDITE DES PRIORITES
NEANT