RÉPUBLIQUE FRANÇAISE

INSTITUT NATIONAL
DE LA PROPRIÉTÉ INDUSTRIELLE

PARIS

(11) N° de publication : **2 526 977**
(A n'utiliser que pour les commandes de reproduction).

A1

DEMANDE DE BREVET D'INVENTION

(21) **N° 82 08405**

(54) **Procédé et dispositif pour authentifier ou certifier au moins une information contenue dans une mémoire d'un support électronique notamment amovible et portatif tel qu'une carte.**

(51) Classification internationale (Int. Cl.³). **G 06 K 5/00.**

(22) Date de dépôt..... 14 mai 1982.

(33) (32) (31) Priorité revendiquée :

(41) Date de la mise à la disposition du public de la demande..... B.O.P.I. — « Listes » n° 46 du 18-11-1983.

(71) Déposant : COMPAGNIE INTERNATIONALE POUR L'INFORMATIQUE, CII HONEYWELL BULL. — FR.

(72) Invention de : Michel Ugon.

(73) Titulaire :

(74) Mandataire : Marc Doireau, CII Honeywell Bull, 94, av. Gambetta, 75020 Paris.

L'invention concerne généralement les problèmes relatifs au contrôle de la validité de données enregistrées dans une mémoire d'un support électronique, et a plus particulièrement pour objet un procédé et un dispositif pour authentifier ou certifier au moins une information contenue dans une mémoire d'un support électronique, notamment amovible et portatif tel qu'une carte, pour enlever à un fraudeur toute possibilité d'intervenir dans le dialogue entre un appareil dénommé appareil de transaction et une carte connectée à cet appareil, en tentant de laisser croire à l'appareil de transaction que le dialogue s'est opéré tout à fait normalement.

Il est connu des systèmes fondés sur l'utilisation de supports électroniques amovibles qui permettent d'habiliter des personnes ou des organismes à effectuer des opérations protégées propres aux applications envisagées.

D'une façon générale, chaque application revient à permettre à un détenteur d'une carte d'accéder à un service protégé, ce qui impose nécessairement de lire et/ou d'écrire des informations dans la mémoire de la carte pour valider l'accès au service demandé et pour éventuellement garder trace de cet accès matérialisé par exemple par un débit d'une somme d'argent inscrit dans la carte dès l'instant où le service est payant.

Compte tenu de la diversification des applications que peuvent couvrir ces systèmes (transactions bancaires, accès à des réseaux, à des banques de données, à des services, à des enceintes protégées,...), des modifications ou perfectionnements sont sans cesse apportés à ces systèmes, ne serait-ce que pour tenir compte des caractéristiques propres à chaque application.

Dès l'instant où intervient une notion d'accès protégé ou de service protégé, il faut obligatoirement associé à

cette notion la notion de fraude. En effet, le détenteur d'une carte ne pourra pas s'empêcher de se poser les questions suivantes :

- dans le cas d'un service payant, n'est-il pas possible, dans certains cas, d'accéder à ce service gratuitement ?, et
- n'est-il pas possible avec la carte d'accéder à des services auxquels je n'ai normalement pas accès ?

Pour pallier ces tentatives de fraude, une amélioration très importante a consisté à utiliser des mots de passe aléatoires et fugitifs de façon à empêcher un fraudeur de reproduire une séquence de dialogue antérieur entre l'appareil de transaction et la carte connectée à cet appareil, et ayant permis un accès licite à une enceinte ou à un service. Une telle amélioration est décrite dans le brevet français n° 2 469 760 de la Demanderesse et intitulé "Procédé et système d'identification de personnes demandant l'accès à certains milieux". Ce système ainsi réalisé est suffisant lorsqu'il s'agit de protéger un accès à un milieu extérieur au support électronique amovible.

Toutefois, il est généralement nécessaire d'écrire ou de lire des informations dans la mémoire du support électronique soit en local, soit à distance.

Dans ce dernier cas, l'interface entre l'appareil de transaction distant et le support électronique est particulièrement vulnérable à l'observation et à la simulation par des spécialistes, dès lors qu'il y a possibilité de déviation du dialogue vers un organe possédant la capacité de générer une séquence plausible. Plus précisémment, un fraudeur averti, pourrait, en générant une séquence d'informations copiées sur les précédentes, créer des signaux ayant pour but de faire

croire à l'appareil distant que les opérations ont bien lieu en relation avec un support électronique dûment habilité.

L'invention a pour but d'éliminer cet inconvénient grâce à l'introduction d'une donnée dépendant du mot à lire et de sa position dans la mémoire du support électronique. Cette précaution permet de s'assurer de l'origine d'une donnée qui transite sur la liaison entre l'appareil de transaction et le support, et ce, même si l'appareil est très distant du support ce qui est indispensable dans des applications domestiques non surveillées in situ.

L'invention propose donc un procédé pour authentifier ou certifier au moins une information (I) contenue dans une mémoire d'un support électronique, notamment amovible et portatif tel qu'une carte connectée à un appareil assurant le transfert d'informations avec la carte ; ladite carte et ledit appareil comprenant des circuits de traitement ; du type consistant :

- à faire exécuter par les circuits de traitement de la carte et de l'appareil, un même programme (P) déroulant un algorithme aboutissant au calcul d'un résultat (R) au niveau de la carte et d'un résultat (R') au niveau de l'appareil ;
- à comparer les résultats (R) et (R'), l'identité entre ces deux résultats prouvant l'authentification de l'information (I) ; caractérisé en ce qu'il consiste à faire prendre en compte par l'algorithme :
- un paramètre (i) représentatif d'une donnée corrélée à l'information (I) à certifier,
- et un paramètre (a) représentatif de la position en mémoire de l'information (I) à certifier.

Avantageusement, le procédé conforme à l'invention consiste à donner au paramètre (i) la valeur de

l'information (I) à certifier, et à donner au paramètre (a) la valeur de l'adresse mémoire de l'information (I) à certifier.

D'autres caractéristiques, avantages et détails ressortiront de la description explicative qui va suivre faite en référence au dessin schématique annexé donné uniquement à titre d'exemple et illustrant les éléments essentiels d'un appareil de transaction et d'une carte connectée à cet appareil pour montrer le principe et la mise en oeuvre du procédé conforme à l'invention.

En se référant au dessin, il a été représenté un appareil (1) dénommé appareil de transaction auquel peut être connecté un support amovible portatif tel qu'une carte (C). L'appareil (1) et la carte (C) sont reliés par l'intermédiaire d'une liaison de transmission (2). Une telle liaison est notamment décrite dans le brevet français n° 2 483 713 au nom de la Demanderesse et intitulé : "Dispositif pour la transmission de signaux entre deux stations de traitement de l'information".

L'appareil de transaction (1) comprend au moins une mémoire (M) et des circuits de traitement (TM) de données, de façon à exécuter un programme (P) préalablement enregistré dans la mémoire (M) et dont le déroulement permet d'exécuter un algorithme aboutissant à un résultat (R') à partir de paramètres qui seront définis plus loin.

La carte (C) contient également au moins une mémoire (m) et des circuits de traitement (TC) de données, de façon à exécuter le même programme (P) préalablement enregistré dans la mémoire (m) et dont le déroulement permet d'exécuter le même algorithme précité en donnant un résultat (R) en fonction de paramètres qui seront définis plus loin.

L'appareil de transaction (1) permet à un certain nombre d'individus constituant une population d'accéder à au moins un service protégé. Tous les individus de cette population sont détenteur d'une carte (C) pour accéder à ce service. A la limite, une seule carte peut être à la disposition de cette population.

D'une façon générale et plus particulièrement dans l'exemple qui va être décrit, l'accès à ce service va donner lieu à des opérations de lecture et d'écriture dans la carte (C) et à des opérations de calcul par les circuits de traitement (TM ; TC) de l'appareil (1) et de la carte (C) conformément au procédé conforme à l'invention.

Soit un individu désirant bénéficier d'un service par l'intermédiaire de sa carte (C). Cette carte (C) est accouplée en local ou à distance avec l'appareil de transaction (1) qui va valider et matérialiser le service rendu à cet individu. La carte (C) est par exemple introduite dans un lecteur de carte (LC) relié à l'appareil de transaction (1) par l'intermédiaire de la ligne de transmission (2) et de deux interfaces (3, 4) prévus respectivement au niveau du lecteur (LC) et de l'appareil (1).

Après l'initialisation du système, le lecteur (LC) ayant par exemple vérifié que la carte est bien détenue par un individu habilité, il va s'établir un dialogue entre l'appareil (1) et la carte (C).

On suppose qu'au cours de ce dialogue, l'appareil de transaction (1) désire certifier une information (I) contenue dans la mémoire (m) de la carte (C). Autrement dit, l'appareil de transaction (1) veut s'assurer qu'une information (I) communiquée par la carte (C) est bien

celle qui est contenue à une adresse déterminée dans la mémoire (m) ou qu'une information (I) qu'il a précédemment écrite dans la mémoire (m) est bien écrite à l'adresse qu'il a spécifiée.

En conclusion, il s'agit de certifier une information (I) enregistrée à l'adresse (a) de la mémoire (m) de la carte (C).

Une telle certification s'effectue par l'exécution successive des opérations suivantes :

1- un générateur de nombres aléatoires (GNA) prévu par exemple dans l'appareil de transaction (1) délivre un nombre aléatoire (E) qui est transmis à la carte (C) ;

2- l'appareil de transaction (1) envoie également à la carte (C), l'adresse (a) de l'information (I) à certifier, cette adresse (a) ainsi que l'information (I) contenue à cette adresse (a) dans la mémoire (m) de la carte étant, bien évidemment, connues de l'appareil de transaction et enregistrées dans sa mémoire (M) ;

3- la carte (C) déroule ensuite le programme (P) par l'intermédiaire de ses circuits de traitement (TC) pour exécuter un algorithme aboutissant au calcul d'un résultat (R) à partir des paramètres suivants : (E), (a), (I) et (S) : où (E) est le nombre aléatoire précité ; (a) une adresse de la mémoire (m) ; (I) l'information contenue à cette adresse (a) ; (S) étant un code secret spécifique du service demandé et enregistré à la fois au niveau de la carte (C) et de l'appareil de transaction (1), ce code secret étant inconnu du détenteur de la carte et inaccessible de l'extérieur ainsi que le programme (P);

4- l'appareil de transaction (1) déroule également le programme (P) par l'intermédiaire de ses circuits de traitement (TM) pour exécuter le même algorithme aboutissant au calcul d'un résultat (R') à partir des paramètres précités (E), (a), (I) et (S) ;

5- la carte (C) transmet son résultat (R) à l'appareil de transaction (1) qui, par l'intermédiaire d'un circuit de comparaison (CC), le compare avec le résultat (R').

S'il y a identité entre les deux résultats (R) et (R'), l'information (I) a été certifiée par l'appareil (1), c'est-à-dire que cette information (I) est non seulement exacte dans son contenu, mais également bien inscrite à l'adresse (a) de la mémoire (m) de la carte (C).

Il va être donné ci-dessous un exemple justifiant l'intérêt de l'invention.

Supposons qu'un individu porteur d'une carte (C) demande l'accès à un service protégé et que ce service soit payant, ce qui se traduira par l'inscription dans la mémoire (m) de la carte (C) d'une somme d'argent pour garder trace de l'accès à ce service.

En conséquence, l'appareil de transaction (1) doit écrire cette somme d'argent dans la carte (C), somme d'argent qui correspond à l'information (I) précédente.

Supposons terminée cette opération d'écriture de l'information (I) à l'adresse (a) de la mémoire (m) de la carte (C), cette adresse (a) étant par exemple le premier emplacement mémoire libre.

Il est important, voire indispensable, que l'appareil de transaction (1) vérifie que l'information (I) a été effectivement bien écrite à l'adresse (a) de la mémoire (m) de la carte (C). Cela revient à certifier l'information (I) en effectuant la suite des opérations de certification décrites précédemment et aboutissant à la comparaison des deux résultats (R) et (R') précités.

Un tel procédé permet d'éviter une tentative de fraude par l'individu porteur de la carte (C). En effet, cet individu dénommé fraudeur, peut être tenté de faire croire que l'information (I) est bien enregistrée à l'adresse (a), alors qu'en réalité il s'est arrangé pour la faire écrire à une autre adresse ou à l'extérieur de la carte (C). Sans faire intervenir les adresses, une telle opération est parfaitement possible par un spécialiste. Par contre, en faisant intervenir l'adresse (a) de l'information (I), la fraude n'est plus possible pour les raisons suivantes.

Cette adresse (a), le nombre aléatoire (E) et le résultat (R) sont les seules données accessibles au fraudeur, c'est-à-dire les données circulant sur la ligne de transmission (2). Cependant, il est important de noter que le fraudeur ne connaît pas le mode de calcul du résultat (R), puisque celui-ci est effectué à l'intérieur de la carte (C) par le programme (P) inaccessible de l'extérieur et par conséquent secret.

Si le fraudeur modifie l'adresse (a), le résultat (R) calculé à l'intérieur de la carte (C) sera obligatoirement différent du résultat (R') calculé par l'appareil de transaction (1) qui, lui, prend en compte l'adresse (a) et non l'adresse modifiée. Ainsi, même si le fraudeur a pu écrire, par un moyen quelconque, l'information (I) à une adresse autre que l'adresse (a), l'appareil de transaction (1) pourra déceler une telle fraude, c'est-à-dire qu'il pourra être certain que l'information (I) n'a pas été écrite à l'adresse (a).

Dans ces conditions, le fraudeur pourra être tenté de communiquer lui-même le résultat (R) normalement calculé à l'intérieur de la carte (C) et prenant en compte l'adresse (a), sachant que la carte (C) calculera un résultat (R) différent qui prendra en compte l'adresse modifiée

nécessairement communiquée par le fraudeur à la carte (C) pour que celle-ci écrive l'information (I) à cette adresse modifiée. Pour cela, il faudrait que le fraudeur puisse calculer ou connaître à l'avance le résultat (R) correspondant à l'adresse (a), mais cela est impossible puisqu'il ne connait pas le mode de calcul de ce résultat tel que défini par le programme (P) inscrit dans la mémoire (m) de la carte (C) et inaccessible de l'extérieur.

Un cas particulier est intéressant à décrire, lorsque l'appareil de transaction (1) veut écrire une information (I_1) à une adresse (a_1) et que le fraudeur sait à l'avance qu'une information identique a déjà été écrite à une adresse (a_2). Dans ce cas, le fraudeur sera tenté de faire réécrire l'information (I_1) à l'adresse (a_2) surtout si cette information représente un débit bancaire. Une telle fraude est également impossible du fait que les deux informations (I_1) sont différenciées par leurs adresses respectives (a_1) et (a_2).

Il est certain que certaines précautions sont également à prendre au niveau de l'appareil de transaction (1) dont la mémoire (M) contient le programme (P). Dans la mesure où cet appareil se trouve dans une enceinte protégée, il n'est pas nécessaire, a priori, de prendre des précautions particulières.

Cependant, dans certains cas, il sera préférable d'enregistrer le programme (P) dans un support électronique (C_1) par exemple de même nature que la carte (C). Dans ces conditions, il faudra valider l'exécution du programme (P) au niveau de l'appareil de transaction (1) par la fourniture d'un code secret déterminé connu de l'opérateur de l'appareil de transaction et testé par la carte (C_1) accouplée à l'appareil de transaction (1). Ce

type de carte est notamment décrite dans le brevet français n° 2 401 459 et dans la demande de brevet français n° 78 12 119 de la demanderesse.

Si le programme (P) est enregistré dans une carte (C_1) au niveau de l'appareil de transaction (1), l'exécution de ce programme nécéssiterait l'introduction dans la carte (C_1) de l'information (I) à certifier et il faudrait que l'information (I) soit inscrite dans la carte (C_1) à une adresse (a) qui soit la même que celle de la mémoire (m) de la carte (C). Dans ces conditions, il est plus simple de considérer au niveau de la carte (C_1), l'information (I) à certifier comme une information externe entrée dans la carte (C_1) par l'opérateur.

REVENDICATIONS

1. Procédé pour authentifier ou certifier au moins une information (I) contenue dans une mémoire d'un support électronique, notamment amovible et portatif tel qu'une carte (C) connectée à un appareil (1) assurant le transfert d'informations avec la carte (C) ; ladite carte (C) et ledit appareil (1) comprenant des circuits de traitement (TC ; TM) ; du type consistant :
- à faire exécuter par les circuits de traitement de la carte (C) et de l'appareil (1) un même programme (P) déroulant un algorithme aboutissant au calcul d'un résultat (R) au niveau de la carte et d'un résultat (R') au niveau de l'appareil (1) ;
- à comparer les résultats (R) et (R'), l'identité de ces deux résultats prouvant l'authentification de l'information (I) ;
caractérisé en ce qu'il consiste à faire prendre en compte par l'algorithme :
- un paramètre (i) représentatif d'une donnée corrélée à l'information (I) à certifier,
- et un paramètre (a) représentatif de la position en mémoire de l'information (I) à certifier.

2. Procédé selon la revendication 1, caractérisé en ce qu'il consiste à donner au paramètre (i), la valeur de l'information (I) à certifier.

3. Procédé selon la revendication 1 ou 2, caractérisé en ce qu'il consiste à donner au paramètre (a), la valeur de l'adresse mémoire de l'information (I) à certifier.

4. Procédé selon l'une des revendications précédentes, caractérisé en ce qu'il consiste à faire également prendre en compte par l'algorithme précité un nombre aléatoire (E) fourni par la carte (C) ou l'appareil (1).

5. Procédé selon l'une des revendications précédentes, caractérisé en ce qu'il consiste à faire également prendre

en compte par l'algorithme précité, un code secret (S) préenregistré dans la carte (C) et dans l'appareil (1).

6. Procédé selon l'une des revendications précédentes, caractérisé en ce qu'il consiste à préenregistrer le programme (P) précité dans la carte (C) et dans l'appareil (1), le programme (P) et le code secret (S) précité étant inacessibles de l'extérieur.

7. Procédé selon la revendication 6, caractérisé en ce qu'il consite à accoupler à l'appareil (1) un support portatif tel qu'une carte (C_1) dans laquelle est enregistré le programme (P) et comprenant des circuits de traitement pour exécuter ce programme.

8. Procédé selon la revendication 7, caractérisé en ce qu'il consiste à entrer dans la carte (C_1) et depuis l'extérieur l'information (I) à certifier.

9. Carte pour la mise en oeuvre du procédé tel que défini selon l'une des revendications 1 à 8, du type comprenant au moins une mémoire (m) contenant au moins une information (I) à certifier, et des circuits de traitement (TC), caractérisé en ce que la mémoire (m) contient également un programme (P) exécutable par les circuits de traitement (TC) pour donner un résultat (R) prenant au moins en compte l'information (I) et l'adresse (a) de cette information (I) dans la mémoire (m), adresse (a) communiquée aux circuits de traitement (TC) depuis l'extérieur de la carte.

10. Carte selon la revendication 9, caractérisé en ce que la mémoire (m) contient également un code secret (S) pris en compte par le programme (P).

11. Carte selon la revendication 9 ou 10, caractérisée en ce que le programme (P) prend également en compte un nombre aléatoire (E) transmis aux circuits de traitement (TC) précités.

12. Appareil de transaction destiné à être accouplé avec une carte (C) telle que définie selon l'une des revendications 9 à 11, du type comprenant une mémoire (M), des circuits de traitement (TM) et un circuit de comparaison (CC), caractérisé en ce que la mémoire (M) contient le même programme (P) précité et dont l'exécution par les circuits de traitement (TM) prend au moins en compte l'information (I) précitée à certifier et l'adresse (a) précitée de l'information (I) dans la mémoire (m) de la carte (C), pour donner le résultat (R') précité, le circuit de comparaison (CC) comparant le résultat (R) calculé au niveau de la carte et le résultat (R'), l'identité de ces résultats assurant l'authentification de l'information (I).

13. Appareil selon la revendication 12, caractérisé en ce que le programme (P) prend en compte un code secret (S) enregistré dans sa mémoire (M), code secret (S) identique au code secret (S) de la carte (C).

14. Appareil selon la revendication 12 ou 13, caractérisé en ce que le programme (P) prend en compte un nombre aléatoire (E) fourni par un générateur de nombres aléatoires (GNA), nombre aléatoire qui est également transmis à la carte (C).

15. Appareil selon l'une des revendications 12 à 14, caractérisé en ce que la mémoire (M), le programme (P) et les circuits de traitement (TM) sont inclus dans une seconde carte (C_1) accouplée audit appareil.

1,1

