(19) RÉPUBLIQUE FRANÇAISE

INSTITUT NATIONAL
DE LA PROPRIÉTÉ INDUSTRIELLE

PARIS

(11) N° de publication : **2 601 535**
(à n'utiliser que pour les commandes de reproduction).

(21) N° d'enregistrement national : **86 10206**

(51) Int Cl⁴ : H 04 L 9/00, 9/04.

(12) DEMANDE DE BREVET D'INVENTION A1

(22) Date de dépôt : 11 juillet 1986.

(30) Priorité :

(43) Date de la mise à disposition du public de la demande : BOPI « Brevets » n° 2 du 15 janvier 1988.

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

(71) Demandeur(s) : *BULL CP8.* — FR.

(72) Inventeur(s) : Michel Hazard.

(73) Titulaire(s) :

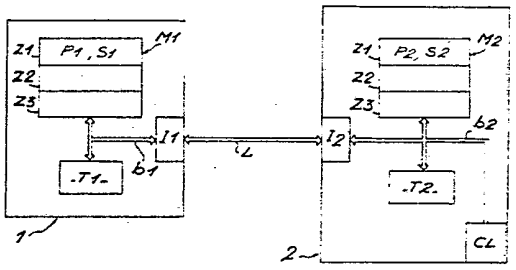
(74) Mandataire(s) : M. Colombe, Bull SA.

(54) Procédé pour certifier l'authenticité d'une donnée échangée entre deux dispositifs connectés en local ou à distance par une ligne de transmission.

(57) L'invention a pour objet un procédé pour certifier l'authenticité d'une donnée échangée entre deux dispositifs connectés en local ou à distance par une ligne de transmission.

Le dispositif émetteur 2 élabore un message chiffré M à partir d'un paramètre X dont au moins un champ X1 doit satisfaire une condition déterminée et un champ X3 qui correspond à la donnée *d* à transmettre. Le dispositif récepteur 1 déchiffre le message M pour trouver un paramètre X' dont le champ X'1 doit satisfaire la même condition que le champ X1 pour que le champ X'3 corresponde à la donnée *d* émise.

L'invention s'applique notamment aux cartes de crédit.



FR 2 601 535 - A1

2601535

Procédé pour certifier l'authenticité d'une donnée échangée entre deux dispositifs connectés en local ou à distance par une ligne de transmission.

L'invention se rapporte à un procédé pour certifier l'authenticité d'une donnée échangée entre deux dispositifs connectés en local ou à distance par une ligne de transmission, chaque dispositif comprenant au moins une mémoire et des circuits de traitement.

L'invention s'applique notamment aux cartes à mémoire accouplées à distance avec un dispositif extérieur pour faire certifier par la carte l'authenticité d'une donnée transmise par le dispositif extérieur ou pour faire certifier par le dispositif extérieur l'authenticité d'une donnée transmise par la carte.

La majorité des applications qui mettent en oeuvre des cartes à mémoire font intervenir des opérations classiques d'écriture et de lecture de données dans la mémoire de la carte. La validité de ces opérations suppose l'authenticité des données échangées entre la carte et le dispositif extérieur, c'est-à-dire qu'une donnée reçue est bien conforme à la donnée émise. Cette authenticité n'est pas garantie lorsque la carte et le dispositif extérieur sont reliés à distance par une voie de transmission classique qui peut être observée par un fraudeur ayant la possibilité de modifier la donnée en cours de transmission. Ce problème est important notamment dans les applications bancaires où les données échangées concernent des crédits ou des débits de sommes d'argent.

Une solution à ce problème peut consister à chiffrer les données à transmettre, mais cette solution n'est pas entièrement satisfaisante. En effet, le récepteur déchiffre la donnée pour obtenir une donnée en clair, mais il n'est pas certain que cette donnée corresponde bien à celle émise.

L'invention pallie cet inconvénient et permet d'authentifier une donnée reçue comme étant non seulement conforme à la donnée émise, mais également émise par un dispositif émetteur habilité. Ainsi l'invention permet de détecter à la fois une donnée modifiée au cours de sa transmission et une donnée émise à partir d'un dispositif émetteur non habilité.

L'invention propose donc un procédé pour certifier l'authenticité d'une donnée échangée entre deux dispositifs émetteur et récepteur reliés par une voie de transmission classique, chaque dispositif comprenant au moins une mémoire et des circuits de traitement, caractérisé en ce qu'il consiste à élaborer au niveau du dispositif émetteur (2) un message chiffré (M) par application de la fonction de chiffrement (f2) d'un algorithme inversible et mise en oeuvre par un programme (P2) exécuté par les circuits de traitement (T2), et tel que :

$$M = f2\ (S2,\ X)$$

où (S2) est la clé de chiffrement de l'algorithme préenregistrée dans la mémoire (M2) du dispositif émetteur (2) et (X) un paramètre décomposé en au moins un champ (X1) satisfaisant une condition prédéterminée et un champ (X2) représentatif de la valeur (v) de la donnée (d),
à transmettre ce message (M) au dispositif récepteur (1),
à déchiffrer ce message (M) par application de la fonction de déchiffrement (f1) dudit algorithme pour obtenir un paramètre (X') tel que :

$$X' = f1\ (M,\ S1)$$

où (S1) est la clé de déchiffrement préenregistrée dans la mémoire (M1) du dispositif récepteur (1),

à décomposer le paramètre (X') en au moins un champ (X'1) et un champ (X'2),
et à vérifier que le champ (X'1) vérifie la même condition prédéterminée que le champ (X1) du paramètre (X) pour en déduire que la valeur de la donnée du champ (X'2) est égale à la valeur de la donnée (d) du champ (X2).

Selon un avantage de l'invention, il est possible d'écrire à distance et en toute sécurité des informations dans un dispositif récepteur notamment constitué par un objet portatif tel qu'une carte de crédit.

D'autres avantages, caractéristiques et détails apparaîtront à la lumière de la description explicative qui va suivre faite en référence à la figure annexée donnée à titre d'exemple et qui représente schématiquement les principaux éléments ou circuits permettant la mise en oeuvre du procédé conforme à l'invention.

En référence à la figure, deux dispositifs électroniques (1, 2) sont connectés en local ou à distance par une voie de transmission classique (L) de type électrique ou optique.

Le dispositif (1) comprend au moins une mémoire (M1), des circuits de traitement (T1) et une interface d'entrée-sortie (I1). Tous ces circuits sont reliés ensemble par l'intermédiaire d'un bus de liaison (b1).

Le dispositif (2) comprend au moins une mémoire (M2), des circuits de traitement (T2), un dispositif d'entrée de données tel qu'un clavier (CL) et une interface d'entrée-sortie (I2). Tous ces circuits sont reliés ensemble par un bus de liaison (b2).

Les mémoires (M1, M2) sont par exemple divisées en au moins deux zones de mémoire (Z1, Z2). Les informations ou

données une fois enregistrées dans les zones de mémoire (Z1) sont vérrouillées afin d'être inaccessibles en lecture et en écriture depuis l'extérieur. Les informations ou données une fois enregistrées dans les zones de mémoire (Z2) ne sont accessibles qu'en lecture depuis l'extérieur. Par contre, toutes les informations enregistrées dans les zones de mémoire (Z1, Z2) sont librement accessibles en interne par les circuits de traitement. Les mémoires (M1, M2) comprennent généralement en plus une zone de travail (Z3) pour le stockage d'informations intermédiaires au cours des opérations exécutées par les circuits de traitement.

A titre d'exemple, le dispositif (1) est constitué par un objet portatif tel qu'une carte, alors que le dispositif (2) est représentatif d'un dispositif extérieur susceptible de dialoguer avec une carte temporairement accouplée à ce dispositif extérieur. Le dialogue qui va s'établir entre la carte et le dispositif permet normalement d'aboutir à la délivrance d'un service ou à une autorisation d'accès par l'intermédiaire de circuits complémentaires non représentés et dont la nature est fonction de l'application envisagée.

Tout dialogue implique nécessairement un échange d'informations et on va supposer que le dispositif extérieur (2) est amené à transmettre une donnée (d) à la carte (1).

Une première mesure de sécurité consiste à ne pas transmettre en clair la donnée (d) qui va être chiffrée avant transmission d'une manière telle que la carte (1) va être capable de pouvoir certifier que la donée déchiffrée est bien conforme à la donnée (d) émise.

La donnée (d) peut être une donnée résultant d'un calcul exécuté par les circuits de traitement (T2) du dispositif

extérieur (2) ou une donnée entrée au clavier (CL) du dispositif extérieur (2) et éventuellement prétraitée par les circuits de traitement (T2).

Le chiffrement de la donnée (d) est obtenu par un programme (P2) préenregistré dans la zone de mémoire (Z1) de la mémoire (M2) et exécuté par les circuits de traitement (T2). Ce programme (P2) est la mise en oeuvre d'une fonction (f2) de chiffrement d'un algorithme inversible. Cette fonction (f2) prend au moins en compte une clé de chiffrement (S2) préenregistrée dans la zone de mémoire (Z1) de la mémoire (M2) et un paramètre (X) qui est lié à la donnée (d).

Plus précisément, le paramètre (X) est décomposé en plusieurs champs (X1, X2, ...Xn) avec au moins un de ces champs qui doit satisfaire une relation prédéterminée et au moins un champ qui est représentatif de la valeur (v) ou configuration binaire de la donnée (d).

A titre d'exemple, le paramètre (X) comprend trois champs (X1, X2, X3) avec :

- X1 = X2 = ad (d)
- X3 = v

où ad(d) est l'adresse mémoire de la carte (1) où doit être enregistrée la donnée (d) et (v) la valeur de la donnée (d).

Il est ainsi obtenu un message chiffré (M) tel que : M = f2(X, S2).

Ce message (M) est transmis à la carte (1) par la voie de transmission (L). Les circuits de traitement (T1) de la carte (1) vont exécuter sur le message (M) reçu un

programme (P1) préenregistré dans la zone de mémoire (Z1) de la mémoire (M1). Ce programme (P1) est la mise en oeuvre de la fonction inverse (f1) ou fonction de déchiffrement de l'algorithme inversible utilisé lors de l'opération de chiffrement par le milieu extérieur (2). Le programme (P1) déchiffre le message (M) au moyen d'une clé de déchiffrement (S1) préenregistrée dans la zone de mémoire (Z1) de la mémoire (M1) et tel que :

$$f1(M, S1) = X'$$

Le paramètre (X') ainsi obtenu est, comme le paramètre (X), décomposé en plusieurs champs (X'1, X'2, ...X'n), et les conditions ou relations qui sont satisfaites par les champs du paramètre (X) doivent également être satisfaites par les champs correspondants du paramètre (X'). En reprenant l'exemple pris précédemment, le paramètre (X') est décomposé en trois champs (X'1, X'2, X'3).

Selon l'invention, si les champs (X'1, X'2) satisfont la même relation que les champs (X1, X2), c'est-à-dire que les informations de ces champs sont identiques et égales à l'adresse (ad) de la donnée (d), la carte considère que le champ (X'3) représente bien la valeur (v) de la donnée (d) transmise par le milieu extérieur (2).

La carte (1) par l'intermédiaire de ses circuits de traitement (T1) peut alors procéder à l'écriture de la donnée (d) à l'adresse (ad) de la zone de mémoire (Z2) ou (Z3) de la mémoire (M1) de la carte (1).

Dans le cas contraire, la carte (1) considère que la valeur (v) de l'information du champ (X'3) du paramètre (X') n'est pas égale à la valeur (v) de la donnée (d) émise. Dans ces conditions, la carte (1) ne prend pas en compte le message (M) reçu sachant qu'il y a eu :

- soit une erreur dans la transmission du message (M),

- soit une modification du message (M) au cours de sa transmission,

- soit que le message (M) n'a pas été émis par un dispositif émetteur habilité si la clé de chiffrement (S2) ne correspond pas à la clé de déchiffrement (S1) de la carte (1) qui est supposée être une bonne carte.

Pour augmenter la sécurité dans la transmission de la donnée (d), le programme de chiffrement (P2) peut également prendre en compte un nombre aléatoire (E). Ainsi, une même donnée (d) sera chiffrée différemment pour éviter qu'un fraudeur puisse réutiliser un message antérieur (M).

Le nombre aléatoire (E) est fourni par la carte elle-même. Plus précisément, ce nombre est prélevé dans la zone de mémoire (Z2) ou zone de contrôle dont au moins un bit est modifié après chaque utilisation de la carte (1). Le nombre aléatoire est alors constitué par le mot de la zone de mémoire (Z1) qui contient le dernier bit modifié. Bien entendu, ce nombre (E) est transmis au milieu extérieur (2) avant l'opération de chiffrement.

En variante, le nombre aléatoire (E) peut être constitué par le contenu initial du mot situé à l'adresse (ad) de la mémoire où l'on désire écrire. Comme l'écriture d'une donnée en mémoire se fait mot par mot, l'écriture d'une donnée (d) de plusieurs mots nécessitera une transmision mot par mot selon le procédé de l'invention avec un nombre aléatoire (E) différent à chaque fois constitué par le contenu du mot à l'adresse (ad) qui est successivement modifié jusqu'à l'écriture complète de la donnée (d).

Bien entendu, l'invention s'applique en sens inverse lorsque le dispositif extérieur (2) veut certifier une donnée (d) transmise par la carte (1).

Les programmes de chiffrement (P2) et de déchiffrement (P1) précités peuvent être identiques, ce qui implique que les clés (S1) et (S2) sont également identiques. Par mesure de sécurité, ces clés doivent rester secrètes et c'est pour cette raison qu'elles sont préenregistrées dans les zones de mémoire (Zi) inaccessibles de l'extérieur.

En variante, l'algorithme précité peut être un algorithme à clé publique connu en soi.

Revendications

1. Procédé pour certifier l'authenticité d'une donnée échangée entre deux dispositifs émetteur et récepteur reliés par une voie de transmission classique, chaque dispositif comprenant au moins une mémoire et des circuits de traitement, caractérisé en ce qu'il consiste à élaborer au niveau du dispositif émetteur (2) un message chiffré (M) par application de la fonction de chiffrement (f2) d'un algorithme inversible et mise en oeuvre par un programme (P2) exécuté par des circuits de traitement (T2), et tel que :

$$M = f2\ (S2,\ X)$$

où (S2) est la clé de chiffrement de l'algorithme préenregistrée dans la mémoire (M2) du dispositif émetteur (2) et (X) un paramètre décomposé en au moins un champ (X1) satisfaisant une condition prédéterminée et un champ (X2) représentatif de la valeur (v) de la donnée (d),
à transmettre ce message (M) au dispositif récepteur (1),
à déchiffrer ce message (M) par application de la fonction de déchiffrement (f1) dudit algorithme pour obtenir un paramètre (X') tel que :

$$X' = f1\ (M,\ S1)$$

où (S1) est la clé de déchiffrement préenregistrée dans la mémoire (M1) du dispositif récepteur (1),
à décomposer le paramètre (X') en au moins un champ (X'1) et un champ (X'2),
et à vérifier que le champ (X'1) vérifie la même condition prédéterminée que le champ (X1) du paramètre (X) pour en déduire que la valeur de la donnée du champ (X'2) est égale à la valeur de la donnée (d) du champ (X2).

2. Procédé selon la revendication 1, caractérisé en ce qu'il consiste à faire prendre en compte par les fonctions (f1, f2) un nombre aléatoire (E).

3. Procédé selon la revendication 2, caractérisé en ce qu'il consiste, lorsque le dispositif émetteur (2) ou le dispositif récepteur (1) est un objet portatif, à faire gérer le nombre aléatoire (E) par l'objet portatif en le prenant dans une zone de mémoire de contrôle (Z2) dont le contenu est modifié à chaque utilisation de l'objet portatif.

4. Procédé selon l'une des revendications précédentes, caractérisé en ce qu'il consiste à définir la condition prédéterminée précitée que doit satisfaire le champ (X1) du parmètre (X), à partir de l'adresse mémoire (ad) à laquelle doit être écrite la donnée (d).

1/1