(19) RÉPUBLIQUE FRANÇAISE

INSTITUT NATIONAL
DE LA PROPRIÉTÉ INDUSTRIELLE

PARIS

(11) **N° de publication :** **2 811 794**
(à n'utiliser que pour les commandes de reproduction)

(21) **N° d'enregistrement national :** **00 09089**

(51) Int Cl[7] : **G 07 F 7/10,** G 07 G 1/14, H 04 L 9/32, G 07 F 7/08

(12) DEMANDE DE BREVET D'INVENTION A1

(22) **Date de dépôt :** 12.07.00.

(30) **Priorité :**

(43) **Date de mise à la disposition du public de la demande :** 18.01.02 Bulletin 02/03.

(56) **Liste des documents cités dans le rapport de recherche préliminaire :** *Ce dernier n'a pas été établi à la date de publication de la demande.*

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

(71) **Demandeur(s) :** *TOKHEIM CORPORATION* — US.

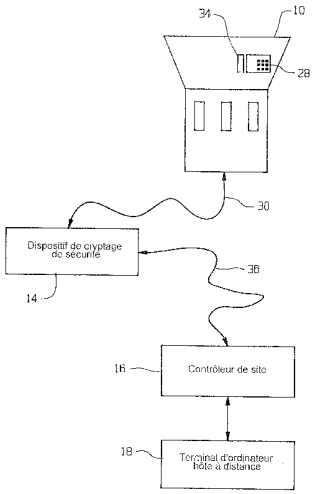
(72) **Inventeur(s) :** BORROS DOUG, PETERS CINDY et SAN GIACOMO RICH.

(73) **Titulaire(s) :**

(74) **Mandataire(s) :** CABINET HERRBURGER.

(54) APPAREIL ET PROCEDE DE PAIEMENT PAR CARTE DE DEBIT DANS UNE STATION DE DISTRIBUTION DE CARBURANT.

(57) Appareil pour effectuer les transactions nécessitant des codes d'identité personnels pour des postes de distribution d'essence. L'appareil comprend une entrée (28) pour le code d'identité personnel, un moyen de cryptage de sécurité (14) pour crypter le code utilisé pour le paiement. Ce cryptage se fait avec un code associé au terminal de l'ordinateur hôte à distance (18) en traversant le contrôleur de site (16).



FR 2 811 794 - A1

Domaine de l'invention.

La présente invention concerne un appareil et un procédé de paiement par carte de débit dans une station de distribution de carburant avec transmission du code d'identité personnel du client.

Description de l'art antérieur

De nombreuses stations services permettent aux clients d'effectuer des transactions de débit pour la distribution de carburant.

Une telle transaction nécessite que le client introduise son code d'identité personnel. Ce code doit être transmis vers un terminal d'ordinateur hôte, à distance qui le compare à l'information ou code PIN pour accepter ou refuser la transaction.

Pour faciliter le paiement, il est souhaitable d'offrir au client une possibilité supplémentaire de payer du carburant dans la station service par une transaction de débit. Toutefois, l'exécution d'une transaction de débit dans un distributeur de carburant nécessite que le client introduise son code d'identité personnel correspondant à son compte de débit. Le code d'identité personnel doit ensuite être transmis au terminal d'ordinateur hôte à distance qui compare l'information de la carte de débit et le code d'identité personnel ainsi introduit pour accepter ou refuser l'opération. La transaction sur les codes d'identité personnels dans les terminaux hôtes à distance se fait par une liaison utilisant des lignes téléphoniques non sécurisées. Le cryptage ou codage des codes d'identité personnels avant leur transmission évite leur interception frauduleuse.

Les systèmes actuels de codage et de transfert du code d'identité personnel consistent à utiliser, au niveau du terminal de paiement de distributeur (DPT), un dispositif de cryptage de sécurité qui assure le cryptage dans le code hôte d'un terminal d'ordinateur hôte à distance. Chaque dispositif de cryptage de sécurité reçoit le code hôte du terminal d'ordinateur hôte à distance dans un environnement sécurisé. Ces dispositifs de cryptage de sécurité sont logés dans un boîtier anti-effraction au niveau du terminal de distribu-

teurs. Les codes d'identité personnels sont cryptés dans le code hôte du terminal d'ordinateur hôte à distance au niveau du terminal de paiement de distributeur avant que ces informations ne soient transmises par le terminal de paiement de distributeur vers le contrôleur de site ou d'autres dispositifs. De cette manière, les codes d'identité personnels sont cryptés avant leur transmission par des lignes téléphoniques non sécurisées.

De plus, on connaît également des systèmes utilisant un dispositif de cryptage de sécurité central qui reçoit le code hôte d'un terminal hôte à distance. Des systèmes classiques utilisant un dispositif de cryptage de sécurité central sont configurés de façon que le dispositif de cryptage de sécurité soit en communication directe seulement avec le contrôleur de site. Ces systèmes utilisent un contrôleur de site pour diriger l'information du terminal de paiement de distributeur vers le dispositif de cryptage et de celui-ci vers le contrôleur de site qui le transmet au terminal hôte à distance. Les systèmes de ce type sont lourds pour le contrôleur de site car toute l'information échangée avec le terminal de distributeur passe à travers le contrôleur de site. Ce contrôleur est le seul dispositif qui communique directement avec le dispositif de cryptage de sécurité.

Certains montages classiques à dispositif de cryptage de sécurité, central, utilisent également un code de cryptage local à l'endroit de l'introduction des codes d'identité personnels pour protéger le transfert du code d'identité personnel du point d'entrée vers le dispositif de cryptage de sécurité central. Le dispositif de cryptage de sécurité, central reçoit ainsi les codes d'identité personnels cryptés par le dispositif d'entrée. Le dispositif de cryptage de sécurité central décrypte les codes d'identité personnels transmis avant de les crypter de nouveau dans le code hôte du terminal d'ordinateur hôte à distance.

La mise en place d'un dispositif de cryptage de sécurité dans lequel on a injecté le code hôte du terminal d'ordinateur hôte à distance au niveau de chaque terminal de paiement de distributeur est une solution sûre et efficace

pour transmettre les codes d'identité personnels cryptés vers un terminal d'ordinateur hôte à distance mais cette configuration est très coûteuse car elle utilise de multiples dispositifs de cryptage de sécurité. Un dispositif de cryptage de sécurité, central est avantageux à cause du moindre coût. Toutefois, ces configurations connues créent des situations dans lesquelles le contrôleur de site est lourdement chargé et doit traiter des flux de trafic d'informations, importants.

La possibilité d'un dispositif de cryptage de sécurité, central diminue le coût des codes d'identité personnels cryptés dans le code hôte du terminal d'ordinateur hôte à distance mais le fait d'avoir un dispositif de cryptage de sécurité, central en communication directe seulement avec le contrôleur de site et décryptant les codes d'identité personnels avant de les recrypter dans le code hôte du terminal hôte à distance crée des difficultés. Dans une telle configuration, le contrôleur de site est surchargé. L'information échangée entre les terminaux de distributeurs et le dispositif de cryptage de sécurité, central, traversent le contrôleur de site qui constitue le seul dispositif en communication directe avec le dispositif de cryptage de sécurité. De plus, le décryptage du code d'identité personnel avant son nouveau cryptage dans le code hôte du terminal d'ordinateur hôte à distance n'est pas la meilleure solution puisque cela crée un endroit supplémentaire dans lequel l'information PIN n'est pas protégée. Les stations services d'essence actuelles, qui permettent des transactions de débit au niveau du distributeur, doivent utiliser des dispositifs de cryptage de sécurité à chaque point d'introduction du code d'identité personnel ; ou encore il faut utiliser un dispositif de cryptage central comme décrit ci-dessus avec les difficultés déjà évoquées.

Résumé de l'invention

La présente invention a pour but de développer l'appareil et le procédé de cryptage et de transmission du code d'identité personnel vers un terminal d'ordinateur hôte à distance, utilisant seulement un dispositif de cryptage de sécurité tout

en réduisant le flux d'informations échangées avec le contrôleur de site et supprimant le décryptage du code d'identité personnel crypté au niveau de chaque point d'entrée.

A cet effet, l'invention concerne un appareil comprenant :

- un moyen d'entrée pour introduire le code d'identité personnel,
- un moyen de cryptage de sécurité pour traduire ce code d'identité personnel dans le code hôte du terminal d'ordinateur hôte à distance, ce moyen de cryptage de sécurité étant relié directement au moyen d'entrée,
- un contrôleur de site coopérant avec le moyen de cryptage de sécurité et relié au terminal hôte à distance, le contrôleur de site n'étant pas relié directement au moyen d'entrée.

Dans cette configuration, le contrôleur de site n'est pas le seul dispositif qui communique directement avec le dispositif de cryptage de sécurité. Comme le contrôleur de site n'est pas le seul responsable de l'échange d'information avec le dispositif de cryptage de sécurité, il n'est pas surchargé par un flux d'information comme dans le cas où il s'agit du seul dispositif dans la ligne de communication pour diriger les communications vers le dispositif de cryptage de sécurité.

L'invention concerne également un procédé et un appareil pour crypter et transmettre des informations dans le code hôte d'un terminal d'ordinateur hôte à distance, n'utilisant pas l'étape de décryptage d'un code d'identité personnel crypté au niveau du point d'entrée.

Sous une forme de réalisation, l'invention concerne un appareil utilisé pour les transactions nécessitant l'introduction du code d'identité personnel et la transmission de celui-ci dans le code hôte du terminal d'ordinateur hôte à distance. Cet appareil comprend des moyens pour introduire le code d'identité personnel et des moyens de cryptage de sécurité pour traduire le code d'identité personnel ainsi introduit dans le code hôte du terminal d'ordinateur hôte à distance. Le dispositif de cryptage de sécurité reçoit les

codes hôtes correspondant à l'ensemble des terminaux d'ordinateurs hôtes à distance. Cette injection se fait dans un environnement sécurisé. Le dispositif de cryptage de sécurité est placé dans un boîtier anti-effraction. Sous cette forme de l'invention, le moyen de cryptage de sécurité est en communication directe avec le moyen d'entrée. Après que le dispositif de cryptage de sécurité ait traduit le code d'identité personnel, celui-ci est transmis à un contrôleur de site communiquant avec le terminal de l'ordinateur hôte à distance. Le contrôleur de site n'est pas en communication directe avec le moyen d'entrée.

Suivant une autre caractéristique de l'invention, il est prévu un moyen d'entrée du code d'identité personnel et un moyen de cryptage local situé à côté du moyen d'entrée. Le moyen de cryptage local crypte les codes d'identité personnels reçus par le moyen d'entrée avant de transmettre ses informations. Un dispositif de cryptage de sécurité reçoit le code d'identité personnel crypté et le traduit dans le code hôte d'un terminal d'ordinateur hôte à distance. Le dispositif de cryptage de sécurité communique le code d'identité personnel crypté au contrôleur de site qui transmet l'information au terminal d'ordinateur hôte à distance.

Sous une autre forme, l'invention concerne un terminal de paiement à distributeur comportant un clavier pour introduire les numéros d'identité personnels, un premier moyen de cryptage injecté dans le terminal de paiement de distributeur, un second dispositif de cryptage, un contrôleur de site et un terminal d'ordinateur hôte à distance. Le premier moyen de cryptage assure le cryptage du code d'identité personnel en utilisant un code de cryptage local. Le terminal de paiement de distributeur communique le code d'identité personnel crypté au moyen de cryptage de sécurité. Le moyen de cryptage de sécurité traduit ce code d'identité personnel crypté dans le code hôte du terminal d'ordinateur hôte à distance. Le moyen de cryptage de sécurité transmet alors le code d'identité personnel crypté vers le contrôleur de site. Le contrôleur de site transmet ensuite cette information au terminal d'ordinateur hôte à distance.

Suivant une autre caractéristique, l'invention concerne un terminal de paiement de distributeur avec un clavier pour introduire le code d'identité personnel et un premier moyen de cryptage pour crypter ce code. Un premier moyen de communication relie le terminal de paiement de distributeur à un dispositif de cryptage de sécurité qui traduit le code d'identité personnel crypté dans le code hôte du terminal hôte à distance. Le dispositif de cryptage de sécurité, mentionné ci-dessus, comporte au moins deux ports de communication dont l'un est relié au premier moyen de communication ci-dessus et l'autre est relié au second moyen de communication. Le second moyen de communication transmet le code d'identité personnel crypté par le dispositif de cryptage au contrôleur de site qui transmet ainsi le code d'identité personnel crypté vers le terminal hôte à distance. Le premier et le second moyen de communication sont tous deux reliés par une liaison RS-485. Le dispositif de cryptage de sécurité comporte également un port d'injection de code et une diode LED indiquant s'il existe une difficulté d'injection de code. Le dispositif de cryptage comporte enfin un indicateur indiquant le fonctionnement des ports de communication de ce dispositif, par exemple une diode LED.

Suivant une autre caractéristique, l'invention concerne un ensemble de terminaux de paiement de distributeur et un multiplexeur qui communique sélectivement les codes d'identité personnels introduits dans chacun des terminaux de paiement de distributeur vers un dispositif de cryptage de sécurité. Ce dispositif de cryptage de sécurité traduit le code d'identité personnel en un code hôte du terminal d'ordinateur hôte à distance.

Suivant une autre caractéristique, l'invention concerne un terminal de paiement de distributeur dans lequel on injecte un premier code de cryptage qui assure le cryptage selon le code dit « code unique, dérivé, par transaction » (code DUKPT). Un dispositif de cryptage de sécurité reçoit le code d'identité personnel qui est crypté en utilisant le schéma de cryptage (DUKPT) ; puis le dispositif de cryptage de sécurité traduit ce code d'identité personnel crypté dans

l'un des différents codes hôtes correspondant chacun à un terminal d'ordinateur hôte à distance. Le dispositif de cryptage transmet alors le code d'identité personnel crypté vers un contrôleur de site communiquant avec un ensemble de terminaux d'ordinateur hôte à distance. Le dispositif de cryptage de sécurité dans cette forme de l'invention comporte un moyen d'addition pour ajouter un moyen de cryptage supplémentaire en cas de besoin. Le dispositif de cryptage de sécurité est contenu dans un boîtier anti-effraction.

La présente invention concerne également un procédé de traitement d'une transaction de débit dans une station de service de carburant. Ce procédé comprend les étapes suivantes :

- on introduit un code d'identité personnel,
- on transmet ce code à un dispositif de cryptage,
- on crypte le code d'identité personnel en un code pour le terminal d'ordinateur hôte à distance,
- on transmet le code d'identité personnel, crypté, vers un contrôleur de site, et
- on transmet ce code d'identité personnel crypté vers le terminal d'ordinateur hôte à distance.

Selon une autre caractéristique de procédé :

- on introduit une carte de débit dans un lecteur de carte du terminal de paiement de distributeur pour accéder aux données de la carte,
- on introduit un code d'identité personnel dans le terminal de paiement de distributeur,
- on crypte le code d'identité personnel pour le paiement dans le distributeur en utilisant un premier code de cryptage,
- on transmet le code d'identité personnel crypté au dispositif de cryptage de sécurité,
- on traduit le code d'identité personnel crypté dans le code hôte d'un terminal d'ordinateur hôte à distance dans le dispositif de cryptage de sécurité,
- on transmet le code d'identité personnel traduit par le dispositif de cryptage de sécurité vers le contrôleur de site,

- on transmet le code d'identité personnel traduit, par le contrôleur de site à un terminal d'ordinateur hôte à distance,
- on transmet l'acceptation ou le refus par l'ordinateur hôte à distance vers le contrôleur de site,
- on transmet l'acception ou le refus du contrôleur de site vers le terminal de paiement de distributeur.

Selon une autre caractéristique, l'invention concerne un moyen de cryptage qui traduit le code d'identité personnel dans le code hôte d'un terminal d'ordinateur hôte à distance. Ce code hôte peut par exemple être l'algorithme Rivest-Shamir-Adelman (RSA), l'algorithme Diffie-Hellman (DH) ou l'algorithme (DUKPT) (code unique dérivé par transaction).

L'avantage principal de l'invention est la possibilité d'assurer le cryptage des codes d'identité personnels dans le code hôte d'un terminal d'ordinateur hôte à distance sans avoir à subir le coût élevé d'un dispositif de cryptage de sécurité à chaque point d'introduction du code d'identité personnel.

Un autre avantage de l'invention est d'utiliser une configuration qui charge moins le contrôleur de site.

Un autre avantage de l'invention est que le dispositif de cryptage de sécurité ne décrypte jamais le code d'identité personnel initialement crypté au niveau du terminal de paiement du distributeur.

Description résumée des dessins.

La présente invention sera décrite ci-après de manière plus détaillée à l'aide des dessins annexés dans lesquels :

- la figure 1 est un diagramme fonctionnel d'un mode de réalisation de l'invention,
- la figure 2 est un diagramme fonctionnel d'un mode de réalisation de l'invention,
- la figure 3 est une vue en perspective du dispositif de traduction de sécurité correspondant à un mode de réalisation de la présente invention,
- la figure 4 est un diagramme fonctionnel d'un mode de réalisation de la présente invention.

Description détaillée de l'invention.

La figure 1 montre un diagramme fonctionnel d'un système d'exécution de transaction de débit dans une station d'essence. Les terminaux de paiement 10 du distributeur coopèrent avec un multiplexeur 12. Ce multiplexeur 12 coopère lui-même avec un dispositif de cryptage 14 qui est relié au site de contrôleur 16. Le site de contrôleur 16 coopère avec des terminaux hôtes à distance 18.

Les terminaux de paiement 10 constituent des moyens pour distribuer des hydrocarbures et des moyens pour exécuter les transactions de débit, pour payer le produit distribué. Les terminaux de paiement 10 comportent un lecteur de carte et une entrée. Les terminaux de paiement comportent également une clef de codage local ; cette clef est introduite dans le terminal de paiement dans un environnement sécurisé. Après avoir reçu les produits, le client paye par une transaction de débit consistant à introduire sa carte de débit dans le lecteur de carte 34. Le client utilise le clavier 28 pour introduire son code d'identité personnel. Le code de cryptage local crypte le code d'identité personnel avant de l'envoyer au multiplexeur 12.

Le multiplexeur 12 reçoit le code d'identité personnel, crypté, provenant des terminaux de paiement 10. Le multiplexeur 12 communique sélectivement les codes d'identité personnels au dispositif de cryptage de sécurité 14. Le dispositif de cryptage de sécurité 14 examine l'information envoyée par le multiplexeur 12. Si le dispositif de cryptage de sécurité détecte le code d'identité personnel, il le traduit en un code hôte pour un terminal d'ordinateur hôte 18, à distance. L'information du code d'identité non personnel traverse le dispositif de cryptage de sécurité pour passer dans le site du contrôleur sans être traduit en un code hôte pour le terminal d'ordinateur hôte à distance. Le dispositif de cryptage communique le code d'identité personnel, traduit, à un contrôleur de site 16. Ce contrôleur 16 transmet alors le code d'identité personnel au terminal d'ordinateur hôte à distance 18. Ainsi, le client peut prendre du carburant et

effectuer une transaction de débit pour payer le carburant au terminal de paiement du distributeur.

La figure 2 montre, sous la forme d'un diagramme fonctionnel, un système d'exécution de transaction de débit. L'entrée 20 reçoit l'information de transaction comprenant le code d'identité personnel. Cette information est communiquée au dispositif de cryptage de sécurité 14 qui détermine la présence d'un code d'identité personnel et traduit ce code en un code hôte pour le terminal d'ordinateur hôte 18 à distance. L'information de code d'identité non personnel est transmise par le dispositif de cryptage de sécurité vers le contrôleur de site 16 sans que sa forme ne soit modifiée. Le contrôleur de site 16 transmet l'information de transaction de débit, y compris le code d'identité personnel codé, au terminal d'ordinateur hôte 18 à distance. Ce terminal 18 compare le code d'identité personnel à l'information de la carte de débit et transmet son accord ou son refus de la transaction au contrôleur de site 16. Cette acceptation ou ce refus est alors communiqué au dispositif de cryptage de sécurité 14 et finalement au dispositif d'entrée 20 ; la transaction peut alors être effectuée dans le dispositif d'entrée 20 où un message indiquant le refus de la transaction peut s'afficher.

La figure 3 montre le dispositif de traduction de sécurité 14 qui fait partie d'un mode de réalisation de l'invention. Le dispositif de traduction 14 comporte au moins deux ports de communication 22. Le dispositif de traduction de sécurité 14 comporte également un indicateur 24 indiquant le fonctionnement des ports de communication 22. Ces indicateurs sont par exemple des diodes LED. Les indicateurs associés aux ports de communication indiquent si les ports de communication sont en cours de transmission d'information. Le dispositif de traduction de sécurité 14 comporte également un port d'introduction de code 32. Le port 32 sert à l'introduction initiale des codes de cryptage dans un environnement de sécurité et il peut aussi servir pour injecter ultérieurement d'autres codes de cryptage. Le dispositif de traduction de sécurité 14 comporte également un indicateur 24 indiquant l'état du port d'injection de code 32. Cet indica-

teur est par exemple une diode LED. Cet indicateur d'état indique si le port d'injection de code est ouvert et prêt pour l'injection, si le port est fermé et si des codes ont été injectés ou si le port est fermé et que des codes n'ont pas été injectés.

La figure 4 montre, sous la forme d'un diagramme fonctionnel, les composants d'un mode de réalisation de l'invention. Le terminal de paiement de distributeur 10 comporte un clavier 28 et un lecteur de carte 34. Le consommateur qui choisit de payer son carburant par une transaction de débit introduit sa carte de débit dans le lecteur de carte 34 et son code d'identité personnel par le clavier 28. L'information de vente et de transaction comprenant le code d'identité personnel est transmise par le terminal de paiement de distributeur 26 au dispositif de cryptage de sécurité 14 par une liaison de communication 30 de type RS-485. A la réception de l'information, le dispositif de cryptage de sécurité détecte si les codes d'identité personnels sont présents et les traduit dans le code hôte d'un terminal d'ordinateur hôte à distance. Le dispositif de cryptage de sécurité transmet alors le code d'identité personnel codé ainsi que les autres informations de transaction vers le contrôleur de site 16. Cette communication du dispositif de cryptage de sécurité 14 vers le contrôleur de site 16 se fait par une liaison de communication 36 de type RS-485. Le contrôleur de site 16 transfère alors cette information à un terminal d'ordinateur hôte à distance 18. Ce terminal 18 compare le code d'identité personnel à l'information de la carte de débit et détermine si la transaction de débit peut être approuvée ou refusée. Cette information est alors transmise en retour au terminal de paiement de distributeur 26 par le site de contrôleur 16 et le dispositif de cryptage de sécurité 14.

REVENDICATIONS

1°) Appareil pour effectuer les transactions nécessitant la soumission de codes d'identité personnels et la transmission de ceux-ci dans un code hôte à un terminal d'ordinateur hôte à distance,
caractérisé en ce qu'il comprend :

- un moyen d'entrée (28) pour introduire le code d'identité personnel,
- un moyen de cryptage de sécurité (14) pour traduire ce code d'identité personnel dans le code hôte du terminal d'ordinateur hôte à distance (18), ce moyen de cryptage de sécurité (14) étant relié directement au moyen d'entrée (28),
- un contrôleur de site (16) coopérant avec le moyen de cryptage de sécurité (14) et relié au terminal hôte à distance (18), le contrôleur de site (16) n'étant pas relié directement au moyen d'entrée (28).

2°) Appareil selon la revendication 1,
caractérisé en ce qu'
il comprend en outre un premier moyen de cryptage pour crypter le code d'identité personnel, ce moyen coopérant avec le moyen d'entrée et avec le moyen de cryptage de sécurité (14).

3°) Appareil selon la revendication 2,
caractérisé en ce que
le moyen d'entrée comprend
un terminal de paiement de distributeur (10) ayant un clavier (28) pour introduire le code d'identité personnel.

4°) Appareil selon la revendication 2,
caractérisé en ce que
le premier moyen de cryptage (14) est injecté dans le terminal de paiement de distributeur (10).

5°) Appareil selon la revendication 4,
caractérisé en ce que

le premier moyen de cryptage (14) crypte selon un schéma de cryptage (DUKPT) (code unique dérivé par transaction).

6°) Appareil selon la revendication 4,
caractérisé en ce que
le moyen de cryptage comprend un second moyen de cryptage pour traduire le code d'identité personnel une fois crypté en un code hôte d'un terminal d'ordinateur hôte à distance (18).

7°) Appareil pour recevoir des code d'identité personnels et les transmettre sous forme codée, lisibles par le code hôte du terminal d'ordinateur hôte à distance d'une banque,
caractérisé en ce qu'il comprend :

- au moins un terminal de paiement de distributeur (10) ayant un clavier (28) pour introduire le code d'identité personnel et un premier moyen de cryptage pour crypter ce code d'identité personnel,
- un premier moyen de communication pour transmettre le code d'identité personnel crypté, ce premier moyen ayant une première extrémité et une seconde extrémité, la première extrémité du premier moyen de communication étant reliée en communication avec le terminal de commande de distributeur,
- un dispositif de cryptage de sécurité (14) pour traduire le code d'identité personnel crypté en un code hôte pour le terminal d'ordinateur hôte à distance (18), ce dispositif de cryptage (14) étant relié à la seconde extrémité du premier moyen de communication, ce dispositif de cryptage de sécurité (14) ayant un second moyen de cryptage et au moins deux ports de communication,
- un second moyen de communication pour transmettre le code d'identité personnel traduit, ce second moyen de communication ayant une première extrémité et une seconde extrémité, la première extrémité du second moyen de communication étant reliée de manière à communiquer avec le dispositif de cryptage de sécurité,
- un contrôleur de site (16) relié à la seconde extrémité du second moyen de communication, et

- un ordinateur hôte, à distance, relié au contrôleur de site (16).

8°) Appareil selon la revendication 7,
caractérisé en ce que
le premier et/ou le second moyen de communication est une liaison RS-485.

9°) Appareil selon la revendication 7,
caractérisé en ce qu'
il comporte en outre plusieurs terminaux de paiement de distributeur (10) et un moyen de multiplexage (12) pour transmettre sélectivement les codes d'identité personnels au dispositif de cryptage de sécurité (14), le multiplexeur (12) étant relié à chacun des différents terminaux de paiement de distributeur (10) et au dispositif de cryptage (14).

10°) Appareil selon la revendication 7,
caractérisé en ce que
le premier moyen de cryptage comprend un moyen cryptant selon le schéma (DUKPT) (code unique dérivé par transaction).

11°) Appareil selon la revendication 7,
caractérisé en ce qu'
il comporte un ensemble de terminaux d'ordinateur hôte à distance (18) ayant un ensemble de moyens de décryptage, ces terminaux d'ordinateur hôte à distance (18) étant reliés au contrôleur de site (16).

12°) Appareil selon la revendication 11,
caractérisé en ce que
le dispositif de cryptage de sécurité comporte un ensemble de seconds moyens de cryptage avec des moyens correspondant à l'ensemble de moyens de décryptage.

13°) Appareil selon la revendication 12,
caractérisé en ce que

le dispositif de cryptage comprend un moyen pour ajouter d'autres moyens de cryptage à l'ensemble des moyens de cryptage.

14°) Appareil selon la revendication 13,
caractérisé en ce que
les moyens supplémentaires comprennent un port d'injection de code prévu sur le dispositif de codage de sécurité.

15°) Appareil selon la revendication 14,
caractérisé en ce que
le dispositif de cryptage de sécurité comprend un premier indicateur indiquant le fonctionnement d'au moins deux ports de communication du dispositif de cryptage de sécurité.

16°) Appareil selon la revendication 15,
caractérisé en ce que
le moyen indicateur comprend au moins une diode LED.

17°) Appareil selon la revendication 14,
caractérisé en ce que
le dispositif de cryptage comprend un moyen indicateur indiquant une difficulté d'injection de code.

18°) Appareil selon la revendication 17,
caractérisé en ce que
le second moyen indicateur est formé d'au moins une diode LED.

19°) Procédé de traitement d'une transaction nécessitant l'introduction d'un code d'identité personnel et sa transmission dans un code hôte vers un terminal d'ordinateur hôte à distance,
caractérisé en ce que

- on introduit un code d'identité personnel,
- on transmet ce code à un dispositif de cryptage,
- on crypte le code d'identité personnel en un code pour le terminal d'ordinateur hôte à distance,

- on transmet le code d'identité personnel, crypté, vers un contrôleur de site, et
- on transmet ce code d'identité personnel crypté vers le terminal d'ordinateur hôte à distance.

20°) Procédé de traitement d'une transaction de débit dans une station service de carburant,
caractérisé en ce qu'

- on introduit une carte de débit dans un lecteur de carte du terminal de paiement de distributeur pour accéder aux données de la carte,
- on introduit un code d'identité personnel dans le terminal de paiement de distributeur,
- on crypte le code d'identité personnel pour le paiement dans le distributeur en utilisant un premier code de cryptage,
- on transmet le code d'identité personnel crypté au dispositif de cryptage de sécurité,
- on traduit le code d'identité personnel crypté dans le code hôte d'un terminal d'ordinateur hôte à distance dans le dispositif de cryptage de sécurité,
- on transmet le code d'identité personnel traduit par le dispositif de cryptage de sécurité vers le contrôleur de site,
- on transmet le code d'identité personnel traduit, par le contrôleur de site à un terminal d'ordinateur hôte à distance,
- on transmet l'acceptation ou le refus par l'ordinateur hôte à distance vers le contrôleur de site,
- on transmet l'acception ou le refus du contrôleur de site vers le terminal de paiement de distributeur.

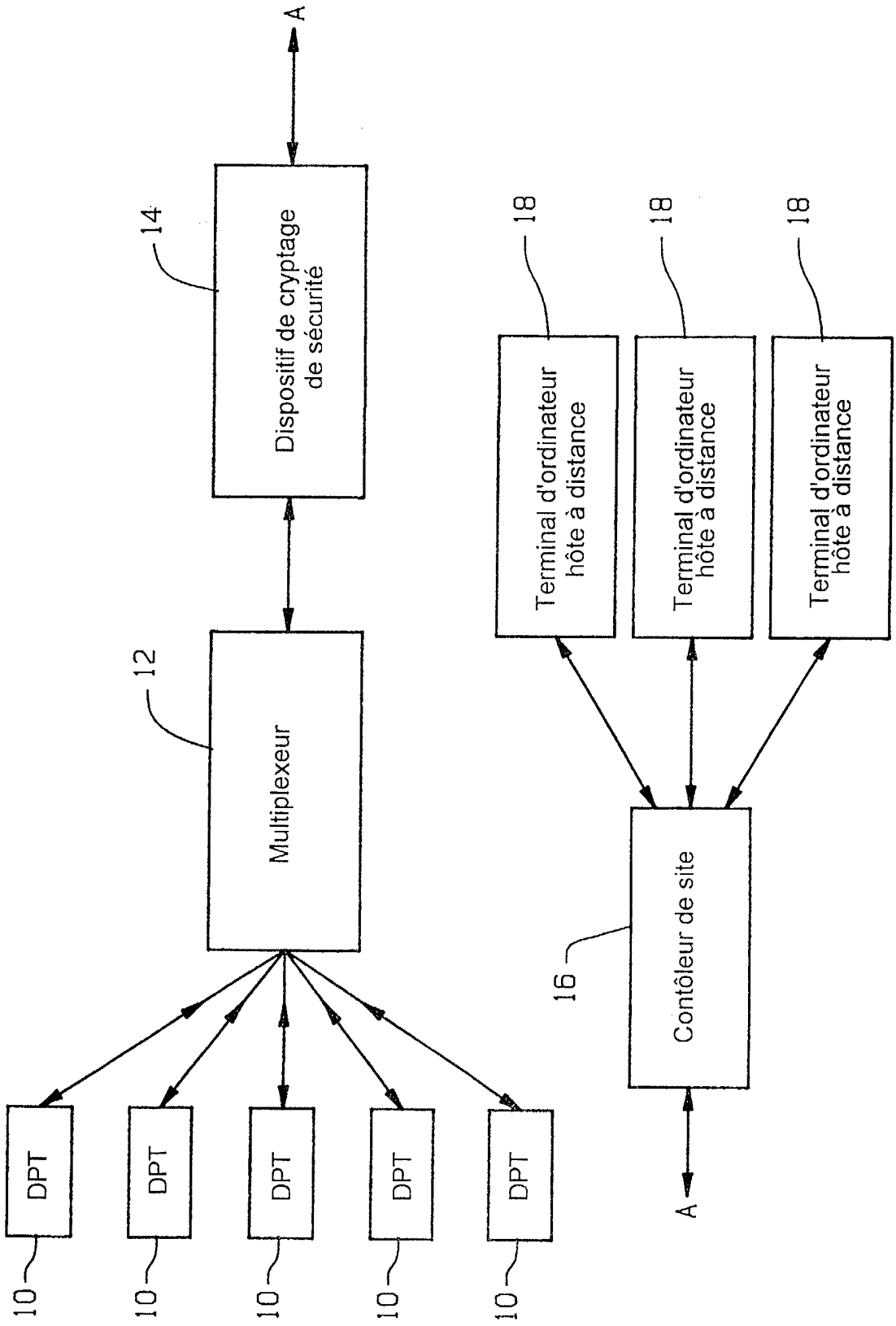

A
14
Dispositif de cryptage de sécurité
12
Multiplexeur
DPT
DPT
DPT
DPT
DPT
10
10
10
10
10
18
18
18
Terminal d'ordinateur hôte à distance
Terminal d'ordinateur hôte à distance
Terminal d'ordinateur hôte à distance
16
Contôleur de site
A

FIGURE 1

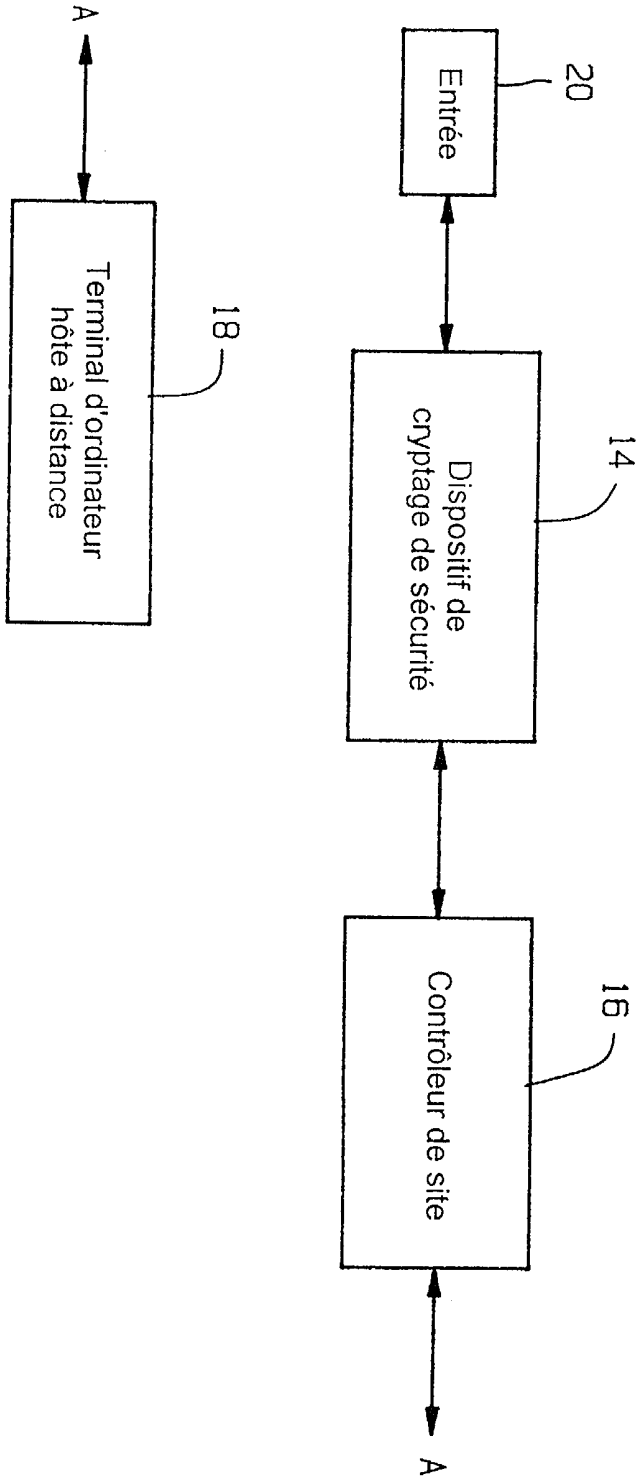

A
Terminal d'ordinateur hôte à distance
18
Entrée
20
Dispositif de cryptage de sécurité
14
Contrôleur de site
16
A

FIGURE 2

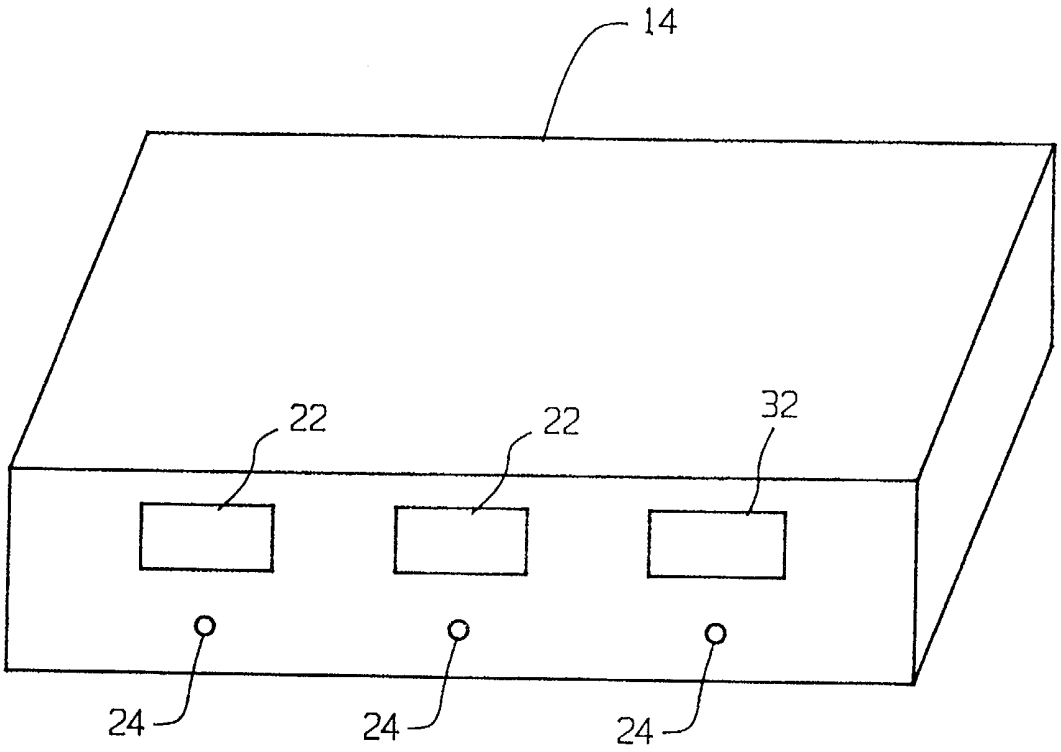


FIGURE 3

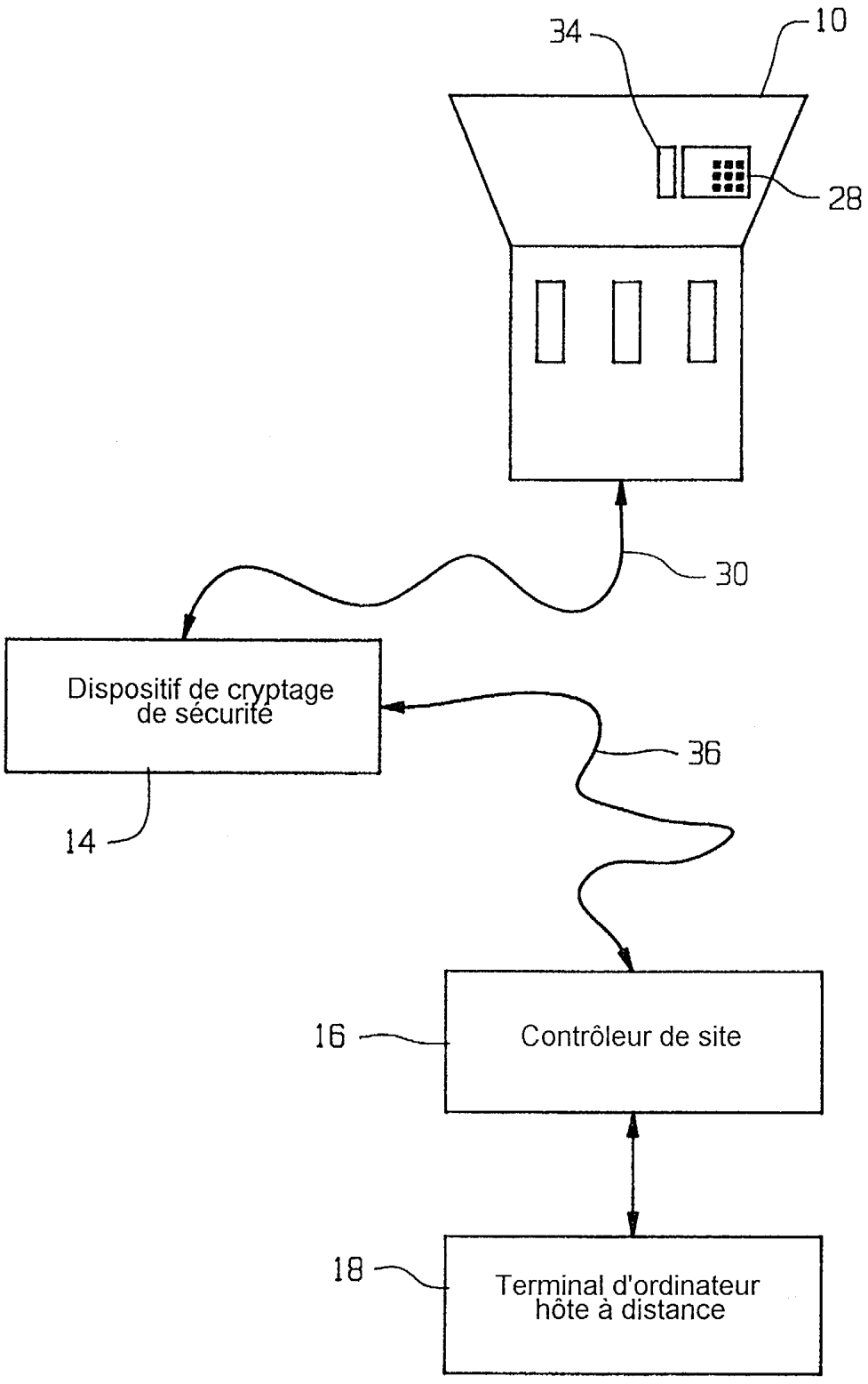

34
10
28
30
Dispositif de cryptage de sécurité
36
14
16
Contrôleur de site
18
Terminal d'ordinateur hôte à distance

FIGURE 4