(19) RÉPUBLIQUE FRANÇAISE

INSTITUT NATIONAL
DE LA PROPRIÉTÉ INDUSTRIELLE

PARIS

(11) N° de publication : **2 706 716**
(à n'utiliser que pour les commandes de reproduction)

(21) N° d'enregistrement national : **93 06942**

(51) Int Cl⁵ : H 04 N 1/419, 1/00, H 04 L 12/00

(12) DEMANDE DE BREVET D'INVENTION A1

(22) **Date de dépôt** : 09.06.93.

(30) **Priorité** :

(43) **Date de la mise à disposition du public de la demande** : 23.12.94 Bulletin 94/51.

(56) **Liste des documents cités dans le rapport de recherche préliminaire** : *Se reporter à la fin du présent fascicule.*

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

(71) **Demandeur(s)** : *KTT Société Anonyme* — FR.

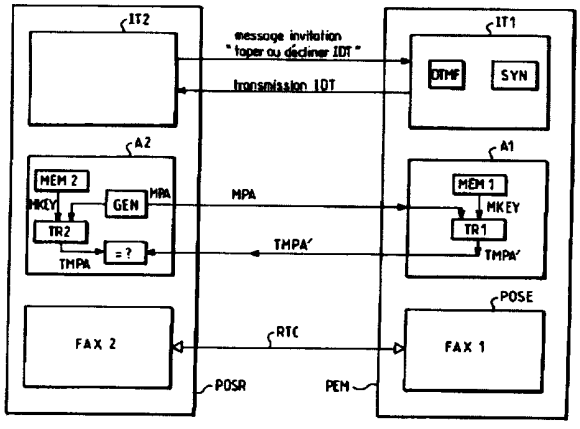
(72) **Inventeur(s)** : Kam Henry.

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

(74) **Mandataire** : Cabinet Netter.

(54) Procédé de télétransmission de documents en particulier du genre télécopie avec authentification de l'identité de la personne émettrice du document et installation pour la mise en œuvre dudit procédé.

(57) Au niveau des moyens de réception (POSR), en réponse à l'identité de la personne émettrice transmise selon une session prédéterminée, il est prévu d'authentifier ladite identité par une authentification active comprenant: au niveau des moyens de réception, la génération et l'émission d'un mot pseudo-aléatoire, et le calcul du transformé de ce mot par la fonction cryptographique à l'aide de la clé émanant des seconds moyens de stockage (MEM2). Au niveau de la personne émettrice, on reçoit le mot ainsi émis, on l'introduit dans les premiers moyens de traitement (TR1) et on calcul le transformé de ce mot par la fonction cryptographique à l'aide de la clé émanant des premiers moyens de stockage (MEM1), et on émet le transformé ainsi calculé. Au niveau des moyens de réception, on reçoit le transformé ainsi émis et on le compare avec le transformé calculé précédemment, et en cas d'authentification positive de l'identité, on établit la télétransmission du document entre le poste émetteur et les moyens de réception.



FR 2 706 716 - A1

Procédé de télétransmission de documents en particulier du genre télécopie avec authentification de l'identité de la personne émettrice du document et installation pour la mise en oeuvre dudit procédé

La présente invention concerne la télétransmission de documents en particulier du genre télécopie avec authentification de l'identité de la personne émettrice du document.

Actuellement, le protocole de communication entre une personne émettrice d'un document utilisant un poste émetteur prédéterminé qui envoie ledit document et les moyens de réception qui le reçoivent à travers un réseau de communication prédéterminé, ne permet pas d'authentifier l'identité de la personne émettrice du document au profit de l'utilisateur des moyens de réception.

Un tel protocole permet au poste émetteur de transmettre aux moyens de réception son indicatif, modifiable selon un mode opératoire prédéterminé à l'initiative de la personne émettrice.

De plus, la télétransmission de documents du genre télécopie est vulnérable aux procédés électroniques connus de falsification de signature appliqués à la télétransmission de document du genre télécopie. Il en résulte qu'un tel protocole a l'inconvénient de ne pas conférer à l'utilisateur des moyens de réception de garantie sur l'intégrité de l'identité de la personne émettrice du document (c'est-à-dire sa signature) apposée sur ledit document télétransmis.

Or, certains utilisateurs de télétransmission de documents tels que les banques, bourses, agents de transactions financières, éprouvent le besoin de savoir de manière sûre et simple que l'identité de la personne émettrice (sa signature) est bien authentique.

La présente invention a justement pour objet de répondre à ce besoin.

Elle porte sur un procédé de télétransmission de documents, en particulier du genre télécopie entre une personne émettrice ayant une identité prédéterminée et utilisant un poste émetteur et des moyens de réception propres à communiquer à travers un réseau de communication prédéterminé avec ledit poste émetteur.

Selon une définition générale de l'invention, le procédé comprend les étapes suivantes :

- 1) au niveau de la personne émettrice, prévoir des premiers moyens de stockage à accès sécurisé, séparés du poste émetteur et propres à stocker une clé secrète, personnelle et associée à l'identité de la personne émettrice, et prévoir des premiers moyens de traitement séparés du poste émetteur et propres à établir une fonction cryptographique à l'aide de ladite clé ;

- 2) au niveau des moyens de réception, prévoir des seconds moyens de stockage propres à stocker ladite clé secrète, personnelle et associée à l'identité de la personne émettrice et son identité associée, des seconds moyens de traitement propres à établir la fonction cryptographique à l'aide de la clé secrète, et prévoir des moyens propres à générer un mot pseudo-aléatoire ;

- 3) au niveau des moyens de réception, en réponse à l'identité de la personne émettrice transmise selon une session prédéterminée entre la personne émettrice et les moyens de réception, authentifier l'identité de la personne émettrice par une authentification active comprenant les étapes suivantes:

*31) au niveau des moyens de réception, générer le mot pseudo-aléatoire, émettre ledit mot pseudo-aléatoire vers la personne émettrice, et calculer le transformé de ce mot

pseudo-aléatoire par la fonction cryptographique à l'aide de la clé émanant des seconds moyens de stockage,

*32) au niveau de la personne émettrice, recevoir le mot pseudo-aléatoire ainsi émis et calculer par les premiers moyens de traitement le transformé de ce mot pseudo-aléatoire par la fonction cryptographique à l'aide de la clé associée à l'identité de la personne émettrice et émanant des premiers moyens de stockage, et émettre le transformé ainsi calculé vers les moyens de réception,

*33) au niveau des moyens de réception, recevoir le transformé ainsi émis et le comparer avec le transformé calculé lors de l'étape 31),

- 4) au niveau de la personne émettrice, en cas d'authentification positive de l'identité de ladite personne émettrice, établir la télétransmission du document avec les moyens de réception en utilisant le poste émetteur.

Un tel procédé offre l'avantage d'authentifier de manière sûre et simple l'identité de la personne émettrice de documents utilisant un poste émetteur.

De préférence, le procédé comprend en outre, au niveau des moyens de réception, l'impression de manière appropriée de l'identité ainsi authentifiée, accompagnée le cas échéant de la date et de l'heure de réception du document ainsi télétransmis.

Selon un mode de réalisation préféré de l'invention, le procédé comprend en outre l'étape dans laquelle, au niveau des moyens de réception, il est prévu d'émettre un accusé de réception au poste émetteur, le cas échéant accompagné de la date et de l'heure d'impression du document ainsi télétransmis.

En pratique, la session relative à la transmission de l'identité de la personne émettrice comprend les étapes suivantes :

- i) au niveau de la personne émettrice, attribuer préalablement une identité prédéterminé à ladite personne émettrice,

- ii) au niveau des moyens de réception, stocker préalablement dans les seconds moyens de stockage l'identité de la personne émettrice en association avec sa clé,

- iii) au niveau de la personne émettrice, établir la communication avec les moyens de réception,

-iv) au niveau des moyens de réception, en cas d'établissement de la communication avec la personne émettrice, émettre un message invitant la personne émettrice à émettre son identité,

-v) au niveau de la personne émettrice, recevoir le message d'invitation ainsi émis et en réponse émettre l'identité de la personne émettrice ainsi attribuée vers les moyens de réception,

-vi) au niveau des moyens de réception, recevoir l'identité ainsi émise, et vérifier l'appartenance de cette identité dans les seconds moyens de stockage, et en cas de vérification positive, procéder à l'étape 31).

De préférence, dans l'étape iv), le message d'invitation est émis par synthèse vocale vers la personne émettrice.

Avantageusement, lors de l'étape v), la personne émettrice compose son identité à l'aide d'un clavier à touches DTMF et/ou décline son identité par la parole.

Selon un autre aspect de l'invention, dans l'étape 32), la personne émettrice introduit le mot pseudo-aléatoire ainsi reçu dans les premiers moyens de traitement tandis qu'il

réachemine le transformé de ce mot pseudo-aléatoire vers les moyens de réception à l'aide d'un clavier à touches DTMF ou à l'aide de la parole via une ligne téléphonique.

L'invention a également pour objet une installation de télétransmission de documents du genre télécopie entre une personne émettrice ayant une identité prédéterminée et utilisant un poste émetteur prédéterminé et des moyens de réception, propres à communiquer à travers un réseau de communication prédéterminé avec ledit poste émetteur, pour la mise en oeuvre du procédé mentionné ci-avant.

Selon une caractéristique importante de l'invention, l'installation comprend:

- au niveau de la personne émettrice, des premiers moyens de stockage à accès sécurisé, séparés du poste émetteur et propres à stocker une clé secrète, personnelle et associée à l'identité de la personne émettrice et des premiers moyens de traitement séparés du poste émetteur et propres à établir une fonction cryptographique à l'aide de ladite clé ;

- au niveau des moyens de réception, des seconds moyens de stockage propres à stocker ladite clé et son identité associée, des seconds moyens de traitement propres à établir la fonction cryptographique à l'aide de ladite clé, et des moyens propres à générer un mot pseudo-aléatoire ;

- au niveau des moyens de réception, en réponse à l'identité de la personne émettrice transmise selon une session prédéterminée entre la personne émettrice et les moyens de réception, les premiers et seconds moyens de traitement étant propres à authentifier l'identité de la personne émettrice par une authentification active dans laquelle:

- au niveau des moyens de réception, les moyens générateurs génèrent le mot pseudo-aléatoire, les moyens de réception émettent ledit mot pseudo-aléatoire vers le poste émetteur, et les seconds moyens de traitement calculent le transformé

de ce mot pseudo-aléatoire par la fonction cryptographique à l'aide de la clé associée à l'identité de la personne émettrice et émanant des seconds moyens de stockage,

- au niveau de la personne émettrice, le poste émetteur reçoit le mot pseudo-aléatoire ainsi émis, la personne émettrice introduit ledit mot pseudo-aléatoire dans les premiers moyens de traitement qui calculent le transformé de ce mot pseudo-aléatoire par la fonction cryptographique à l'aide de la clé associée à l'identité de la personne émettrice et émanant des premiers moyens de stockage, et la personne émettrice émet le transformé ainsi calculé vers les moyens de réception,

- au niveau des moyens de réception, les seconds moyens de traitement reçoivent le transformé ainsi émis et comparent le transformé ainsi reçu et le transformé précédemment calculé,

- en cas d'authentification positive de l'identité de ladite personne émettrice, le poste émetteur établit la télétransmission du document avec les moyens de réception.

En pratique, les premiers moyens de traitement comprennent :

- des moyens d'introduction propres à introduire le mot pseudo-aléatoire ainsi reçu dans les premiers moyens de traitement ;

- des premiers moyens de calcul du transformé du mot pseudo-aléatoire par la fonction cryptographique à l'aide de la clé secrète et personnelle à la personne émettrice émanant des premiers moyens de stockage ; et

- des moyens de délivrance et de réacheminement du transformé ainsi calculé vers le moyens de réception.

Avantageusement, les premiers moyens de traitement ainsi que les premiers moyens de stockage sont logés dans un boîtier portatif de type calculette.

Par ailleurs, les premiers moyens de stockage sont constitués d'une mémoire non volatile protégée contre les agressions extérieures tandis que la clé secrète et personnelle à la personne émettrice est stockée initialement dans lesdits premiers moyens de stockage dans un site sécurisé prédéterminé.

De préférence, les premiers moyens de traitement comprennent des moyens de contrôle d'accès sécurisé.

En variante, les premiers moyens de traitement comprennent un lecteur de carte tandis que les premiers moyens de stockage sont logés dans une carte à mémoire susceptible d'être en liaison avec ou sans contact avec ledit lecteur de carte pour l'utilisation de la clé par la fonction cryptographique à l'issue d'un contrôle d'accès prédéterminé.

Dans cette variante, les premiers moyens de stockage comprennent des moyens de contrôle d'accès sécurisé.

Selon un autre aspect de l'invention, les seconds moyens de traitement comprennent:
- des seconds moyens de calcul du transformé du mot pseudo-aléatoire par la fonction cryptographique à l'aide de la clé émanant des seconds moyens de stockage, et
- des moyens de comparaison du transformé ainsi calculé avec le transformé reçu.

Avantageusement, dans les moyens de réception il est prévu d'associer à l'identité de la personne émettrice un numéro annuaire correspondant à un poste du genre télécopieur sur lequel des compte rendus sont transmis en liaison avec la télétransmission dont l'identité de la personne émettrice est ainsi authentifiée.

D'autres caractéristiques apparaîtront à la lumière de la description détaillée ci-après et des dessins annexés dans lesquels :

- la figure 1 est une représentation schématique de l'installation selon l'invention ;

- la figure 2 est un organigramme illustrant la session relative à la transmission de l'identité de la personne émettrice selon l'invention ; et

- la figure 3 est une représentation schématique illustrant l'authentification active de l'identité de la personne émettrice ainsi transmise selon l'invention.

En référence à la figure 1, une installation de télétransmission de documents en particulier du genre télécopie met en coopération un poste émetteur POSE et des moyens de réception POSR. Le poste émetteur et les moyens de réception communiquent à travers un réseau de communication prédéterminé par exemple le réseau de communication commuté public RTC.

Le poste émetteur comprend des moyens FAX1 propres à assurer les fonctions d'un télécopieur classique.

A l'autre extrémité, les moyens de réception comprennent des moyens FAX2 propres à assurer certaines fonctions d'un télécopieur classique.

D'une manière connue, les moyens télécopieurs FAX2 comprennent des moyens d'impression simultanée ou différée (non représentés) des documents télétransmis.

Comme mentionné ci-avant, une telle installation présente l'inconvénient de ne pas garantir à l'utilisateur des moyens de réception l'intégrité de l'identité IDT de la personne émettrice PEM du document télétransmis à partir du poste émetteur POSE.

Selon l'invention, il est prévu de compléter une telle installation par des moyens IT1 et IT2 permettant de transmettre l'identité IDT de la personne émettrice PEM entre ladite personne émettrice et les moyens de réception selon

une session décrite en référence à la figure 2 et des moyens A1 et A2 permettant d'authentifier ladite identité ainsi transmise avec précision, simplicité et certitude selon le procédé dont les étapes sont décrites en référence à la figure 3.

Sur la figure 2, on a représenté schématiquement les étapes relatives à la transmission de l'identité de la personne émettrice précédant l'authentification active de l'identité de la personne émettrice selon l'invention.

Lors de l'étape i), au niveau de la personne émettrice PEM, il est prévu d'attribuer une identité IDT prédéterminée. Par exemple cette identité est une suite numérique à quatre chiffres ou un nom ou mot à plusieurs caractères.

Dans l'étape ii), en symétrie, il est prévu de stocker dans les moyens IT2 l'identité IDT ainsi attribuée en correspondance avec la clé secrète associée MKEY que l'on décrira plus en détail ci-après. De préférence, l'identité IDT est stockée dans les seconds moyens de stockage MEM2 que l'on décrira plus en détail ci-après.

Lors de l'étape iii), la personne émettrice PEM demande l'établissement d'une communication avec les moyens de réception de manière appropriée, par exemple par un appel téléphonique.

Dans l'étape iv), en réponse à cette demande, les moyens de réception établissent la communication de manière appropriée et engendre un message d'invitation "taper et/ou décliner votre identité SVP".

Dans l'étape v), la personne émettrice reçoit le message d'invitation, par exemple par synthèse vocale SYN.

La personne émettrice en réponse à cette diffusion tape sur un clavier à touches DTMF et/ou décline par la parole en

utilisant une ligne téléphonique prédéterminée, l'identité IDT qui lui a été préalablement attribuée.

En l'absence de réponse de la personne émettrice, les moyens de réception se positionnent avantageusement après une temporisation d'une durée prédéterminée en réception télécopie sans authentification de l'identité de la personne émettrice. Par exemple, la télétransmission du document est accompagnée d'une indication relative à la non authentification de l'identié de la personne émettrice.

Lors de l'étape vi), les moyens de réception reçoivent l'identité IDT et vérifie au niveau des moyens IT2 si elle est connue des moyens IT2 (ou MEM2) en correspondance avec la clé secrète MKEY.

En cas de vérification positive, il est procédé à l'authentification active de l'identité, tandis qu'en cas de vérification négative, la télétransmission est tout de même effectuée avec de préférence une indication relative à l'authentification négative de l'identité de la personne émettrice.

Dans la figure 3, on a représenté l'organigramme illustrant l'authentification de l'identité ainsi transmise.

Lors de l'étape 1), au niveau de la personne émettrice PEM, on prévoit des premiers moyens de stockage MEM1 à accès sécurisés, séparés du poste émetteur, et propres à stocker une clé secrète, personnelle, et associée à l'identité de la personne émettrice MKEY. On prévoit également des premiers moyens de traitement TR1 propres à établir une fonction cryptographique F à l'aide de ladite clé associée à l'identité de la personne émettrice MKEY.

Lors de l'étape 2), au niveau du moyens de réception POSR, on prévoit des seconds moyens de traitement TR2 propres à établir la fonction cryptographique F à l'aide de la clé associée à l'identité de la personne émettrice MKEY. On prévoit également des moyens générateurs GEN propres à

générer un mot pseudo-aléatoire MPA et des seconds moyens de stockage MEM2 propres à stocker ladite clé associée à l'identité de la personne émettrice MKEY, et l'identité IDT correspondante.

Lors de l'étape 3), aux niveau des moyens de réception, en réponse à la session relative à la transmission de l'identité de la personne émettrice décrite en référence à la figure 2, il est prévu d'authentifier l'identité IDT de la personne émettrice ainsi transmise par une authentification active comprenant les étapes suivantes:

*31) au niveau des moyens de réception, générer le mot pseudo-aléatoire par les moyens générateurs GEN, calculer le transformé TMPA de ce mot pseudo-aléatoire par la fonction cryptographique F établit par les seconds moyens de traitement TR2 à l'aide de la clé associée à l'identité IDT émanant des seconds moyens de stockage et émettre ledit mot pseudo-aléatoire MPA vers la personne émettrice, à travers la ligne téléphonique reliant les moyens IT1 et IT2 mentionnés ci-avant.

*32) au niveau de la personne émettrice PEM, recevoir le mot pseudo-aléatoire ainsi émis, par ladite ligne téléphonique, introduire ledit mot pseudo-aléatoire MPA dans les premiers moyens de traitement TR1 et calculer le transformé TMPA'de ce mot pseudo-aléatoire par la fonction cryptographique F établit par les premiers moyens de traitement TR1 à l'aide de la clé MKEY associée à l'identité de la personne émettrice et émanant des premiers moyens de stockage MEM1, et émettre le transformé TMPA' ainsi calculé vers les moyens de réception, par ladite ligne téléphonique.

*33) au niveau des moyens de réception, recevoir le transformé ainsi émis et comparer le transformé ainsi reçu TMPA' et le transformé TMPA calculé lors de l'étape 31),

Dans l'étape 4), en cas d'authentification positive de l'identité de ladite personne émettrice, établir la télé-

transmission du document entre le poste émetteur et les moyens de réception par les moyens FAX1 et FAX2 mentionnés ci-avant.

Avantageusement lors de l'étape 5), il est prévu d'imprimer sous la forme d'une page d'accompagnement l'identité ainsi authentifiée, accompagnée le cas échéant de la date et de l'heure de réception du document.

Eventuellement, lors de l'étape 6), au niveau du moyens de réception, il est prévu d'émettre un accusé de réception au poste émetteur, le cas échéant accompagné de la date et de l'heure d'impression du document.

Bien entendu, d'autres opérations de gestion peuvent être prévues à l'issue de l'authentification de l'identité du poste émetteur telles que l'impression différée ou l'impression de compte rendus à destination de numéros d'annuaires choisis correspondant à des postes télécopieurs choisis.

Les seconds moyens de traitement TR2 ainsi que les seconds moyens de stockage MEM2 sont à proximité ou éloignés des moyens de réception.

Par exemple, la fonction cryptographique F correspond à un algorithme de chiffrement/déchiffrement de données de type à clés secrètes, de très haute performance, par exemple un algorithme DES.

Selon un mode particulier de l'invention, les moyens de traitement TR1 sont logés dans un boîtier portatif du type calculette (non représentée).

Cette calculette comprend un dispositif d'affichage et un clavier.

A l'intérieur de cette calculette, sont logés les moyens de calcul du transformé du mot pseudo-aléatoire. Par ailleurs, les moyens de stockage MEM1 contenant la clé secrète MKEY

sont logés également de manière appropriée dans cette calculette.

Avantageusement, la mémoire MEM1 contenant la clé secrète est une mémoire non volatile protégée de manière appropriée à l'égard des agressions extérieures physiques, mécaniques ou logiciels.

En pratique, la clé secrète MKEY est programmée en usine, c'est-à-dire dans un milieu extérieur à l'utilisation du poste. Cette clé secrète est indissociablement liée à la personne émettrice.

Ainsi, la calculette peut permettre à la personne émettrice, en réponse au mot pseudo-aléatoire MPA émanant des moyens de réception, d'introduire ce mot pseudo-aléatoire dans la calculette, par exemple à l'aide du clavier de ladite calculette, et de calculer le transformé de ce mot aléatoire par la fonction cryptographique F à l'aide de la clé secrète et personnelle émanant des moyens de stockage MEM1.

Avantageusement, l'utilisation de la clé secrète par les premiers moyens de traitement s'effectue à l'issue d'un contrôle d'accès.

Dans le cadre de la calculette, le contrôle d'accès s'effectue au niveau des premiers moyens de traitement TR1, par exemple par un mot de passe composé au clavier de la calculette. Le degré de sécurité est ici conféré par l'utilisation du mot de passe associé au clavier de la calculette.

En variante, les premiers moyens de traitement TR1 comprennent un lecteur de carte tandis que les premiers moyens de stockage sont logés dans une carte du type carte à puce susceptible d'être en liaison avec ou sans contact avec ledit lecteur de carte pour permettre l'utilisation de la clé par les premiers moyens de traitement TR1.

Avantageusement, cette utilisation s'effectue aussi à l'issue d'un contrôle d'accès prédéterminé.

Dans le cadre de la variante où l'interactivité réside dans la coopération d'un lecteur de carte et d'une carte, le contrôle d'accès s'effectue au niveau de l'usage de ladite carte, par exemple par la composition d'un code confidentiel au niveau du lecteur de carte. Le degré de sécurité est ici conféré par l'utilisation du code confidentiel associé à la carte.

Selon un autre aspect de l'invention, dans les moyens de réception il est prévu d'associer à l'identité de la personne émettrice un numéro annuaire correspondant à un poste du genre télécopieur sur lequel des compte rendus sont transmis en liaison avec la télétransmission dont l'identité de la personne émettrice est ainsi authentifiée.

Revendications

1. Procédé de télétransmission de documents en particulier du genre télécopie entre une personne émettrice ayant une identité prédéterminée et utilisant un poste émetteur prédéterminé et des moyens de réception propres à communiquer à travers un réseau de communication prédéterminé avec ledit poste émetteur, caractérisé en ce qu'il comprend les étapes suivantes:

- 1) au niveau de la personne émettrice, prévoir des premiers moyens de stockage à accès sécurisé, séparés du poste émetteur (POSE) et propres à stocker une clé (MKEY) secrète, personnelle et associée à l'identité (IDT) de la personne émettrice (PEM)et prévoir des premiers moyens de traitement (TR1) séparés du poste émetteur (POSE) et propres à établir une fonction cryptographique à l'aide de ladite clé ;

- 2) au niveau des moyens de réception (POSR), prévoir des seconds moyens de stockage (MEM2) propres à stocker ladite clé (MKEY) et son identité associée (IDT), prévoir des seconds moyens de traitement (TR2) propres à établir la fonction cryptographique (F) à l'aide de ladite clé (MKEY), et prévoir des moyens générateurs (GEN) propres à générer un mot pseudo-aléatoire (MPA);

- 3) au niveau des moyens de réception (POSR), en réponse à l'identité (IDT) de la personne émettrice transmise selon une session prédéterminée entre la personne émettrice et les moyens de réception, authentifier l'identité de la personne émettrice par une authentification active comprenant les étapes suivantes:

*31) au niveau des moyens de réception, générer le mot pseudo-aléatoire, émettre ledit mot pseudo-aléatoire vers la personne émettrice, et calculer par les seconds moyens de traitement (TR2) le transformé de ce mot pseudo-aléatoire par

la fonction cryptographique à l'aide de la clé émanant des seconds moyens de stockage (MEM2),

*32) au niveau de la personne émettrice, recevoir le mot pseudo-aléatoire ainsi émis, introduire ledit mot pseudo-aléatoire dans les premiers moyens de traitement (TR1) et calculer par lesdits premiers moyens de traitement (TR1) le transformé de ce mot pseudo-aléatoire par la fonction cryptographique à l'aide de la clé émanant des premiers moyens de stockage (MEM1), et émettre le transformé ainsi calculé vers les moyens de réception,

*33) au niveau des moyens de réception, recevoir le transformé ainsi émis et le comparer avec le transformé calculé lors de l'étape 31),

- 4) en cas d'authentification positive de l'identité de ladite personne émettrice, établir la télétransmission du document entre le poste émetteur et les moyens de réception.

2. Procédé selon la revendication 1, caractérisé en ce qu'il comprend en outre l'étape suivante:

-5) au niveau des moyens de réception, imprimer de manière appropriée l'identité ainsi authentifiée, accompagnée le cas échéant de la date et de l'heure de réception du document ainsi télétransmis.

3. Procédé selon la revendication 1 ou la revendication 2, caractérisé en ce qu'il comprend en outre l'étape suivante:

-6) au niveau des moyens de réception (POSR), émettre un accusé de réception au poste émetteur, le cas échéant accompagné de la date et de l'heure d'impression du document ainsi télétransmis.

4. Procédé selon l'une des revendications précédentes, caractérisé en ce que la session relative à la transmission

de l'identité de la personne émettrice comprend les étapes suivantes :

-i) au niveau de la personne émettrice (PEM), attribuer préalablement une identité prédéterminée (IDT),

- ii) au niveau des moyens de réception, stocker préalablement dans les seconds moyens de stockage (MEM2) l'identité (IDT) de la personne émettrice en association avec sa clé (MKEY),

- iii) au niveau de la personne émettrice, établir la communication avec les moyens de réception,

-iv) au niveau des moyens de réception, en cas d'établissement de la communication avec la personne émettrice, émettre un message invitant la personne émettrice à émettre son identité ainsi préalablement attribuée (IDT),

-v) au niveau de la personne émettrice, recevoir le message d'invitation ainsi émis et en réponse émettre l'identité de ladite personne émettrice vers les moyens de réception,

-vi) au niveau des moyens de réception, recevoir l'identité ainsi émise, et vérifier l'appartenance de cette identité dans les seconds moyens de stockage (MEM2), et en cas de vérification positive, procéder à l'étape 31).

5. Procédé selon la revendication 4, caractérisé en ce que dans l'étape iv), le message d'invitation est émis par synthèse vocale vers la personne émettrice.

6. Procédé selon la revendication 4, caractérisé en ce que dans l'étape v), la personne émettrice du poste émetteur compose son identité (IDT) à l'aide d'un clavier à touches DTMF et/ou décline son identité par la parole.

7. Procédé selon la revendication 1, caractérisé en ce que dans l'étape 32) la personne émettrice introduit le mot

pseudo-aléatoire (MPA) ainsi reçu dans les premiers moyens de traitement (TR1) tandis qu'elle réachemine le transformé (TMPA') de ce mot pseudo-aléatoire vers les moyens de réception à l'aide d'un clavier à touches DTMF ou à l'aide de la parole via une ligne téléphonique prédéterminée.

8. Installation de télétransmission de documents du genre télécopie entre une personne émettrice ayant une identité prédéterminée (IDT) et utilisant un poste émetteur prédéterminé (POSE) et des moyens de réception (POSR), propres à communiquer à travers un réseau de communication prédéterminé avec ledit poste émetteur (POSE), pour la mise en oeuvre du procédé selon l'une quelconque des précédentes revendications 1 à 7, caractérisée en ce qu'elle comprend:

- au niveau de la personne émettrice (PEM), des premiers moyens de stockage (MEM1) à accès sécurisé, séparés du poste émetteur (POSE) et propres à stocker une clé (MKEY) secrète, personnelle et associée à l'identité (IDT) de la personne émettrice et des premiers moyens de traitement (TR1) séparés du poste émetteur (POSE) et propres à établir une fonction cryptographique (F) à l'aide de ladite clé (MKEY);

- au niveau des moyens de réception (POSR), des seconds moyens de stockage (MEM2) propres à stocker ladite clé (MKEY) et son identité associée (IDT), des seconds moyens de traitement (TR2) propres à établir la fonction cryptographique (F) à l'aide de ladite clé, et des moyens (GEN) propres à générer un mot pseudo-aléatoire (MPA);

- au niveau des moyens de réception (POSR), en réponse à l'identité (IDT) de la personne émettrice transmise selon une session prédéterminée entre la personne émettrice et les moyens de réception, les premiers et seconds moyens de traitement (TR1 et TR2) étant propres à authentifier l'identité de la personne émettrice ainsi transmise par une authentification active dans laquelle:

- au niveau des moyens de réception, les moyens générateurs (GEN) génèrent le mot pseudo-aléatoire (MPA), les moyens de réception émettent ledit mot pseudo-aléatoire vers la personne émettrice, et les seconds moyens de traitement (TR2) calculent le transformé (TMPA) de ce mot pseudo-aléatoire par la fonction cryptographique (F) à l'aide de la clé (MKEY) émanant des seconds moyens de stockage (MEM2) et
- au niveau de la personne émettrice, ladite personne émettrice reçoit le mot pseudo-aléatoire ainsi émis, elle introduit ledit mot pseudo-aléatoire dans les premiers moyens de traitement (TR1) qui calculent le transformé (TMPA') de ce mot pseudo-aléatoire par la fonction cryptographique (F) à l'aide de la clé (MKEY) émanant des premiers moyens de stockage (MEM1), et la personne émettrice émet le transformé ainsi calculé (TMPA') vers les moyens de réception,

- au niveau des moyens de réception, les seconds moyens de traitement (TR2) reçoivent le transformé ainsi émis (TMPA') et le comparent avec le transformé précédemment calculé (TMPA),

- en cas d'authentification positive de l'identité de ladite personne émettrice, le poste émetteur établit la télétransmission du document avec les moyens de réception.

9. Installation selon la revendication 8, caractérisée en ce que les premiers moyens de traitement (TR1) comprennent :

- des moyens d'introduction propres à introduire le mot pseudo-aléatoire ainsi reçu,

- des premiers moyens de calcul du transformé de ce mot pseudo-aléatoire par la fonction cryptographique à l'aide de la clé (MKEY) émanant des premiers moyens de stockage (MEM1), et

- des moyens de délivrance et de réacheminement du transformé ainsi calculé vers les moyens de réception.

10. Installation selon la revendication 9, caractérisée en ce que les premiers moyens de traitement (TR1) ainsi que les premiers moyens de stockage (MEM1) sont logés dans un boîtier portatif de type calculette.

11. Installation selon la revendication 10, caractérisée en ce que les premiers moyens de stockage (MEM1) sont constitués d'une mémoire non volatile protégée contre les agressions extérieures tandis que la clé secrète et personnelle à la personne émettrice est stockée initialement dans lesdits premiers moyens de stockage dans un site sécurisé prédéterminé.

12. Installation selon la revendication 10, caractérisée en ce que les premiers moyens de traitement (TR1) comprennent des moyens de contrôle d'accès.

13. Installation selon la revendication 9, caractérisée en ce que les premiers moyens de traitement (TR1) comprennent un lecteur de carte tandis que les premiers moyens de stockage (MEM1) sont logés dans une carte à mémoire susceptible d'être en liaison avec ou sans contact avec ledit lecteur de carte pour l'utilisation de la clé à l'issue d'un contrôle d'accès prédéterminé.

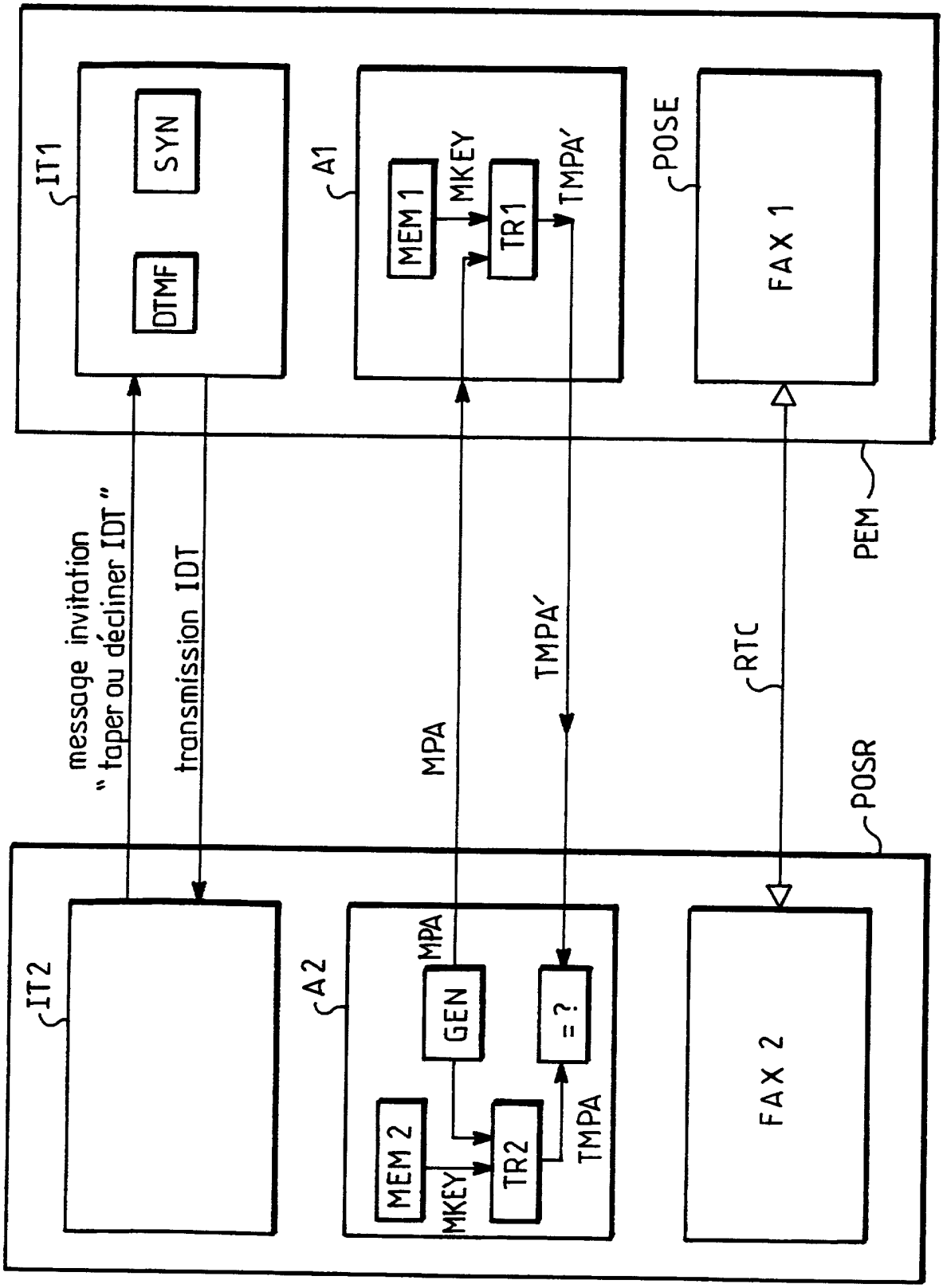
14. Installation selon la revendication 13, caractérisée en ce que les premiers moyens de stockage (MEM1) comprennent des moyens de contrôle d'accès sécurisé.

15. Installation selon la revendication 8, caractérisée en ce que les seconds moyens de traitement (TR2) comprennent:
- des seconds moyens de calcul du transformé du mot pseudo-aléatoire par la fonction cryptographique à l'aide de la clé émanant des seconds moyens de stockage, et
- des moyens de comparaison du transformé ainsi calculé avec le transformé reçu.

16. Installation selon la revendication 8, caractérisée en ce que dans les moyens de réception il est prévu d'associer à

l'identité de la personne émettrice un numéro annuaire correspondant à un poste du genre télécopieur sur lequel des compte rendus sont transmis en liaison avec la télétransmission dont l'identité de la personne émettrice est ainsi authentifiée.

FIG.1


IT1
SYN
DTMF
A1
MEM 1
MKEY
TR1
TMPA'
POSE
FAX 1
PEM
message invitation
" taper ou décliner IDT "
transmission IDT
MPA
TMPA'
RTC
POSR
IT2
A2
MPA
GEN
= ?
MEM 2
MKEY
TR2
TMPA
FAX 2

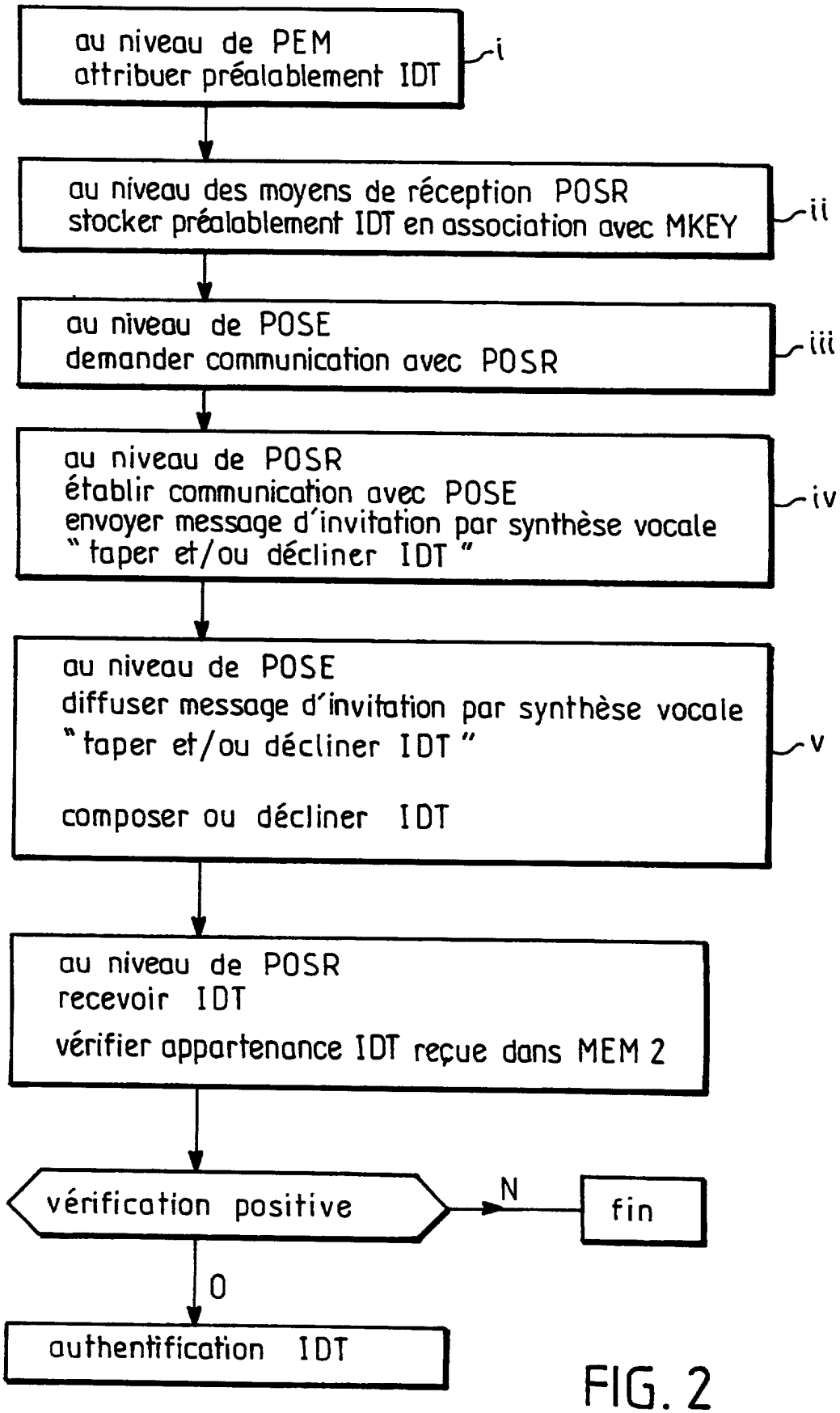

au niveau de PEM
attribuer préalablement IDT
i
au niveau des moyens de réception POSR
stocker préalablement IDT en association avec MKEY
ii
au niveau de POSE
demander communication avec POSR
iii
au niveau de POSR
établir communication avec POSE
envoyer message d'invitation par synthèse vocale
" taper et/ou décliner IDT "
iv
au niveau de POSE
diffuser message d'invitation par synthèse vocale
" taper et/ou décliner IDT "
composer ou décliner IDT
v
au niveau de POSR
recevoir IDT
vérifier appartenance IDT reçue dans MEM 2
vérification positive
N
fin
O
authentification IDT

FIG. 2

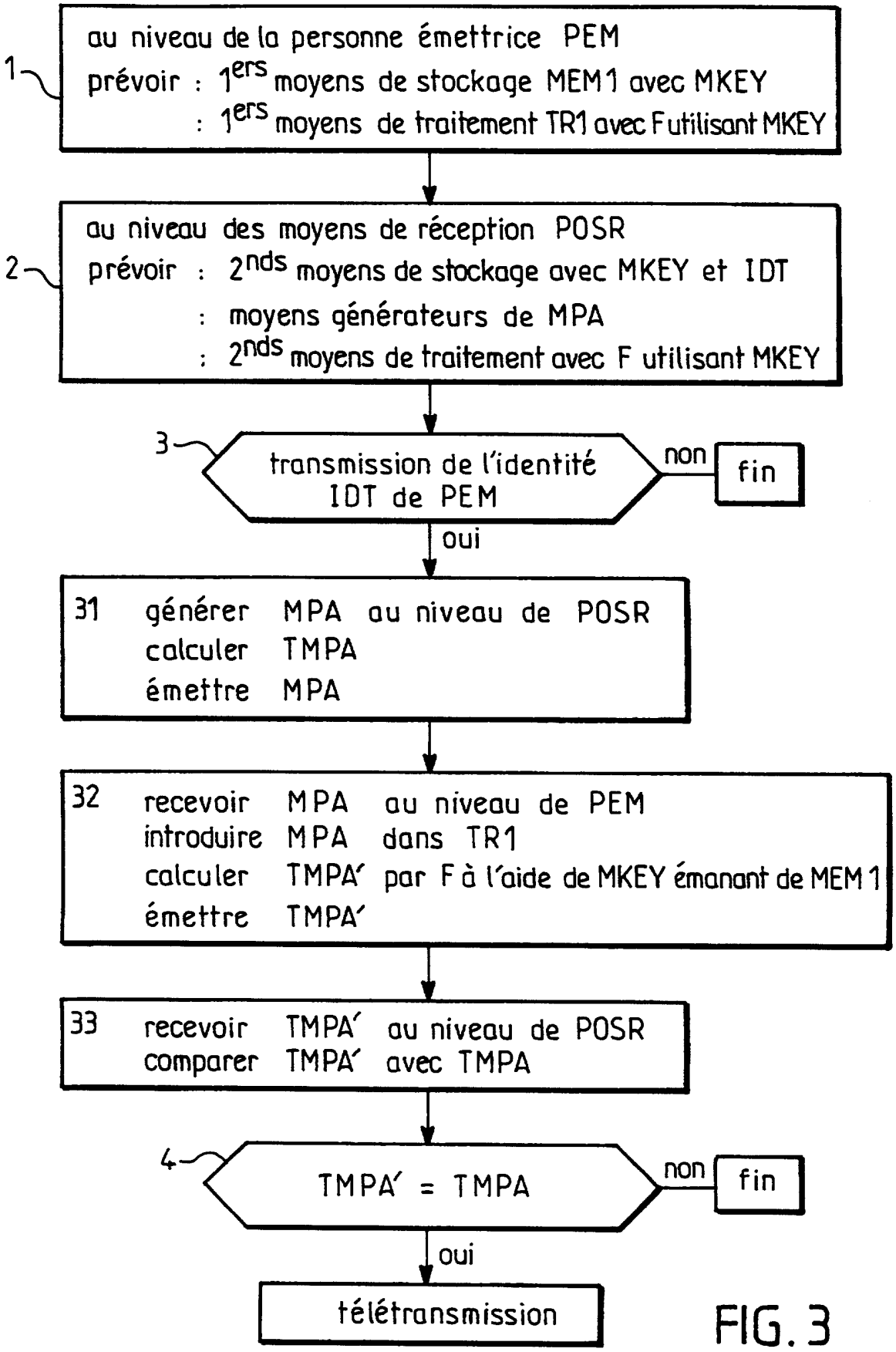

1
au niveau de la personne émettrice PEM
prévoir : 1ers moyens de stockage MEM1 avec MKEY
: 1ers moyens de traitement TR1 avec F utilisant MKEY
2
au niveau des moyens de réception POSR
prévoir : 2nds moyens de stockage avec MKEY et IDT
: moyens générateurs de MPA
: 2nds moyens de traitement avec F utilisant MKEY
3
transmission de l'identité IDT de PEM
non
fin
oui
31 générer MPA au niveau de POSR
calculer TMPA
émettre MPA
32 recevoir MPA au niveau de PEM
introduire MPA dans TR1
calculer TMPA' par F à l'aide de MKEY émanant de MEM1
émettre TMPA'
33 recevoir TMPA' au niveau de POSR
comparer TMPA' avec TMPA
4
TMPA' = TMPA
non
fin
oui
télétransmission

FIG. 3

RÉPUBLIQUE FRANÇAISE

2706716

INSTITUT NATIONAL
de la
PROPRIETE INDUSTRIELLE

RAPPORT DE RECHERCHE PRELIMINAIRE

établi sur la base des dernières revendications déposées avant le commencement de la recherche

N° d'enregistrement national

FA 488365
FR 9306942

DOCUMENTS CONSIDERES COMME PERTINENTS

Catégorie	Citation du document avec indication, en cas de besoin, des parties pertinentes	Revendications concernées de la demande examinée
A	EP-A-0 532 381 (GEMPLUS CARD INTERNATIONAL) 17 Mars 1993 * colonne 6, ligne 22 - colonne 7, ligne 1; figures 3,4 *	1-4,8-16
A	PATENT ABSTRACTS OF JAPAN vol. 13, no. 248 (E-770)9 Juin 1989 & JP-A-10 049 365 (OKI ELECTRIC IND CO LTD) 23 Février 1989 * abrégé *	1-4,8-16
A	THE TRANSACTIONS OF THE IECE vol. E73, no. 7 , Juillet 1990 , TOKYO pages 1111 - 1118 XP159226 MATSUMOTO, T. ET AL. 'A Prototype KPS and Its Application - IC Card Based Key Sharing and Cryptographic Communication' * abrégé, 1. Introduction * * figure 1 *	1,6-9,14

DOMAINES TECHNIQUES RECHERCHES (Int.Cl.5)

H04N

Date d'achèvement de la recherche: 3 Février 1994

Examinateur: Revellio, H.S.

CATEGORIE DES DOCUMENTS CITES

X : particulièrement pertinent à lui seul
Y : particulièrement pertinent en combinaison avec un autre document de la même catégorie
A : pertinent à l'encontre d'au moins une revendication ou arrière-plan technologique général
O : divulgation non-écrite
P : document intercalaire

T : théorie ou principe à la base de l'invention
E : document de brevet bénéficiant d'une date antérieure à la date de dépôt et qui n'a été publié qu'à cette date de dépôt ou qu'à une date postérieure.
D : cité dans la demande
L : cité pour d'autres raisons

& : membre de la même famille, document correspondant

EPO FORM 1503 03.82 (P04C13)