(12) DEMANDE INTERNATIONALE PUBLIÉE EN VERTU DU TRAITÉ DE COOPÉRATION EN MATIÈRE DE BREVETS (PCT)

(19) Organisation Mondiale de la Propriété Intellectuelle
Bureau international

(43) Date de la publication internationale
6 février 2003 (06.02.2003)

PCT

(10) Numéro de publication internationale
WO 03/010721 A2

(51) Classification internationale des brevets[7] : G07F

(21) Numéro de la demande internationale :
PCT/FR02/02658

(22) Date de dépôt international : 24 juillet 2002 (24.07.2002)

(25) Langue de dépôt : français

(26) Langue de publication : français

(30) Données relatives à la priorité :

0109903	25 juillet 2001 (25.07.2001)	FR
0109904	25 juillet 2001 (25.07.2001)	FR

(71) Déposant *(pour tous les États désignés sauf US)* : **CREDIT LYONNAIS** [FR/FR]; 18, rue de la République, F-69002 Lyon (FR).

(72) Inventeurs; et

(75) Inventeurs/Déposants *(pour US seulement)* : **ASSUERUS, Frédéric** [FR/FR]; River Side, 74, rue Camille Claudel, F-78955 Carrières sous Poissy (FR). **BERGSTEN, Ulrik** [FR/FR]; 17, rue Louis Maurice, F-94210 La Varenne (FR).

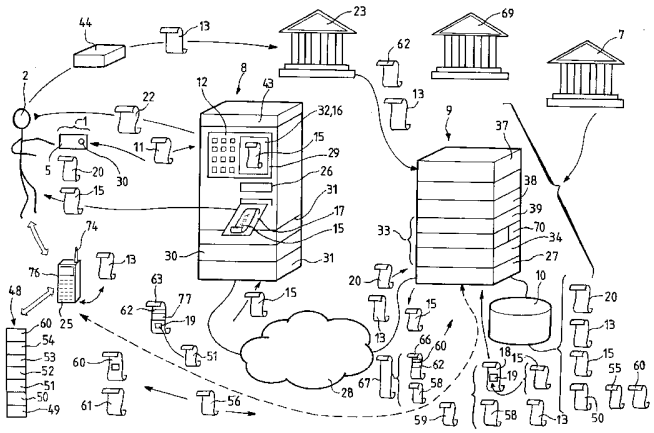
(74) Mandataire : **GRYNWALD, Albert**; Cabinet Grynwald, 127, rue du Faubourg Poissonnière, F-75009 Paris (FR).

(81) États désignés *(national)* : AE, AG, AL, AM, AT, AU, AZ, BA, BB, BG, BR, BY, BZ, CA, CH, CN, CO, CR, CU, CZ,

[Suite sur la page suivante]

(54) Title: METHOD AND SYSTEM FOR FORMAL GUARANTEE OF A PAYMENT, USING A PORTABLE TELEPHONE

(54) Titre : PROCEDE ET SYSTEME PERMETTANT DE GARANTIR FORMELLEMENT UN PAIEMENT, EN METTANT EN OEUVRE UN TELEPHONE PORTABLE



(57) Abstract: The invention concerns a method and a system enabling a user to perform remote payment settlement with a purchaser (23) payment for goods and/or services without risk of repudiation on the part of the user (2). The method comprises a step whereby the user (2) of goods and/or services transmits to a purchaser (23) supplying goods and/or services, the call number (13) of the mobile telephone (25) of the user (2); the step, whereby the user (2) transmits directly or indirectly, a password (15) to a banking institution (7). When the user (2) is registered, the password is transmitted by the banking institution (7) to the user (2), entirely or partly via a terminal (8), in particular an ATM/ABM automatic cash dispensing machine. The method further comprises a step, whereby the user (2) electronically signs the payment, by activating a private key, located in particular in the SIM card (48) of the mobile telephone (25) of the user (2). The user (2) thus remotely settle the payment for goods and/or services without the possibility of subsequent repudiation.

(57) Abrégé : L'invention concerne un procédé et un système permettant à un utilisateur (2) d'acquitter à distance auprès d'un acquéreur (23) le paiement de biens et/ou de services, sans risque de répudiation de la part de l'utilisateur (2). Le procédé comprend: l'étape, pour l'utilisateur (2) des biens et/ou services, de transmettre, à un acquéreur (23)

[Suite sur la page suivante]

WO 03/010721 A2

DE, DK, DM, DZ, EC, EE, ES, FI, GB, GD, GE, GH, GM, HR, HU, ID, IL, IN, IS, JP, KE, KG, KP, KR, KZ, LC, LK, LR, LS, LT, LU, LV, MA, MD, MG, MK, MN, MW, MX, MZ, NO, NZ, OM, PH, PL, PT, RO, RU, SD, SE, SG, SI, SK, SL, TJ, TM, TN, TR, TT, TZ, UA, UG, US, UZ, VN, YU, ZA, ZM, ZW.

(84) États désignés *(régional)* **:** brevet ARIPO (GH, GM, KE, LS, MW, MZ, SD, SL, SZ, TZ, UG, ZM, ZW), brevet eurasien (AM, AZ, BY, KG, KZ, MD, RU, TJ, TM), brevet européen (AT, BE, BG, CH, CY, CZ, DE, DK, EE, ES, FI, FR, GB, GR, IE, IT, LU, MC, NL, PT, SE, SK, TR), brevet OAPI (BF, BJ, CF, CG, CI, CM, GA, GN, GQ, GW, ML, MR, NE, SN, TD, TG).

Publiée :

— *sans rapport de recherche internationale, sera republiée dès réception de ce rapport*

En ce qui concerne les codes à deux lettres et autres abréviations, se référer aux "Notes explicatives relatives aux codes et abréviations" figurant au début de chaque numéro ordinaire de la Gazette du PCT.

fournissant les biens et/ou services, le numéro d'appel 13 du téléphone mobile (25) de l'utilisateur (2), l'étape, pour l'utilisateur (2), de transmettre, directement ou indirectement, un mot de passe (15) à un organisme bancaire (7). Lors d'une phase préalable d'enregistrement de l'utilisateur (2), le mot de passe (15) a été transmis, par l'organisme bancaire (7) à l'utilisateur (2), en tout ou partie via un terminal (8), notamment un distributeur automatique de billets de banque du type DAB/GAB.Le procédé comprend en outre: l'étape, pour l'utilisateur (2), de signer électroniquement le paiement, en activant une clé privée, notamment située dans la carte SIM (48) du téléphone mobile (25) de l'utilisateur (2). L'utilisateur (2) acquitte ainsi à distance le paiement des biens et/ou services sans possibilité de répudiation ultérieure.

PROCEDE ET SYSTEME PERMETTANT DE GARANTIR FORMELLEMENT UN PAIEMENT, EN METTANT EN ŒUVRE UN TELEPHONE PORTABLE

Domaine concerné, problème posé

La présente invention concerne un procédé et un système destiné à permettre à un utilisateur, disposant d'un objet portable et d'un terminal mobile ayant une fonction de téléphonie, d'effectuer un paiement à distance auprès d'un accepteur, sans risque de répudiation de la part de l'utilisateur.

Art antérieur

Solution

Procédé

L'invention concerne un procédé destiné à permettre à un utilisateur, disposant d'un objet portable et d'un terminal mobile ayant une fonction de téléphonie, d'effectuer un paiement à distance auprès d'un accepteur. L'objet portable se présente notamment sous la forme d'une carte bancaire. Le procédé comprend un mode avancé comportant trois phases :

- une phase d'enregistrement
- un processus de demande et de délivrance de certificat
- une phase de paiement.

On décrira ci-après chacune des trois phases :

(a) La phase d'enregistrement

Lors d'une phase d'enregistrement d'un utilisateur auprès d'un organisme, notamment un organisme bancaire le procédé comprend l'étape, pour l'utilisateur, d'accoupler l'objet portable à un terminal, notamment de type distributeur automatique de billets (DAB-GAB) ou de type terminal de paiement électronique (TPE).

le terminal est connecté de manière directe ou indirecte à un serveur associé à une base de données de l'organisme.

le procédé comprend en outre, lors de la phase d'enregistrement :

- l'étape, pour l'utilisateur, sur requête du terminal, d'entrer dans le terminal des données d'authentification de l'utilisateur, notamment un code confidentiel et/ou des données bio-métriques, associées à l'objet portable,

- l'étape, pour le terminal, de vérifier que les données d'authentification de l'utilisateur, correspondent à l'objet portable.

Il résulte de la combinaison des traits techniques que la phase d'enregistrement permet d'authentifier l'objet portable et de vérifier que l'utilisateur est bien le titulaire de l'objet portable.

le procédé comprend en outre :

- l'étape, pour le terminal, de lire dans l'objet portable et de transmettre au serveur des données d'identification, notamment le numéro et la date d'expiration de l'objet portable ainsi que le nom et le prénom du titulaire de l'objet portable,

- l'étape, pour l'utilisateur, sur requête du terminal, de composer, au moyen d'un clavier du terminal, le numéro d'appel associé au terminal mobile.

le numéro d'appel associé au terminal mobile est transmis, par le terminal, au serveur. le procédé comprend en

outre l'étape, pour le terminal, de transmettre un mot de passe à l'utilisateur, notamment en affichant le mot de passe sur un écran du terminal et/ou en délivrant à l'utilisateur un ticket sur lequel est imprimé le mot de passe. le mot de passe a été déterminé par le serveur et transmis au terminal. Il résulte de la combinaison des traits techniques que le mot de passe attribué par le serveur ne peut être transmis qu'à l'utilisateur titulaire de l'objet portable authentifié. le procédé comprend en outre, lors de la phase d'enregistrement, l'étape, pour le serveur, de mémoriser et d'associer dans la base de données de l'organisme les données d'identification, le numéro d'appel associé au terminal mobile, et le mot de passe.

Dans le cas de certaines variantes de réalisation la phase d'enregistrement peut être complétée par une étape au cours de laquelle l'utilisateur signe une demande d'enregistrement confirmant ainsi qu'il accepte des droits obligations du processus de paiement en toute confiance.

(b) Le processus de demande, de production et de délivrance d'un certificat

Le processus de demande, de production et de délivrance d'un certificat comporte une phase préalable

(b1) Phase préalable

Le terminal mobile doit comporter une carte SIM personnalisée par un opérateur de téléphonie mobile. la carte SIM est associée au numéro d'appel du terminal mobile.

On entend par carte SIM tout moyen ajouté au terminal mobile sous contrôle de l'opérateur de téléphonie mobile et qui sert à reconnaître l'utilisateur aussi bien pour la fonction de téléphonie que pour des fonctions mettant en œuvre une authentification et/ou un signature électronique vis-à-vis de différentes application au delà des fonctions de téléphonie.

la carte SIM contient :

- une clé privée de signature associée à une clé publique de signature,
- un mot de passe de signature.

le mot de passe de signature est soit un mot de passe de signature d'origine que l'opérateur de téléphonie a déterminé et transmis à l'utilisateur, soit un nouveau mot de passe de signature que l'utilisateur a substitué au mot de passe de signature d'origine.

La carte SIM comprend en outre :

- des fonctions cryptographiques,
- une application de demande de certificat comportant un mécanisme de signature mettant en œuvre la clé privée de signature,
- une application de paiement,

L'organisme dispose de la clé publique de signature.

L'organisme est par conséquent capable d'établir un lien entre le numéro d'appel et la clé publique de signature.

(b2) Phase de demande d'un certificat

Le procédé comprend en outre, pour permettre à l'utilisateur de demander et d'obtenir un certificat auprès de l'organisme considéré, l'étape, pour l'utilisateur, de transmettre une demande de certificat à cet organisme :

- en actionnant l'application de demande de certificat de la carte SIM,
- en saisissant sur le clavier du terminal mobile le mot de passe,
- en structurant, au moyen de l'application de demande de certificat, un message, notamment de type SMS, contenant le numéro d'appel et le mot de passe,
- en saisissant sur le clavier du terminal mobile un mot de passe de signature.

le mot de passe de signature ainsi saisi est comparé avec le mot de passe de signature de la carte SIM. le mot de passe de signature active le mécanisme de signature :

- pour produire une signature, et
- pour produire un message signé composé du message et de la signature ainsi produite, en mettant en œuvre la clé privée de signature, et

- pour transmettre le message signé à l'organisme considéré.

Le procédé comprend en outre, pour l'organisme considéré, les étapes suivantes :

- l'étape de vérifier que le numéro d'appel et le mot de passe ainsi transmis ont bien été mémorisés lors de la phase d'enregistrement et sont associés dans la base de données de l'organisme,

- l'étape d'extraire, de la base de données, les données d'identification, correspondant au numéro d'appel et au mot de passe, notamment le numéro et la date d'expiration de l'objet portable ainsi que le nom et le prénom du titulaire de l'objet portable,

- l'étape de rechercher la clé publique de signature associée audit numéro d'appel,

- l'étape de vérifier la signature au moyen de la clé publique de signature.

L'établissement du certificat est en principe demandé à une autorité de certification. Dans le cas de certaines variantes de réalisation l'autorité de certification peut avoir mandaté l'organisme considéré, notamment un organisme bancaire pour procéder à l'établissement et à la délivrance du certificat.

(b3) Phase de production et de délivrance du certificat

Le procédé comprend en outre :

- l'étape de fabriquer un certificat en utilisant notamment le numéro d'appel, tout ou partie des données d'identification et la clé publique de signature,

- l'étape de mémoriser et d'associer avec le numéro d'appel et le mot de passe, dans la base de données de l'organisme, le certificat et une référence de certificat dudit certificat,

- l'étape de transmettre audit terminal mobile, en réponse à la demande de certificat, la référence de certificat

et une requête d'activation de l'application de demande de certificat,

- l'étape, pour le terminal mobile, d'activer l'application de demande de certificat,

- l'étape, pour l'application de demande de certificat, de mémoriser la référence de certificat dans la carte SIM.

(c) La phase de paiement

Le procédé comprend en outre lors d'une phase de paiement :

- l'étape, pour l'utilisateur, de transmettre à l'accepteur le numéro d'appel associé au terminal mobile,

- l'étape, pour l'accepteur, de transmettre à l'organisme le numéro d'appel associé au terminal mobile ainsi que des informations relatives au paiement, dont le montant du paiement,

- l'étape, pour l'organisme d'adresser au terminal mobile de l'utilisateur un message de demande de paiement, notamment de type SMS, en utilisant le numéro d'appel associé au terminal mobile.

Le message comprend :

- les informations relatives au paiement,
- une requête d'activation de l'application de paiement.

Le procédé comprend en outre:

- l'étape, pour le terminal mobile, d'activer l'application de paiement,

- l'étape, pour l'application de paiement ainsi activée d'afficher les informations relatives au paiement ainsi que les références de certificat mémorisées dans la carte SIM,

- l'étape, pour l'utilisateur, de sélectionner, au moyen du clavier du terminal mobile, en cas de choix multiples, une référence de certificat à utiliser pour effectuer le paiement,

- l'étape, pour l'application de paiement, d'afficher un champ de saisie du mot de passe de signature,

- l'étape, pour l'utilisateur, de donner son accord concernant le paiement en saisissant le mot de passe de signature, dans le champ de saisie, au moyen du clavier du terminal mobile,

- l'étape, pour l'application de paiement, de contrôler le mot de passe de signature ainsi saisi en le comparant avec le mot de passe de signature de la carte SIM,

- l'étape, pour l'application de paiement :

• (i) de structurer un message de paiement, notamment de type SMS, contenant la référence de certificat et des données de paiement, au moins en partie constituées à partir des informations relatives au paiement, notamment le montant du paiement, la date du paiement, une référence de transaction, une identification de l'accepteur,

• (ii) de signer le message de paiement, en mettant en œuvre la clé privée de signature,

• (iii) de produire un message de paiement signé composé du message de paiement et de la signature ainsi obtenue, et

• (iv) de renvoyer à l'organisme le message de paiement signé ainsi produit.

Le procédé comprend en outre:

- l'étape, pour l'organisme, d'extraire de la base de données, le certificat et tout ou partie des données d'identification, notamment le numéro et la date d'expiration de l'objet portable, correspondant au numéro d'appel associé au terminal mobile et à la référence de certificat,

- l'étape, pour ledit organisme, de vérifier la signature du message de paiement signé en mettant en œuvre la clé publique de signature du certificat,

- l'étape, pour l'organisme, de vérifier que le certificat correspond à l'utilisateur a transmis audit accepteur le numéro d'appel associé au terminal mobile et de vérifier que

le message de paiement signé ainsi renvoyé correspond au message de demande de paiement,

- l'étape, pour l'organisme :

• de faire débiter ou débiter un compte bancaire associé à l'objet portable du montant du paiement et de faire créditer ou créditer l'accepteur du montant,

• de confirmer auprès de l'accepteur le paiement à distance de l'utilisateur.

Ainsi le paiement est acquitté à distance par l'utilisateur sans qu'il ait eu à communiquer à l'accepteur les données d'identification de l'objet portable, notamment le numéro et de la date d'expiration de la carte bancaire de l'utilisateur.

On obtient ainsi une signature électronique qualifiée avec un enchaînement de preuves successives : le paiement est signé par le certificat, la demande de certificat est signée par la carte SIM avec authentification du client par son mot de passe, et la demande d'enregistrement est signée par la puce de la carte bancaire du client. La (ou les) organismes, notamment les banques, gérant le mode avancé peuvent donc garantir formellement le paiement vis à vis du commerçant.

De préférence, le procédé selon l'invention comprend, outre le mode avancé, un mode de base et un processus de sélection automatique du mode approprié. La phase d'enregistrement du mode de base est identique à la phase d'enregistrement du mode avancé. le processus de sélection automatique comprend l'étape de déterminer si le paiement peut être effectué selon le mode avancé ou s'il doit être effectué selon le mode de base. la détermination peut être effectuée au cours de la phase de paiement (c) et/ou au cours du processus de demande et de délivrance de certificat (b). dans le cas où le paiement ne peut pas être effectué selon le mode avancé, les étapes du processus de demande de délivrance de certificat (b) et les étapes du processus de la phase de paiement (c) du mode

avancé sont substituées par les étapes ci-après décrites du mode de base, lors de la phase de paiement.

Le procédé comprend :

- l'étape, pour l'utilisateur, de transmettre à l'accepteur le numéro d'appel associé au terminal mobile.

- l'étape, pour l'accepteur, de transmettre à l'organisme le numéro d'appel associé au terminal mobile ainsi que des informations relatives au paiement, dont le montant du paiement,

- l'étape, pour l'organisme d'adresser à l'utilisateur un message, notamment de type SMS, en utilisant le numéro d'appel associé au terminal mobile.

le message comprend des informations relatives au paiement et une requête de saisie du mot de passe, se présentant notamment sous la forme d'un champ de saisie dans le message.

Le procédé comprend en outre :

- l'étape, pour l'utilisateur, de transmettre en retour le mot de passe à l'organisme, notamment en saisissant le mot de passe dans le champ de saisie,

- l'étape, pour l'organisme, de vérifier dans la base de données que le mot de passe, transmis par l'utilisateur, correspond au numéro d'appel associé au terminal mobile transmis par l'accepteur,

- l'étape, pour l'organisme :

• de rechercher, dans la base de données, tout ou partie des données d'identification, notamment le numéro et la date d'expiration de l'objet portable, correspondant au numéro d'appel associé au terminal mobile et au mot de passe,

• de faire débiter ou débiter un compte bancaire associé à l'objet portable du montant du paiement et de faire créditer ou créditer le accepteur du montant,

• de confirmer auprès de l'accepteur le paiement à distance de l'utilisateur.

Il résulte de la combinaison des traits techniques que le paiement est acquitté à distance par l'utilisateur sans qu'il

ait eu à communiquer à l'accepteur les données d'identification de l'objet portable, notamment le numéro et de la date d'expiration de la carte bancaire de l'utilisateur.

Dans le cas de certaines variantes de réalisation le procédé peut en outre comprendre l'étape de vérifier la validité de l'objet portable,

De préférence, selon l'invention le procédé est tel que pour déterminer si le paiement peut être effectué selon le mode avancé ou s'il doit être effectué selon le mode de base, l'organisme détecte qu'une clé publique de signature est associée au numéro d'appel. Il peut procéder à cette détection à partir d'une information provenant soit de l'opérateur de téléphonie soit du terminal mobile.

En fonction des résultats de cette détection et selon les options qu'il entend privilégier, l'organisme peut :

- soit inviter l'utilisateur à demander un certificat de manière à ce qu'il puisse accéder au mode avancé,
- soit accepter que l'utilisateur puisse continuer à effectuer des paiements à distance selon le mode de base.

De préférence, selon l'invention le procédé est tel que la détection intervient, au cours de ladite phase de paiement en mode de base, lors de la transmission par l'accepteur à l'organisme du numéro d'appel associé au terminal mobile.

De préférence, selon l'invention le procédé comprend en outre l'étape pour l'organisme de bloquer la mise en œuvre du mode de base dans le cas où l'organisme détecte qu'une clé publique de signature est associée au numéro d'appel. Il résulte de la combinaison des traits techniques que l'utilisateur n'a pas d'autre solution pour effectuer des paiements à distance que de demander un certificat selon le mode avancé.

De préférence, dans le cas cette variante de réalisation de l'invention le procédé comprend en outre l'étape, pour l'organisme, de contrôler qu'un utilisateur demandant un certificat n'utilise pas un mot de passe ayant déjà été utilisé

en paiement en mode de base en association avec le numéro d'appel de l'utilisateur.

Il résulte de la combinaison des traits techniques que les risques de compromission de mots de passe sont réduits. De plus le niveau de sécurité est ainsi optimisé en mode avancé.

Système

L'invention concerne un système destiné à permettre à un utilisateur, disposant d'un objet portable et d'un terminal mobile ayant une fonction de téléphonie, d'effectuer un paiement à distance auprès d'un accepteur. L'objet portable se présentant notamment sous la forme d'une carte bancaire. le système comprend un mode avancé comportant trois phases :

- une phase d'enregistrement
- un processus de demande et de délivrance de certificat
- une phase de paiement.

On décrira ci-après les moyens mis en œuvre lors de chacune des trois phases.

(a) La phase d'enregistrement

Le système comprend, pour permettre l'enregistrement de l'utilisateur auprès d'un organisme, notamment un organisme bancaire :

- un terminal, notamment un terminal de type distributeur automatique de billets (DAB-GAB) ou de type terminal de paiement électronique (TPE), comportant des moyens d'accouplements permettant à l'utilisateur, d'accoupler l'objet portable au terminal,
- un serveur associé à une base de données de l'organisme.

le serveur comprend des moyens de connexion pour connecter, de manière directe ou indirecte, le terminal au serveur via un réseau de communication, notamment informatique. le terminal comprend en outre :

- une interface utilisateur-terminal permettant à l'utilisateur d'entrer dans le terminal, sur requête du

terminal, des données d'authentification de l'utilisateur, notamment un code confidentiel et/ou des données bio-métriques, associées à l'objet portable,

- des moyens de vérification terminal pour vérifier que les données d'authentification de l'utilisateur, correspondent à l'objet portable.

Il résulte de la combinaison de ces traits techniques que la phase d'enregistrement permet d'authentifier l'objet portable et de vérifier que l'utilisateur est bien le titulaire de l'objet portable.

le terminal comprend en outre :

- des moyens de lecture terminal permettant de lire dans l'objet portable des données d'identification, notamment le numéro et la date d'expiration de l'objet portable ainsi que le nom et le prénom du titulaire de l'objet portable,

- des moyens de transmission terminal permettant de transmettre les données d'identification au serveur.

les moyens de lecture terminal et les moyens de transmission terminal sont mis en œuvre lors de la phase d'enregistrement de l'utilisateur. le terminal est tel que la interface utilisateur-terminal comporte un clavier permettant à l'utilisateur de composer, sur requête du terminal, le numéro d'appel associé au terminal mobile.

le terminal comporte :

- des moyens de transmission terminal pour transmettre au serveur le numéro d'appel associé au terminal mobile,

- des moyens de communication terminal pour communiquer un mot de passe à l'utilisateur, notamment en affichant le mot de passe sur un écran du terminal ou en délivrant à l'utilisateur un ticket sur lequel est imprimé le mot de passe.

le mot de passe a été déterminé par le serveur en mettant en œuvre des moyens de traitement informatique serveur. le mot de passe a été transmis par le serveur au terminal, via le réseau de communication. Il résulte de la combinaison des

traits techniques que le mot de passe attribué par le serveur ne peut être transmis qu'à l'utilisateur titulaire de l'objet portable authentifié. les moyens de traitement informatique serveur comportent des moyens d'enregistrement pour mémoriser et associer dans la base de données : les données d'identification, le numéro d'appel associé au terminal mobile, et le mot de passe.

(b) Le processus de demande, de production et de délivrance de certificat.

Le processus de demande, de production et de délivrance de certificat comporte une phase préalable.

(b1) Phase préalable.

Le terminal mobile doit comporter une carte SIM personnalisée par un opérateur de téléphonie mobile. la carte SIM est associée au numéro d'appel du terminal mobile. la carte SIM doit contenir une clé privée de signature associée à une clé publique de signature et un mot de passe de signature. le mot de passe de signature est soit un mot de passe de signature d'origine que l'opérateur de téléphonie a déterminé et transmis à l'utilisateur, soit un nouveau mot de passe de signature que l'utilisateur a substitué au mot de passe de signature d'origine. la carte SIM comprend en outre :

- des fonctions cryptographiques,
- une application de demande de certificat comporte un mécanisme de signature mettant en œuvre la clé privée de signature,
- une application de paiement.

l'organisme dispose de la clé publique de signature.

Il résulte de la combinaison des traits techniques que l'organisme est capable d'établir un lien entre le numéro d'appel et la clé publique de signature.

(b2) Processus de demande.

Le système comprend en outre des moyens de demande et de délivrance de certificat susceptibles d'être mis en œuvre par l'utilisateur et l'organisme pour demander et obtenir un

certificat auprès de l'organisme. les moyens de demande et de délivrance de certificat sont composés de moyens de transmission terminal mobile pour transmettre une demande de certificat à l'organisme :

- en actionnant l'application de demande de certificat de la carte SIM,
- en saisissant sur le clavier du terminal mobile le mot de passe,
- en structurant, au moyen de l'application de demande de certificat, un message, notamment de type SMS, contenant le numéro d'appel et le mot de passe,
- en saisissant sur le clavier du terminal mobil'un mot de passe de signature. le mot de passe de signature ainsi saisi est comparé avec le mot de passe de signature de la carte SIM.

le mot de passe de signature active le mécanisme de signature :

- pour signer ledit message et produire une signature, et
- pour produire un message signé composé dudit message et de la signature ainsi produite, en mettant en œuvre ladite clé privée de signature, et
- pour transmettre ledit message signé audit organisme.

(b3) processus de vérification ;

Les moyens de demande et de délivrance de certificat sont en outre composés :

- des moyens de vérification serveur, mis en œuvre par l'organisme, pour vérifier que le numéro d'appel et le mot de passe ainsi transmis ont bien été mémorisés lors de la phase d'enregistrement et sont associés dans la base de données de l'organisme,
- des moyens de traitement informatique serveur mis en œuvre par l'organisme et agencés pour extraire, de la base de données, les données d'identification correspondant au numéro

d'appel et au mot de passe, notamment le numéro et la date d'expiration dudit objet portable ainsi que le nom et le prénom du titulaire dudit objet portable,

- des moyens de traitement informatique serveur mis en œuvre par ledit organisme et agencés pour rechercher la clé publique de signature associée au numéro d'appel,

- des moyens de traitement informatique serveur mis en œuvre par l'organisme et agencés pour vérifier la signature au moyen de la clé publique de signature.

(b4) Processus de production ;

Les moyens de demande, de production et de délivrance de certificat sont en outre composés :

- des moyens de production serveur pour fabriquer un certificat en utilisant notamment le numéro d'appel, tout ou partie des données d'identification et la clé publique de signature,

- des moyens de traitement informatique serveur mis en œuvre par l'organisme et agencés pour mémoriser et associer avec le numéro d'appel et le mot de passe, dans la base de données de l'organisme, le certificat et une référence de certificat dudit certificat,

- desdits moyens de transmission serveur mis en œuvre par l'organisme et agencés pour transmettre au terminal mobile, en réponse à la demande de certificat, la référence de certificat et une requête d'activation de l'application de demande de certificat,

- du terminal mobile agencé pour activer l'application de demande de certificat,

- de l'application de demande de certificat agencée pour mémoriser la référence de certificat dans la carte SIM.

(c) La phase de paiement ;

Le système comprend en outre des moyens de transmission accepteur permettant audit utilisateur de transmettre audit accepteur ledit numéro d'appel associé audit terminal mobile.

Le serveur dudit organisme comprend en outre :

- des moyens de réception serveur pour recevoir de l'accepteur le numéro d'appel associé au terminal mobile ainsi que des informations relatives au paiement, dont le montant du paiement,

- des moyens de transmission serveur pour adresser au terminal mobile de l'utilisateur un message de demande de paiement, notamment de type SMS, en utilisant le numéro d'appel associé au terminal mobile.

Le message de demande de paiement comprend des informations relatives au paiement et une requête d'activation de l'application de paiement. Le terminal mobile est agencé pour d'activer l'application de paiement. L'application de paiement ainsi activée est agencée pour afficher les informations relatives au paiement ainsi que les références de certificat mémorisées dans la carte SIM.

Le terminal mobile est agencé pour que l'utilisateur puisse sélectionner, au moyen du clavier du terminal mobile, en cas de choix multiples, une référence de certificat à utiliser pour effectuer le paiement.

L'application de paiement est agencée pour afficher un champ de saisie du mot de passe de signature de sorte que l'utilisateur peut donner son accord concernant le paiement en saisissant le mot de passe de signature, dans ledit champ de saisie, au moyen dudit clavier du terminal mobile.

L'application de paiement est agencée pour contrôler le mot de passe de signature ainsi saisi en le comparant avec le mot de passe de signature de la carte SIM.

L'application de paiement est agencée pour :

- (i) structurer un message de paiement, notamment de type SMS, contenant la référence de certificat et des données de paiement, au moins en partie constituées à partir des informations relatives au paiement, notamment le montant du paiement, la date du paiement, une référence de transaction, une identification de l'accepteur,

• (ii) produire une signature en mettant en œuvre la clé privée de signature,

• (iii) produire un message de paiement signé composé du message de paiement et de la signature ainsi obtenue, et

• (iv) renvoyer au serveur de l'organisme, via les moyens de transmission terminal mobile, le message de paiement signé ainsi produit.

Les moyens traitement informatique serveur dudit organisme sont agencés pour extraire de la base de données, le certificat et tout ou partie des données d'identification, notamment le numéro et la date d'expiration de l'objet portable, correspondant au numéro d'appel associé au terminal mobile et à la référence de certificat.

Les moyens traitement informatique serveur dudit organisme sont agencés pour vérifier la signature du message de paiement signé en mettant en œuvre la clé publique de signature du certificat.

Les moyens de traitement informatique serveur de l'organisme sont agencés pour vérifier que le certificat correspond à l'utilisateur ayant transmis à l'accepteur le numéro d'appel associé au terminal mobile et pour vérifier que le message de paiement signé ainsi renvoyé correspond au message de demande de paiement.

Les moyens de traitement informatique serveur dudit organisme sont agencés pour :

• faire débiter ou débiter un compte bancaire associé à l'objet portable du montant du paiement et faire créditer ou créditer l'accepteur du montant,

• confirmer auprès de l'accepteur le paiement à distance de l'utilisateur.

Ainsi, le paiement est acquitté à distance par l'utilisateur sans qu'il ait eu à communiquer à l'accepteur les données d'identification de l'objet portable, notamment le numéro et la date d'expiration de la carte bancaire de l'utilisateur.

De préférence, selon l'invention le système comprend, outre le mode avancé, un mode de base et un processus de sélection automatique du mode approprié. les moyens mis en œuvre lors de la phase d'enregistrement du mode de base sont identiques aux moyens mis en œuvre lors de la phase d'enregistrement du mode avancé. les moyens de traitement informatique serveur sont agencés pour déterminer si le paiement peut être effectué selon le mode avancé ou s'il doit être effectué selon le mode de base. la détermination peut être effectuée au cours de la phase de paiement (c) et/ou au cours du processus de demande et de délivrance de certificat (b). dans le cas où le paiement ne peut pas être effectué selon le mode avancé, les moyens mis en œuvre lors du processus de demande de délivrance de certificat (b) et lors du processus de la phase de paiement (c) du mode avancé sont substitués par les moyens ci-après spécifiés plus particulièrement agencés au paiement en mode de base.

le système comprend en outre des moyens de transmission accepteur permettant à l'utilisateur de transmettre à l'accepteur le numéro d'appel associé au terminal mobile. les moyens de réception serveur du serveur de l'organisme sont agencés pour recevoir de l'accepteur le numéro d'appel associé au terminal mobile ainsi que des informations relatives au paiement, dont le montant du paiement. les moyens de réception serveur du serveur de l'organisme sont agencés pour adresser à l'utilisateur un message, notamment de type SMS, en utilisant le numéro d'appel associé au terminal mobile. le message comprend les informations relatives au paiement et une requête de saisie du mot de passe, se présentant notamment sous la forme d'un champ de saisie dans le message. les moyens de transmission terminal mobile sont agencés pour permettre à l'utilisateur de transmettre en retour le mot de passe au serveur de l'organisme, notamment en saisissant le mot de passe dans le champ de saisie. les moyens de traitement informatique serveur sont agencés pour vérifier dans la base de données que le mot de passe, transmis

par l'utilisateur, correspond au numéro d'appel associé au terminal mobile transmis par l'accepteur. les moyens de traitement informatique serveur sont agencés pour rechercher dans la base de données, tout ou partie des données d'identification, notamment le numéro et la date d'expiration de l'objet portable, correspondant au numéro d'appel associé au terminal mobile et au mot de passe. les moyens de traitement informatique serveur sont agencés pour faire débiter ou débiter un compte bancaire associé à l'objet portable du montant du paiement et faire créditer ou créditer l'accepteur du montant. les moyens de traitement informatique serveur sont agencés pour confirmer auprès de l'accepteur le paiement à distance de l'utilisateur. Il résulte de la combinaison des traits techniques que le paiement est acquitté à distance par l'utilisateur sans qu'il ait eu à communiquer à l'accepteur les données d'identification de l'objet portable, notamment le numéro et la date d'expiration de la carte bancaire de l'utilisateur.

De préférence, selon l'invention le système est tel que pour déterminer si le paiement peut être effectué selon le mode avancé ou s'il doit être effectué selon le mode de base, les moyens de traitement informatique serveur de l'organisme détectent si une clé publique de signature est associée au numéro d'appel soit que cette information provienne de l'opérateur de téléphonie soit qu'elle provienne du terminal mobile. Il résulte de la combinaison des traits techniques que l'organisme peut, selon les options qu'il entend privilégier :

- soit inviter l'utilisateur à demander un certificat de manière qu'il puisse accéder au mode avancé,
- soit accepter que l'utilisateur puisse continuer à effectuer des paiements à distance selon le mode de base.

De préférence, selon l'invention le système est tel que la détection par les moyens de traitement informatique serveur intervient, au cours de ladite phase de paiement en mode

de base, lors de la transmission par l'accepteur à l'organisme du numéro d'appel associé au terminal mobile.

De préférence, selon l'invention, les moyens de traitement informatique serveur comprennent en outre des moyens de verrouillage pour bloquer la mise en œuvre du mode de base dans le cas où l'organisme détecte qu'une clé publique de signature est associée au numéro d'appel. Il résulte de la combinaison des traits techniques que l'utilisateur n'a pas d'autre solution pour effectuer des paiements à distance que de demander un certificat selon le mode avancé.

De préférence, selon l'invention, les moyens de traitement informatique serveur comprennent en outre des moyens de contrôle pour contrôler qu'un utilisateur demandant un certificat n'utilise pas un mot de passe ayant déjà été utilisé en paiement en mode de base en association avec le numéro d'appel de l'utilisateur. Il résulte de la combinaison des traits techniques que les risques de compromission de mots de passe sont réduits. Le niveau de sécurité est ainsi optimisé en mode avancé.

Description détaillée

D'autres caractéristiques et avantages de l'invention apparaîtront à la lecture de la description de variante de réalisation de l'invention données à titre d'exemple indicatif et non limitatif, et de la

- figure 1 qui représente, de manière schématique, les moyens techniques mis en œuvre lors de la phase d'enregistrement (mode avancé ou mode de base),

- figure 2 qui représente, de manière schématique, les moyens techniques mis en œuvre lors du processus de demande et de délivrance d'un certificat (mode avancé),

- figure 3 qui représente, de manière schématique, les moyens techniques mis en œuvre lors de la phase de paiement (mode avancé),

- figure 4 qui représente, de manière schématique, les moyens techniques mis en œuvre lors de la phase de paiement (mode de base).

On va maintenant décrire, en se référant aux figures 1 à 4, une variante de réalisation d'un système permettant d'effectuer un paiement à distance auprès d'un accepteur 23. A cet effet, l'utilisateur 2 dispose d'un objet portable 1 et d'un terminal mobile 25 ayant une fonction de téléphonie. l'objet portable 1 se présente notamment sous la forme d'une carte bancaire 5.

le système opère selon deux modes un mode de base et un mode avancé.

Le mode avancé

On décrira en premier lieu le mode avancé en se référant aux figures 1 à 3 puis enduite le mode de base en se référant aux figures 1 et 4.

Le mode avancé comporte trois phases :

- une phase d'enregistrement
- un processus de demande et de délivrance de certificat,
- une phase de paiement.

(a) La phase d'enregistrement.

On va décrire les moyens techniques mis en œuvre lors de la phase d'enregistrement en se référant à la figure 1.

Le système comprend, pour permettre l'enregistrement de l'utilisateur 2 auprès d'un organisme 7, notamment un organisme bancaire, un terminal 8, notamment un terminal de type distributeur automatique de billets (DAB-GAB) ou de type terminal de paiement électronique (TPE). Le terminal 8 comporte des moyens d'accouplements 26 permettant à l'utilisateur 2, d'accoupler l'objet portable 1 au terminal 8. Le système comprend en outre un serveur 9 associé à une base de données 10 de l'organisme 7. le serveur 9 comprend des moyens de connexion 27 pour connecter, de manière directe ou indirecte, le terminal

8 au serveur 9 via un réseau de communication 28, notamment informatique.

le terminal 8 comprend en outre :

- une interface utilisateur-terminal 29 permettant à l'utilisateur 2 d'entrer dans le terminal 8, sur requête du terminal 8, des données d'authentification 11 de l'utilisateur 2, notamment un code confidentiel et/ou des données biométriques, associées à l'objet portable 1.

- des moyens de vérification terminal 30 pour vérifier que les données d'authentification 11 de l'utilisateur 2, correspondent à l'objet portable 1.

Il résulte de la combinaison des traits techniques ci-dessus décrits que la phase d'enregistrement permet d'authentifier l'objet portable 1 et de vérifier que l'utilisateur 2 est bien le titulaire de l'objet portable 1.

le terminal 8 comprend en outre :

- des moyens de lecture terminal 43 permettant de lire dans l'objet portable 1 des données d'identification 20, notamment le numéro et la date d'expiration de l'objet portable 1 ainsi que le nom et le prénom du titulaire de l'objet portable 1,

- des moyens de transmission terminal 31 permettant de transmettre les données d'identification 20 au serveur 9.

les moyens de lecture terminal 43 et les moyens de transmission terminal 31 sont mis en œuvre lors de la phase d'enregistrement de l'utilisateur 2. le terminal 8 est tel que l'interface utilisateur-terminal 29 comporte un clavier 12 permettant à l'utilisateur 2 de composer, sur requête du terminal 8, le numéro d'appel 13 associé au terminal mobile 25.

le terminal 8 comporte en outre :

- des moyens de transmission terminal 31 pour transmettre au serveur 9 le numéro d'appel 13 associé au terminal mobile 25,

- des moyens de communication terminal 32 pour communiquer un mot de passe 15 à l'utilisateur 2, notamment en

affichant le mot de passe 15 sur un écran 16 du terminal 8 ou en délivrant à l'utilisateur 2 un ticket 17 sur lequel est imprimé le mot de passe 15.

le mot de passe 15 est déterminé par le serveur 9 en mettant en œuvre des moyens de traitement informatique serveur 33. le mot de passe 15 est été transmis par le serveur 9 au terminal 8, via le réseau de communication 28.

Il résulte de la combinaison des traits techniques que le mot de passe 15 attribué par le serveur 9 ne peut être transmis qu'à l'utilisateur 2 titulaire de l'objet portable 1 authentifié.

les moyens de traitement informatique serveur 33 comportent des moyens d'enregistrement 34 pour mémoriser et associer dans la base de données 10 :

- les données d'identification 20,
- le numéro d'appel 13 associé au terminal mobile 25,
- le mot de passe 15.

(b) Le processus de demande et de délivrance de certificat.

On va maintenant décrire les moyens techniques mis en œuvre lors du processus de demande et de délivrance de certificat 55 en se référant à la figure 2.

(b1) Phase préalable.

Le système comprend des moyens de demande et de délivrance de certificat 55. Ces moyens sont susceptibles d'être mis en œuvre par l'utilisateur 2 et l'organisme 7 dans le cas où le terminal mobile 25 comporte une carte SIM 48 personnalisée par un opérateur de téléphonie 69 mobile.

La carte SIM 48 est associée au numéro d'appel 13 du terminal mobile 25. la carte SIM 48 contient une clé privée de signature 49 associée à une clé publique de signature 50 et un mot de passe de signature 51. le mot de passe de signature 51 est soit un mot de passe de signature 51 d'origine que l'opérateur de téléphonie 69 a déterminé et transmis à l'utilisateur 2, soit un nouveau mot de passe de signature 51

que l'utilisateur 2 a substitué au mot de passe de signature 51 d'origine. la carte SIM 48 comprend en outre :

- des fonctions cryptographiques,
- une application de demande de certificat 52 comportant un mécanisme de signature 53 mettant en œuvre la clé privée de signature 49,
- une application de paiement 54.

l'organisme 7 dispose de la clé publique de signature 50.

Il résulte de la combinaison des traits techniques que l'organisme 7 est capable d'établir un lien entre le numéro d'appel 13 et la clé publique de signature 50.

(b2) Processus de demande de certificat 55

Les moyens 55, pour demander et obtenir la délivrance d'un certificat 55 auprès de l'organisme 7, sont composés de moyens de transmission terminal mobile 74, mis en œuvre par l'utilisateur 2, pour transmettre une demande de certificat 56 à l'organisme 7. La demande de certificat 56 est obtenue :

- en actionnant l'application de demande de certificat 52 de la carte SIM 48,
- en saisissant sur le clavier terminal mobile 76 le mot de passe 15,
- en structurant, au moyen de l'application de demande de certificat 52, un message 18, notamment de type SMS, contenant le numéro d'appel 13 et le mot de passe 15,
- en saisissant sur le clavier terminal mobile 76 un mot de passe signature 51.

le mot de passe de signature 51 ainsi saisi par l'utilisateur 2 est comparé avec le mot de passe de signature 51 de la carte SIM 48. le mot de passe de signature 51 active le mécanisme de signature 53 qui a pour effet :

- de signer le message 18, et
- de produire un message signé 59 composé du message 18 et de la signature 58 ainsi obtenue, en mettant en œuvre la clé privée de signature 49, et

- de transmettre le message signé 59 à l'organisme 7.

(b3) Processus de vérification.

Les moyens 55, pour demander et obtenir un certificat 55 auprès de l'organisme 7, comprennent en outre:

- des moyens de vérification serveur 39, mis en œuvre par l'organisme 7, pour vérifier que le numéro d'appel 13 et le mot de passe 15 ainsi transmis ont bien été mémorisés lors de la phase d'enregistrement et sont associés dans la base de données 10 de l'organisme 7,

- des moyens de traitement informatique serveur 33 mis en œuvre par l'organisme 7 et agencés pour extraire, de la base de données 10, les données d'identification 20, correspondant au numéro d'appel 13 et au mot de passe 15, notamment le numéro et la date d'expiration de l'objet portable 1 ainsi que le nom et le prénom du titulaire de l'objet portable 1,

- des moyens de traitement informatique serveur 33 mis en œuvre par l'organisme 7 et agencés pour rechercher la clé publique de signature 50 associée au numéro d'appel 13,

- des moyens de traitement informatique serveur 33 mis en œuvre par l'organisme 7 et agencés pour vérifier la signature 58 au moyen de la clé publique de signature 50.

(b4) Processus de production du certificat 55.

les moyens 55, pour demander et obtenir un certificat 55 auprès de l'organisme 7, comprennent en outre :

- de moyens de production serveur 70 pour fabriquer un certificat 55 en utilisant notamment le numéro d'appel 13, tout ou partie des données d'identification 20 et la clé publique de signature 50,

- des moyens de traitement informatique serveur 33 mis en œuvre par l'organisme 7 et agencés pour mémoriser et associer avec le numéro d'appel 13 et le mot de passe 15, dans la base de données 10 de l'organisme 7, le certificat 55 et une référence de certificat 60 du certificat 55,

- des moyens de transmission serveur 38 mis en œuvre par l'organisme 7 et agencés et agencés pour transmettre au

terminal mobile 25, en réponse à la demande de certificat 56, la référence de certificat 60 et une requête d'activation 61 de l'application de demande de certificat 52.

Le terminal mobile 25 est agencé pour activer l'application de demande de certificat 52 lorsqu'il reçoit la requête d'activation 61. L'application de demande de certificat 52 est agencée pour mémoriser la référence de certificat 60 dans la carte SIM 48.

(c) La phase de paiement.

On va maintenant décrire les moyens techniques mis en œuvre lors de la phase de paiement en se référant à la figure 3.

le système comprend des moyens de transmission accepteur 44 permettant à l'utilisateur 2, de transmettre à l'accepteur 23 le numéro d'appel 13 associé au terminal mobile 25.

le serveur 9 de l'organisme 7 comprend en outre :

- des moyens de réception serveur 37 pour recevoir de l'accepteur 23 le numéro d'appel 13 associé au terminal mobile 25 ainsi que des informations relatives au paiement 62, dont le montant du paiement,
- des moyens de transmission serveur 38 pour adresser au terminal mobile 25 de l'utilisateur 2 un message de demande de paiement 63, notamment de type SMS, en utilisant le numéro d'appel 13 associé au terminal mobile 25.

le message de demande de paiement 63 comprend les informations relatives au paiement 62 et une requête d'activation de l'application de paiement 77. le terminal mobile 25 est agencé pour d'activer l'application de paiement 54 lorsqu'il reçoit la requête d'activation de l'application de paiement 77. L'application de paiement 54 ainsi activée est agencée pour afficher les informations relatives au paiement 62 ainsi que les références de certificat 60 mémorisées dans la carte SIM 48. le terminal mobile 25 est agencé pour que l'utilisateur 2 puisse sélectionner, au moyen du clavier terminal mobile 76, en cas de choix multiples, une référence de

certificat 60 à utiliser pour effectuer le paiement. L'application de paiement 54 est agencée pour afficher un champ de saisie 19 du mot de passe de signature 51 de sorte que l'utilisateur 2 puisse donner son accord concernant le paiement en saisissant le mot de passe de signature 51, dans le champ de saisie 19, au moyen du clavier terminal mobile 76. L'application de paiement 54 est agencée pour contrôler le mot de passe de signature 51 ainsi saisi en le comparant avec le mot de passe de signature 51 de la carte SIM 48.

L'application de paiement 54 est agencée pour :

- (i) structurer un message de paiement 66, notamment de type SMS, contenant la référence de certificat 60 et des données de paiement, au moins en partie constituées à partir des informations relatives au paiement 62, notamment le montant du paiement, la date du paiement, une référence de transaction, une identification de l'accepteur 23,
- (ii) produire une signature 58 en mettant en œuvre la clé privée de signature 49,
- (iii) produire un message de paiement signé 67 composé du message de paiement 66 et de la signature 58 ainsi obtenue, et
- (iv) renvoyer au serveur 9 de l'organisme 7, via les moyens de transmission terminal mobile 74, le message de paiement signé 67 ainsi produit.

les moyens de traitement informatique serveur 33 de l'organisme 7 sont agencés pour extraire de la base de données 10 :

(i) le certificat 55, et

(ii) tout ou partie des données d'identification 20, notamment le numéro et la date d'expiration de l'objet portable 1, correspondant au numéro d'appel 13 associé au terminal mobile 25 et à la référence de certificat 60.

les moyens de traitement informatique serveur 33 de l'organisme 7 sont agencés pour vérifier la signature 58 du message de paiement signé 67 en mettant en œuvre la clé publique

de signature 50 du certificat 55. Les moyens de traitement informatique serveur 33 de l'organisme 7 sont également agencés pour vérifier que le certificat 55 correspond à l'utilisateur 2 ayant transmis à l'accepteur 23 le numéro d'appel 13 associé au terminal mobile 25 et pour vérifier que le message de paiement signé 67 ainsi renvoyé correspond au message de demande de paiement 63. les moyens de traitement informatique serveur 33 de l'organisme 7 sont également agencés pour :

- faire débiter ou débiter un compte bancaire associé à l'objet portable 1 du montant du paiement et de faire créditer ou créditer l'accepteur 23 du montant,
- confirmer auprès de l'accepteur 23 le paiement à distance de l'utilisateur 2.

Il serait préférable, avant de confirmer auprès de l'accepteur le paiement à distance de l'utilisateur, de vérifier la validité de l'objet portable et du certificat.

Il résulte de la combinaison des traits techniques que le paiement est acquitté à distance par l'utilisateur 2 sans qu'il ait eu à communiquer à l'accepteur 23 les données d'identification 20 de l'objet portable 1, notamment le numéro et la date d'expiration de la carte bancaire 5 de l'utilisateur 2.

On constate que le paiement ainsi acquitté à distance est non-répudiable. Tout se passe comme si l'utilisateur 2 titulaire et porteur de la carte bancaire 5 a signé de façon manuscrite un ticket de paiement par carte bancaire. Sa responsabilité est engagée même si au niveau interbancaire on n'a pas ou plus les moyens de vérifier la validité de telles facturettes papier.

En effet, on dispose d'une signature électronique susceptible d'être qualifiée avec un enchaînement de preuves successives :

- le paiement est signé en référence au certificat 55,

- la demande de certificat 56 est signée par la carte SIM avec authentification du porteur par son mot de passe de signature 51,

- la demande d'enregistrement au système de paiement selon l'invention est validée par la puce de la carte bancaire du porteur et par une première utilisation du mot de passe fourni.

Sur ces bases, la banque de l'accepteur jouant le rôle de l'organisme ou s'appuyant sur celui-ci doit pouvoir garantir formellement le paiement vis à vis de l'accepteur.

On constate enfin qu'il n'est pas utile de gérer la révocation de tels certificats et donc qu'il n'est pas nécessaire de mettre en place un service de validation car :

- si la carte bancaire est perdue ou volée : la mise en opposition de la carte bancaire 5 empêche l'utilisation du certificat 55 puisque, lors des opérations de vérification par l'organisme 7 que le certificat 55 correspond à l'utilisateur concerné, il apparaîtra que sa carte bancaire 5 a été mise en opposition,

- si la carte SIM 48 est perdue ou volée : la mise en opposition de la carte SIM bloque toute possibilité de communication et donc toute possibilité d'utilisation du certificat 55 présent dans la carte SIM.

Le système peut également opérer selon un autre appelé mode de base qui sera ci-après décrit en se référant aux figures 1 et 4. Ce mode de base comporte une phase d'enregistrement et une phase de paiement.

Les moyens mis en œuvre lors de la phase d'enregistrement du mode de base sont identiques aux moyens mis en œuvre lors de la phase d'enregistrement du mode avancé. Ils ont été décrits en se référant à la figure 1.

Un processus de sélection automatique approprié permet de sélectionner le mode selon lequel le paiement à distance sera effectué (mode avancé en principe ou mode de base à défaut).

Les moyens de traitement informatique serveur 33 sont agencés pour déterminer si le paiement peut être effectué selon le mode avancé ou s'il doit être effectué selon le mode de base. Cette détermination peut être effectuée au cours de la phase de paiement (c) et/ou au cours du processus (b) de demande et de délivrance de certificat 55.

Selon une variante de réalisation préférentielle de l'invention pour déterminer si le paiement peut être effectué selon le mode avancé ou s'il doit être effectué selon le mode de base, les moyens de traitement informatique serveur 33 de l'organisme 7 détectent, au cours de la phase de paiement en mode de base, si une clé publique de signature 50 est associée au numéro d'appel 13 soit que cette information provienne de l'opérateur de téléphonie 69 soit qu'elle provienne du terminal mobile 25. L'organisme 7 peut alors, selon les options qu'il entend privilégier :

soit inviter l'utilisateur 2 à demander un certificat 55 de manière à ce qu'il puisse accéder au mode avancé,

soit accepter que l'utilisateur 2 puisse continuer à effectuer des paiements à distance selon le mode de base.

Il est toujours souhaitable de sélectionner, parmi les modes possibles, le plus sécurisé. L'objectif à terme est de généraliser le mode le plus sécurisé, c'est à dire le mode avancé. Si on est obligé momentanément d'admettre un mode de base c'est qu'il serait économiquement trop contraignant voir impossible d'exiger d'emblée le mode avancé. L'objectif pour les accepteurs est de pouvoir se passer du mode de vente à distance classique.

Plus particulièrement, dans le cas de la variante de réalisation décrite, la détection par les moyens de traitement informatique serveur 33 intervient lors de la transmission par l'accepteur 23 à l'organisme 7 du numéro d'appel 13 associé au terminal mobile 25.

Plus particulièrement également, dans le cas de la variante de réalisation décrite, les moyens de traitement

informatique serveur 33 comprennent en outre des moyens de verrouillage 72 pour bloquer la mise en œuvre du mode de base dans le cas où l'organisme 7 détecte qu'une clé publique de signature 50 est associée au numéro d'appel 13. Il en résulte que l'utilisateur 2 n'a pas d'autre solution pour effectuer des paiements à distance que de demander un certificat 55 selon le mode avancé.

De préférence, les moyens de traitement informatique serveur 33 comprennent en outre des moyens de contrôle 73 pour contrôler qu'un utilisateur 2 demandant un certificat 55 n'utilise pas un mot de passe 15 ayant déjà été utilisé en paiement en mode de base en association avec le numéro d'appel 13 de l'utilisateur 2. Il en résulte que les risques de compromission de mots de passe sont réduits. le niveau de sécurité est optimisé en mode avancé. De préférence, le processus de demande de délivrance de certificat met en œuvre un mécanisme préservant la confidentialité du mot de passe lors de la transmission à l'organisme.

Phase de paiement en mode de base

Dans le cas où le paiement ne peut pas être effectué selon le mode avancé, les moyens mis en œuvre lors du processus (b) de demande de délivrance de certificat 55 et lors de la phase de paiement (c) du mode avancé sont substitués par les moyens ci-après spécifiés plus particulièrement agencés en vue du paiement en mode de base.

Le système comprend à cet effet des moyens de transmission accepteur 44 permettant à l'utilisateur 2 de transmettre à l'accepteur 23 le numéro d'appel 13 associé au terminal mobile 25. les moyens de réception serveur 37 du serveur 9 de l'organisme 7 sont agencés pour recevoir de l'accepteur 23 le numéro d'appel 13 associé au terminal mobile 25 ainsi que des informations relatives au paiement 62, dont le montant du paiement. les moyens de réception serveur 37 du serveur 9 de l'organisme 7 sont agencés pour adresser à l'utilisateur 2 un message de saisie 75, notamment de type SMS,

en utilisant le numéro d'appel 13 associé au terminal mobile 25. le message de saisie 75 comprend les informations relatives au paiement 62 et une requête de saisie du mot de passe 68, se présentant notamment sous la forme d'un champ de saisie 19 dans le message de saisie 75. les moyens de transmission terminal mobile 74 sont agencés pour permettre à l'utilisateur 2 de transmettre en retour le mot de passe 15 au serveur 9 de l'organisme 7, notamment en saisissant le mot de passe 15 dans le champ de saisie 19. les moyens de traitement informatique serveur 33 sont agencés pour vérifier dans la base de données 10 que le mot de passe 15, transmis par l'utilisateur 2, correspond au numéro d'appel 13 associé au terminal mobile 25 transmis par le accepteur 23. Les moyens de traitement informatique serveur 33 sont agencés pour rechercher dans la base de données 10, tout ou partie des données d'identification 20, notamment le numéro et la date d'expiration de l'objet portable 1, correspondant au numéro d'appel 13 associé au terminal mobile 25 et au mot de passe 15. Les moyens de traitement informatique serveur 33 sont agencés pour faire débiter ou débiter un compte bancaire associé à l'objet portable 1 du montant du paiement et de faire créditer ou créditer l'accepteur 23 du montant. Les moyens de traitement informatique serveur 33 sont agencés pour confirmer auprès de l'accepteur 23 le paiement à distance de l'utilisateur 2. Il serait préférable, avant de confirmer auprès de l'accepteur le paiement à distance de l'utilisateur, de vérifier la validité de l'objet portable. Il résulte de la combinaison des traits techniques que le paiement est acquitté à distance par l'utilisateur 2 sans qu'il ait eu à communiquer à l'accepteur 23 les données d'identification 20 de l'objet portable 1, notamment le numéro et de la date d'expiration de la carte bancaire 5 de l'utilisateur 2.

Modèle économique

Les opérateurs de téléphonie mobile 69 devraient trouver un fort intérêt pour le procédé et le système selon l'invention, en mode de base et en mode avancé. Ils ont en effet

un problème aigu en matière de rechargement et ils ont besoin de nouvelles sources de revenu pour justifier les investissements considérables qui sont nécessaires pour passer à la technologie haut débit (dont UMTS).

Les rechargements par carte à gratter leur coûtent très cher et les rechargements par carte bancaire en mode vente à distance occasionnent un taux d'impayé excessif.

Pour pouvoir bénéficier de la réduction du taux d'impayé permis par le procédé et le système selon l'invention, les opérateurs de téléphonie mobile 69 ne devront plus accepter des paiements en mode vente à distance traditionnel par carte bancaire car :

- seuls les clients honnêtes sont susceptibles d'accepter de payer selon le procédé ou le système selon l'invention (ou selon d'autres formes de paiement sécurisé)
- alors que 100 % des fraudeurs risquent de continuer à payer en mode vente à distance traditionnelle.

Le procédé et le système selon l'invention permettent à un accepteur 23 et notamment aux opérateurs français de téléphonie mobile 69 de refuser de continuer à accepter des paiements en mode vente à distance traditionnel. En effet, la phase d'enregistrement préalable est accessible, à tout utilisateur d'un terminal mobile disposant d'une carte bancaire, en libre service sur des distributeurs automatiques de billets (DAB) présents à travers toute la France. La souplesse de la phase d'enregistrement offerte par le procédé et le système selon l'invention ne constitue donc pas une contrainte inacceptable pour les utilisateurs. Selon l'ancienneté du terminal mobile et de sa carte SIM, l'utilisateur pourra accéder au mode avancé et sinon, au pire, au mode de base qui est en tout état de cause accessible.

L'opération de rechargement, vitales pour les opérateurs de téléphonie, sera l'application de lancement (la « killer application ») du procédé et du système selon l'invention : cette application sera suffisante pour assurer

l'adhésion d'un très grand nombre d'utilisateurs au procédé et au système selon l'invention.

Grâce à cette dynamique, d'autres accepteurs 23 offrant des biens ou des services à distance adopteront à leur tour le procédé et le système selon l'invention. Ils pourront ainsi bénéficier pour eux-mêmes d'une réduction de leur taux d'impayés sur les paiements encaissés par carte bancaire 5.

Les opérateurs de téléphonie mobile 69 seront néanmoins les premiers bénéficiaires du procédé et le système selon l'invention. Le succès commercial de la présente invention dépendra largement d'eux :

- ils refuseront de continuer à accepter le mode vente à distance et en pousseront les utilisateurs à s'enregistrer au procédé et au système selon l'invention,
- ils permettront ainsi de généraliser progressivement l'utilisation des cartes SIM préparées pour la signature électronique, pour effectuer des paiements à distance non-répudiables.

Les opérateurs seront donc associés à l'organisme, notamment une ou des banques, au lancement du procédé et du système selon l'invention.

NOMENCLATURE

Groupe nominal	Réf. Num.
objet portable	1
utilisateur	2
carte bancaire	5
organisme	7
terminal	8
serveur	9
base de données	10
données d'authentification	11
clavier	12
numéro d'appel	13
mot de passe	15
écran	16
ticket	17
message	18
champ de saisie	19
données d'identification	20
accepteur	23
terminal mobile	25
moyens d'accouplements	26
moyens de connexion	27
réseau de communication	28
interface utilisateur-terminal	29
moyens de vérification terminal	30
moyens de transmission terminal	31
moyens de communication terminal	32
moyens de traitement informatique serveur	33
moyens d'enregistrement	34
moyens de réception serveur	37
moyens de transmission serveur	38
moyens de vérification serveur	39
moyens de lecture terminal	43

moyens de transmission accepteur	44
carte SIM	48
clé privée de signature	49
publique de signature	50
mot de passe de signature	51
application de demande de certificat	52
mécanisme de signature	53
une application de paiement	54
certificat	55
demande de certificat	56
signature	58
message signé	59
Référence(s) de certificat	60
requête d'activation de l'application de demande de certificat	61
informations relatives audit paiement	62
message de demande de paiement	63
message de paiement	66
message de paiement signé	67
requête de saisie dudit mot de passe	68
opérateur de téléphonie	69
moyens de production serveur	70
moyens de transmission serveur	71
moyens de verrouillage	72
moyens de contrôle	73
moyens de transmission terminal mobile	74
Message de saisie	75
Clavier terminal mobile	76
Requête d'activation de l'application de paiement	77

REVENDICATIONS

1. Procédé destiné à permettre à un utilisateur (2), disposant d'un objet portable (1) et d'un terminal mobile (25) ayant une fonction de téléphonie, d'effectuer un paiement à distance auprès d'un accepteur (23) ; ledit objet portable (1) se présentant notamment sous la forme d'une carte bancaire (5) ;

ledit procédé comprenant un mode avancé comportant trois phases :

-une phase d'enregistrement

-un processus de demande et de délivrance de certificat

- une phase de paiement ;

(a) une phase d'enregistrement

Lors d'une phase d'enregistrement dudit utilisateur (2) auprès d'un organisme (7), notamment un organisme bancaire :

- l'étape, pour ledit utilisateur (2), d'accoupler ledit objet portable (1) à un terminal (8), notamment de type distributeur automatique de billets (DAB-GAB) ou de type terminal de paiement électronique (TPE) ; ledit terminal (8) étant connecté de manière directe ou indirecte à un serveur (9) associé à une base de données (10) dudit organisme (7) ;

ledit procédé comprenant en outre, lors de ladite phase d'enregistrement :

- l'étape, pour ledit utilisateur (2), sur requête dudit terminal (8), d'entrer dans ledit terminal (8) des données d'authentification (11) dudit utilisateur (2), notamment un code confidentiel et/ou des données bio-métriques, associées audit objet portable (1),

- l'étape, pour ledit terminal (8), de vérifier que lesdites données d'authentification (11) dudit utilisateur (2), correspondent audit objet portable (1) ;

de sorte que la phase d'enregistrement permet d'authentifier l'objet portable (1) et de vérifier que l'utilisateur (2) est bien le titulaire de l'objet portable (1) ;

ledit procédé comprenant en outre :

- l'étape, pour ledit terminal (8), de lire dans ledit objet portable (1) et de transmettre audit serveur (9) des données d'identification (20), notamment le numéro et la date d'expiration dudit objet portable (1) ainsi que le nom et le prénom du titulaire dudit objet portable (1),

- l'étape, pour ledit utilisateur (2), sur requête dudit terminal (8), de composer, au moyen d'un clavier (12) dudit terminal (8), le numéro d'appel (13) associé audit terminal mobile (25) ; ledit numéro d'appel (13) associé audit terminal mobile (25) étant transmis, par ledit terminal (8), audit serveur (9) ;

ledit procédé comprenant en outre :

- l'étape, pour ledit terminal (8), de transmettre un mot de passe (15) audit utilisateur (2), notamment en affichant ledit mot de passe (15) sur un écran (16) dudit terminal (8) et/ou en délivrant audit utilisateur (2) un ticket (17) sur lequel est imprimé ledit mot de passe (15) ; ledit mot de passe (15) ayant été déterminé par ledit serveur (9) et transmis audit terminal (8) ;

de sorte que ledit mot de passe (15) attribué par le serveur (9) ne peut être transmis qu'audit utilisateur (2) titulaire dudit objet portable (1) authentifié ;

ledit procédé comprenant en outre, lors de ladite phase d'enregistrement :

- l'étape, pour ledit serveur (9), de mémoriser et d'associer, dans ladite base de données (10) dudit organisme (7) :

  - lesdites données d'identification (20),
  - ledit numéro d'appel (13) associé audit terminal mobile (25),
  - ledit mot de passe (15) ;

(b) processus de demande et de délivrance de certificat (55)

(b1) étape préalable

ledit terminal mobile (25) comportant une carte SIM (48) personnalisée par un opérateur de téléphonie mobile ; ladite carte SIM (48) étant associée audit numéro d'appel (13) dudit terminal mobile (25) ; ladite carte SIM (48) contenant :

- une clé privée de signature (49) associée à une clé publique de signature (50),
- un mot de passe de signature (51); ledit mot de passe de signature (51) étant soit un mot de passe de signature (51) d'origine que ledit opérateur de téléphonie (69) a déterminé et transmis audit utilisateur (2), soit un nouveau mot de passe de signature (51) que ledit utilisateur (2) a substitué audit mot de passe de signature (51) d'origine ;

ladite carte SIM (48) comprenant en outre :

- des fonctions cryptographiques,
- une application de demande de certificat (52) comportant un mécanisme de signature (53) mettant en œuvre ladite clé privée de signature (49),
- une application de paiement (54),

ledit organisme (7) disposant de ladite clé publique de signature (50) ;

de sorte que l'organisme (7) est capable d'établir un lien entre le numéro d'appel (13) et la clé publique de signature (50) ;

(b2) processus de demande et de délivrance de certificat (55) à proprement parler

ledit procédé comprenant en outre, pour permettre audit utilisateur (2) de demander et d'obtenir un certificat (55) auprès dudit organisme (7), les étapes suivantes :

- l'étape, pour ledit utilisateur (2), de transmettre une demande de certificat (56) audit organisme (7) :
  - en actionnant ladite application de demande de certificat (52) de ladite carte SIM (48),
  - en saisissant sur ledit clavier terminal mobile (76) ledit mot de passe (15),

• en structurant, au moyen de ladite application de demande de certificat (52), un message (18), notamment de type SMS, contenant ledit numéro d'appel (13) et ledit mot de passe (15),

• en saisissant sur le clavier terminal mobile (76) un mot de passe de signature (51) ; ledit mot de passe de signature (51) ainsi saisi étant comparé avec ledit mot de passe de signature (51) de ladite carte SIM (48) ;

ledit mot de passe de signature (51) activant ledit mécanisme de signature (53) :

- pour produire une signature (58), et
- pour produire un message signé (59) composé dudit message (18) et de ladite signature (58) ainsi obtenue, en mettant en œuvre ladite clé privée de signature (49), et
- pour transmettre ledit message signé (59) audit organisme (7) ;

ledit procédé comprenant en outre, pour ledit organisme (7), les étapes suivantes :

- l'étape de vérifier que ledit numéro d'appel (13) et ledit mot de passe (15) ainsi transmis ont bien été mémorisés lors de la phase d'enregistrement et sont associés dans ladite base de données (10) dudit organisme (7),
- l'étape d'extraire, de ladite base de données (10), lesdites données d'identification (20), correspondant audit numéro d'appel (13) et audit mot de passe (15), notamment le numéro et la date d'expiration dudit objet portable (1) ainsi que le nom et le prénom du titulaire dudit objet portable (1),
- l'étape de rechercher la clé publique de signature (50) associée audit numéro d'appel (13),
- l'étape de vérifier ladite signature (58) au moyen de ladite clé publique de signature (50) ;

(b3) production et délivrance du certificat (55)

ledit procédé comprenant en outre :

- l'étape de fabriquer un certificat (55) en utilisant notamment ledit numéro d'appel (13), tout ou partie desdites

données d'identification (20) et ladite clé publique de signature (50),

- l'étape de mémoriser et d'associer avec ledit numéro d'appel (13) et ledit mot de passe (15), dans ladite base de données (10) dudit organisme (7), ledit certificat (55) et une référence de certificat (60) dudit certificat (55),

- l'étape de transmettre audit terminal mobile (25), en réponse à la demande de certificat (56), ladite référence de certificat (60) et une requête d'activation (61) de ladite application de demande de certificat (52),

- l'étape, pour ledit terminal mobile (25), d'activer ladite application de demande de certificat (52),

- l'étape, pour ladite application de demande de certificat (52), de mémoriser ladite référence de certificat (60) dans ladite carte SIM (48) ;

(c) une phase de paiement

ledit procédé comprenant en outre lors d'une phase de paiement :

- l'étape, pour ledit utilisateur (2), de transmettre audit accepteur (23) ledit numéro d'appel (13) associé audit terminal mobile (25) ;

- l'étape, pour ledit accepteur (23), de transmettre audit organisme (7) ledit numéro d'appel (13) associé audit terminal mobile (25) ainsi que des informations relatives audit paiement (62), dont le montant dudit paiement,

- l'étape, pour ledit organisme (7) d'adresser audit terminal mobile (25) dudit utilisateur (2) un message de demande de paiement (63), notamment de type SMS, en utilisant ledit numéro d'appel (13) associé audit terminal mobile (25) ; ledit message de demande paiement (63) comprenant :

- lesdites informations relatives audit paiement (62),
- une requête d'activation de l'application de paiement (77),

- l'étape, pour ledit terminal mobile (25), d'activer ladite application de paiement (54),

- l'étape, pour ladite application de paiement (54) ainsi activée, d'afficher lesdites informations relatives audit paiement (62) ainsi que lesdites références de certificat (60) mémorisées dans ladite carte SIM (48),

- l'étape, pour ledit utilisateur , de sélectionner, au moyen dudit clavier terminal mobile (76), en cas de choix multiples, une référence de certificat (60) à utiliser pour effectuer ledit paiement,

- l'étape, pour ladite application de paiement (54), d'afficher un champ de saisie (19) dudit mot de passe de signature (51),

- l'étape, pour ledit utilisateur (2), de donner son accord concernant ledit paiement en saisissant ledit mot de passe de signature (51), dans ledit champ de saisie (19), au moyen dudit clavier terminal mobile (76),

- l'étape, pour ladite application de paiement (54), de contrôler ledit mot de passe de signature (51) ainsi saisi en le comparant avec ledit mot de passe de signature (51) de ladite carte SIM (48),

- l'étape, pour ladite application de paiement (54) :

• (i) de structurer un message de paiement (66), notamment de type SMS, contenant ladite référence de certificat (60) et des données de paiement, au moins en partie constituées à partir desdites informations relatives audit paiement (62), notamment le montant dudit paiement, la date dudit paiement, une référence de transaction, une identification dudit accepteur (23),

• (ii) de signer ledit message de paiement (66), en mettant en œuvre ladite clé privée de signature (49),

• (iii) de produire un message de paiement signé (67) composé dudit message de paiement (66) et de ladite signature (58) ainsi obtenue, et

• (iv) de renvoyer audit organisme (7) ledit message de paiement signé (67) ainsi produit,

- l'étape, pour ledit organisme (7), d'extraire de ladite base de données (10), ledit certificat (55) et tout ou partie desdites données d'identification (20), notamment ledit numéro et ladite date d'expiration dudit objet portable (1), correspondant audit numéro d'appel (13) associé audit terminal mobile (25) et à ladite référence de certificat (60),

- l'étape, pour ledit organisme (7), de vérifier la signature (58) dudit message de paiement signé (67) en mettant en œuvre ladite clé publique de signature (50) dudit certificat (55),

- l'étape, pour ledit organisme (7), de vérifier que ledit certificat (55) correspond audit utilisateur (2) ayant transmis audit accepteur (23) ledit numéro d'appel (13) associé audit terminal mobile (25) et de vérifier que ledit message de paiement signé (67) ainsi renvoyé correspond audit message de demande de paiement (63),

- l'étape, pour ledit organisme (7) :

• de faire débiter ou débiter un compte bancaire associé audit objet portable (1) du montant dudit paiement et de faire créditer ou créditer ledit accepteur (23) dudit montant,

• de confirmer auprès dudit accepteur (23) ledit paiement à distance dudit utilisateur (2) ;

de sorte que le paiement est acquitté à distance par l'utilisateur (2) sans qu'il ait eu à communiquer à l'accepteur (23) les données d'identification (20) de l'objet portable (1), notamment le numéro et de la date d'expiration de la carte bancaire (5) de l'utilisateur (2).

2. Procédé selon la revendication 1 ; ledit procédé comprenant, outre ledit mode avancé faisant l'objet de la revendication 1, un mode de base et un processus de sélection automatique du mode approprié ; la phase d'enregistrement du mode de base étant identique à la phase d'enregistrement du mode avancé ; ledit processus de sélection automatique comprenant l'étape de déterminer si ledit paiement peut être effectué selon ledit mode avancé ou s'il doit être effectué selon ledit mode de

base ; ladite détermination pouvant être effectuée au cours de ladite phase de paiement (c) et/ou au cours du processus de demande et de délivrance de certificat (55) (b) ;

dans le cas où ledit paiement ne peut pas être effectué selon ledit mode avancé, les étapes du processus de demande de délivrance de certificat (55) (b) et les étapes du processus de la phase de paiement (c) dudit mode avancé sont substituées par les étapes suivantes dudit mode de base, lors de la phase de paiement :

- l'étape, pour ledit utilisateur (2), de transmettre audit accepteur (23) ledit numéro d'appel (13) associé audit terminal mobile (25) ;
- l'étape, pour ledit accepteur (23), de transmettre audit organisme (7) ledit numéro d'appel (13) associé audit terminal mobile (25) ainsi que des informations relatives audit paiement (62), dont le montant dudit paiement,
- l'étape, pour ledit organisme (7) d'adresser audit utilisateur (2) un message de saisie (75), notamment de type SMS, en utilisant ledit numéro d'appel (13) associé audit terminal mobile (25) ; ledit message de saisie (75) comprenant :
  - lesdites informations relatives audit paiement (62),
  - une requête de saisie dudit mot de passe (68), se présentant notamment sous la forme d'un champ de saisie (19) dans ledit message de saisie (75),
- l'étape, pour ledit utilisateur (2), de transmettre en retour ledit mot de passe (15) audit organisme (7), notamment en saisissant ledit mot de passe (15) dans ledit champ de saisie (19),
- l'étape, pour ledit organisme (7), de vérifier dans ladite base de données (10) que ledit mot de passe (15), transmis par ledit utilisateur (2), correspond audit numéro d'appel (13) associé audit terminal mobile (25) transmis par ledit accepteur (23),
- l'étape, pour ledit organisme (7) :

• de rechercher, dans ladite base de données (10), tout ou partie desdites données d'identification (20), notamment ledit numéro et ladite date d'expiration dudit objet portable (1), correspondant audit numéro d'appel (13) associé audit terminal mobile (25) et audit mot de passe (15),

• de faire débiter ou débiter un compte bancaire associé audit objet portable (1) du montant dudit paiement et de faire créditer ou créditer ledit accepteur (23) dudit montant,

• de confirmer auprès dudit accepteur (23) ledit paiement à distance dudit utilisateur (2) ;

de sorte que le paiement est acquitté à distance par l'utilisateur (2) sans qu'il ait eu à communiquer à l'accepteur (23) les données d'identification (20) de l'objet portable (1), notamment le numéro et de la date d'expiration de la carte bancaire (5) de l'utilisateur (2).

3. Procédé selon la revendication 2 ; ledit procédé étant tel que pour déterminer si ledit paiement peut être effectué selon ledit mode avancé ou s'il doit être effectué selon ledit mode de base, ledit organisme (7) détecte qu'une clé publique de signature (50) est associée audit numéro d'appel (13) soit que cette information provienne dudit opérateur de téléphonie (69) soit qu'elle provienne dudit terminal mobile (25) ;

de sorte que ledit organisme (7) peut, selon les options qu'il entend privilégier :

soit inviter ledit utilisateur (2) à demander un certificat (55) de manière qu'il puisse accéder audit mode avancé,

soit accepter que ledit utilisateur (2) puisse continuer à effectuer des paiements à distance selon ledit mode de base.

4. Procédé selon la revendication 3 ; ledit procédé étant tel que ladite détection intervient, au cours de ladite phase de paiement en mode de base, lors de la transmission par

ledit accepteur (23) audit organisme (7) dudit numéro d'appel (13) associé audit terminal mobile (25).

5. Procédé selon l'une quelconque des revendications 3 ou 4 ; ledit procédé comprenant en outre l'étape pour ledit organisme (7) de bloquer la mise en œuvre dudit mode de base dans le cas où ledit organisme (7) détecte qu'une clé publique de signature (50) est associée audit numéro d'appel (13) ;

de sorte que ledit utilisateur (2) n'a pas d'autre solution pour effectuer des paiements à distance que de demander un certificat (55) selon ledit mode avancé.

6. Procédé selon la revendication 5 ; ledit procédé comprenant en outre l'étape, pour ledit organisme (7), de contrôler qu'un utilisateur (2) demandant un certificat (55) n'utilise pas un mot de passe (15) ayant déjà été utilisé en paiement en mode de base en association avec ledit numéro d'appel (13) dudit utilisateur (2).

de sorte que les risques de compromission de mots de passe sont réduits ;

de sorte que le niveau de sécurité est optimisé en mode avancé.

Système

7. Système destiné à permettre à un utilisateur (2), disposant d'un objet portable (1) et d'un terminal mobile (25) ayant une fonction de téléphonie, d'effectuer un paiement à distance auprès d'un accepteur (23) ; ledit objet portable (1) se présentant notamment sous la forme d'une carte bancaire (5) ;

ledit système comprenant un mode avancé comportant trois phases :

- une phase d'enregistrement
- un processus de demande et de délivrance de certificat (55)
- une phase de paiement ;

(a) une phase d'enregistrement

ledit système comprenant, pour permettre l'enregistrement dudit utilisateur (2) auprès d'un organisme (7), notamment un organisme (7) bancaire :

- un terminal (8), notamment un terminal (8) de type distributeur automatique de billets (DAB-GAB) ou de type terminal (8) de paiement électronique (TPE), comportant des moyens d'accouplements (26) permettant audit utilisateur (2), d'accoupler ledit objet portable (1) audit terminal (8),

- un serveur (9) associé à une base de données (10) dudit organisme (7) ;

ledit serveur (9) comprenant des moyens de connexion (27) pour connecter, de manière directe ou indirecte, ledit terminal (8) audit serveur (9) via un réseau de communication (28), notamment informatique ;

ledit terminal (8) comprenant en outre :

- une interface utilisateur-terminal (29) permettant audit utilisateur (2) d'entrer dans ledit terminal (8), sur requête dudit terminal (8), des données d'authentification (11) dudit utilisateur (2), notamment un code confidentiel et/ou des données bio-métriques, associées audit objet portable (1),

- des moyens de vérification terminal (30) pour vérifier que lesdites données d'authentification (11) dudit utilisateur (2), correspondent audit objet portable (1) ;

de sorte que la phase d'enregistrement permet d'authentifier l'objet portable (1) et de vérifier que l'utilisateur (2) est bien le titulaire de l'objet portable (1) ;

ledit terminal (8) comprenant en outre :

- des moyens de lecture terminal (43) permettant de lire dans ledit objet portable (1) des données d'identification (20), notamment le numéro et la date d'expiration dudit objet portable (1) ainsi que le nom et le prénom du titulaire dudit objet portable (1),

- des moyens de transmission terminal (31) permettant de transmettre lesdites données d'identification (20) audit serveur (9) ;

lesdits moyens de lecture terminal (43) et lesdits moyens de transmission terminal (31) étant mis en œuvre lors de la phase d'enregistrement dudit utilisateur (2) ;

ledit terminal (8) étant tel que ladite interface utilisateur-terminal (29) comporte un clavier (12) permettant audit utilisateur (2) de composer, sur requête dudit terminal (8), le numéro d'appel (13) associé audit terminal mobile (25) ;

ledit terminal (8) comportant :

- des moyens de transmission terminal (31) pour transmettre audit serveur (9) ledit numéro d'appel (13) associé audit terminal mobile (25),

- des moyens de communication terminal (32) pour communiquer un mot de passe (15) audit utilisateur (2), notamment en affichant ledit mot de passe (15) sur un écran (16) dudit terminal (8) ou en délivrant audit utilisateur (2) un ticket (17) sur lequel est imprimé ledit mot de passe (15) ;

- ledit mot de passe (15) ayant été déterminé par ledit serveur (9) en mettant en œuvre des moyens de traitement informatique serveur (33) ; ledit mot de passe (15) ayant été transmis par ledit serveur (9) audit terminal (8), via ledit réseau de communication (28) ;

de sorte que ledit mot de passe (15) attribué par le serveur (9) ne peut être transmis qu'audit utilisateur (2) titulaire dudit objet portable (1) authentifié ;

lesdits moyens de traitement informatique serveur (33) comportant des moyens d'enregistrement (34) pour mémoriser et associer dans ladite base de données (10) :

- lesdites données d'identification (20),
- ledit numéro d'appel (13) associé audit terminal mobile (25),
- ledit mot de passe (15) ;

b) processus de demande et de délivrance de certificat (55) ;

b1) phase préalable ;

ledit système comprenant en outre des moyens de demande et de délivrance de certificat (55) susceptibles d'être mis en œuvre par ledit utilisateur (2) et ledit organisme (7) dans le cas où ledit terminal mobile (25) comporte une carte SIM (48) personnalisée par un opérateur de téléphonie (69) mobile ; ladite carte SIM (48) étant associée audit numéro d'appel (13) dudit terminal mobile (25) ; ladite carte SIM (48) contenant :

- une clé privée de signature (49) associée à une clé publique de signature (50),
- un mot de passe de signature (51); ledit mot de passe de signature (51) étant soit un mot de passe de signature (51) d'origine que ledit opérateur de téléphonie (69) a déterminé et transmis audit utilisateur (2), soit un nouveau mot de passe de signature (51) que ledit utilisateur (2) a substitué audit mot de passe de signature (51) d'origine ;

ladite carte SIM (48) comprenant en outre :

- des fonctions cryptographiques,
- une application de demande de certificat (52) comportant un mécanisme de signature (53) mettant en œuvre ladite clé privée de signature (49),
- une application de paiement (54) ;

ledit organisme (7) disposant de ladite clé publique de signature (50) ;

de sorte que l'organisme (7) est capable d'établir un lien entre le numéro d'appel (13) et la clé publique de signature (50) ;

b2) Processus de demande ;

lesdits moyens de demande et de délivrance de certificat (55) pour demander et obtenir un certificat (55) auprès dudit organisme (7), étant composés de moyens de transmission terminal mobile (74), mis en œuvre par ledit

utilisateur (2), pour transmettre une demande de certificat (56) audit organisme (7) :

- en actionnant ladite application de demande de certificat (52) de ladite carte SIM (48),
- en saisissant sur ledit clavier terminal mobile (76) ledit mot de passe (15),
- en structurant, au moyen de ladite application de demande de certificat (52), un message (18), notamment de type SMS, contenant ledit numéro d'appel (13) et ledit mot de passe (15),
- en saisissant sur ledit clavier terminal mobile (76) un mot de passe signature (51) ; ledit mot de passe de signature (51) ainsi saisi étant comparé avec ledit mot de passe de signature (51) de ladite carte SIM (48) ;

ledit mot de passe de signature (51) activant ledit mécanisme de signature (53) :

- pour signer ledit message (18), et
- pour produire un message signé (59) composé dudit message (18) et de la signature (58) ainsi obtenue, en mettant en œuvre ladite clé privée de signature (49), et
- pour transmettre ledit message signé (59) audit organisme (7) ;

b3) processus de vérification ;

lesdits moyens de demande et de délivrance de certificat (55) pour demander et obtenir un certificat (55) auprès dudit organisme (7), étant en outre composés :

- de moyens de vérification serveur (39), mis en œuvre par ledit organisme (7), pour vérifier que ledit numéro d'appel (13) et ledit mot de passe (15) ainsi transmis ont bien été mémorisés lors de la phase d'enregistrement et sont associés dans ladite base de données (10) dudit organisme (7),
- desdits moyens de traitement informatique serveur (33) mis en œuvre par ledit organisme (7) et agencés pour extraire, de ladite base de données (10), lesdites données d'identification (20), correspondant audit numéro d'appel (13)

et audit mot de passe (15), notamment le numéro et la date d'expiration dudit objet portable (1) ainsi que le nom et le prénom du titulaire dudit objet portable (1),

- desdits moyens de traitement informatique serveur (33) mis en œuvre par ledit organisme (7) et agencés pour rechercher la clé publique de signature (50) associée audit numéro d'appel (13),

- desdits moyens de traitement informatique serveur (33) mis en œuvre par ledit organisme (7) et agencés pour vérifier ladite signature (58) au moyen de ladite clé publique de signature (50) ;

b4) processus de production ;

lesdits moyens de demande et de délivrance de certificat (55) pour demander et obtenir un certificat (55) auprès dudit organisme (7), étant en outre composés :

- de moyens de production serveur (70) pour fabriquer un certificat (55) en utilisant notamment ledit numéro d'appel (13), tout ou partie desdites données d'identification (20) et ladite clé publique de signature (50),

- desdits moyens de traitement informatique serveur (33) mis en œuvre par ledit organisme (7) et agencés pour mémoriser et associer avec ledit numéro d'appel (13) et ledit mot de passe (15), dans ladite base de données (10) dudit organisme (7), ledit certificat (55) et une référence de certificat (60) dudit certificat (55),

- desdits moyens de transmission serveur (38) mis en œuvre par ledit organisme (7) et agencés et agencés pour transmettre audit terminal mobile (25), en réponse à la demande de certificat (56), ladite référence de certificat (60) et une requête d'activation (61) de ladite application de demande de certificat (52),

- dudit terminal mobile (25) agencé pour activer ladite application de demande de certificat (52),

- de ladite application de demande de certificat (52) agencée pour mémoriser ladite référence de certificat (60) dans ladite carte SIM (48) ;

(c) une phase de paiement ;

ledit système comprenant des moyens de transmission accepteur (44) permettant audit utilisateur (2), de transmettre audit accepteur (23) ledit numéro d'appel (13) associé audit terminal mobile (25) ;

ledit serveur (9) dudit organisme (7) comprenant en outre :

- des moyens de réception serveur (37) pour recevoir dudit accepteur (23) ledit numéro d'appel (13) associé audit terminal mobile (25) ainsi que des informations relatives audit paiement (62), dont le montant dudit paiement,

- des moyens de transmission serveur (38) pour adresser audit terminal mobile (25) dudit utilisateur (2) un message de demande de paiement (63), notamment de type SMS, en utilisant ledit numéro d'appel (13) associé audit terminal mobile (25) ;

ledit message de demande de paiement (63) comprenant lesdites informations relatives audit paiement (62) et une requête d'activation de l'application de paiement (77) ;

ledit terminal mobile (25) étant agencé pour d'activer ladite application de paiement (54) ;

ladite application de paiement (54) ainsi activée étant agencée pour afficher lesdites informations relatives audit paiement (62) ainsi que lesdites références de certificat (60) mémorisées dans ladite carte SIM (48) ;

ledit terminal mobile (25) étant agencé pour que ledit utilisateur (2) puisse sélectionner, au moyen dudit clavier terminal mobile (76), en cas de choix multiples, une référence de certificat (60) à utiliser pour effectuer ledit paiement ;

ladite application de paiement (54) étant agencée pour afficher un champ de saisie (19) dudit mot de passe de signature (51) de sorte que ledit utilisateur (2) puisse donner son accord

concernant ledit paiement en saisissant ledit mot de passe de signature (51), dans ledit champ de saisie (19), au moyen dudit clavier terminal mobile (76) ;

ladite application de paiement (54) étant agencée pour contrôler ledit mot de passe de signature (51) ainsi saisi en le comparant avec ledit mot de passe de signature (51) de ladite carte SIM (48) ;

ladite application de paiement (54) étant agencée pour :

- (i) structurer un message de paiement (66), notamment de type SMS, contenant ladite référence de certificat (60) et des données de paiement, au moins en partie constituées à partir desdites informations relatives audit paiement (62), notamment le montant dudit paiement, la date dudit paiement, une référence de transaction, une identification dudit accepteur (23),
- (ii) produire une signature (58) en mettant en œuvre ladite clé privée de signature (49),
- (iii) produire un message de paiement signé (67) composé dudit message de paiement (66) et de ladite signature (58) ainsi obtenue, et
- (iv) renvoyer audit serveur (9) dudit organisme (7), via lesdits moyens de transmission terminal mobile (74), ledit message de paiement signé (67) ainsi produit ;

lesdits moyens de traitement informatique serveur (33) dudit organisme (7) étant agencés pour extraire de ladite base de données (10), ledit certificat (55) et tout ou partie desdites données d'identification (20), notamment ledit numéro et ladite date d'expiration dudit objet portable (1), correspondant audit numéro d'appel (13) associé audit terminal mobile (25) et à ladite référence de certificat (60) ;

lesdits moyens de traitement informatique serveur (33) dudit organisme (7) étant agencés pour vérifier ladite signature (58) dudit message de paiement signé (67) en mettant en œuvre ladite clé publique de signature (50) dudit certificat (55) ;

lesdits moyens de traitement informatique serveur (33) dudit organisme (7) étant agencés pour vérifier que ledit certificat (55) correspond audit utilisateur (2) ayant transmis audit accepteur (23) ledit numéro d'appel (13) associé audit terminal mobile (25) et pour vérifier que ledit message de paiement signé (67) ainsi renvoyé correspond audit message de demande de paiement (63) ;

lesdits moyens de traitement informatique serveur (33) dudit organisme (7) étant agencés pour :

- faire débiter ou débiter un compte bancaire associé audit objet portable (1) du montant dudit paiement et de faire créditer ou créditer ledit accepteur (23) dudit montant,
- confirmer auprès dudit accepteur (23) ledit paiement à distance dudit utilisateur (2) ;

de sorte que le paiement est acquitté à distance par l'utilisateur (2) sans qu'il ait eu à communiquer à l'accepteur (23) les données d'identification (20) de l'objet portable (1), notamment le numéro et la date d'expiration de la carte bancaire (5) de l'utilisateur (2).

8. Système selon la revendication 7 ; ledit système comprenant, outre ledit mode avancé faisant l'objet de la revendication 7, un mode de base et un processus de sélection automatique du mode approprié ; les moyens mis en œuvre lors de la phase d'enregistrement du mode de base étant identique aux moyens mis en œuvre lors de la phase d'enregistrement du mode avancé ; lesdits moyens de traitement informatique serveur (33) étant agencés pour déterminer si ledit paiement peut être effectué selon ledit mode avancé ou s'il doit être effectué selon ledit mode de base ; ladite détermination pouvant être effectuée au cours de ladite phase de paiement (c) et/ou au cours du processus de demande et de délivrance de certificat (55) (b) ; dans le cas où ledit paiement ne peut pas être effectué selon ledit mode avancé, lesdits moyens mis en œuvre lors du processus de demande de délivrance de certificat (55) (b) et lors du processus de la phase de paiement (c) dudit mode

avancé étant substitués par les moyens ci-après spécifiés plus particulièrement agencés au paiement en mode de base ;

ledit système comprend en outre des moyens de transmission accepteur (44) permettant audit utilisateur (2) de transmettre audit accepteur (23) ledit numéro d'appel (13) associé audit terminal mobile (25) ;

lesdits moyens de réception serveur (37) dudit serveur (9) dudit organisme (7) sont agencés pour recevoir dudit accepteur (23) ledit numéro d'appel (13) associé audit terminal mobile (25) ainsi que des informations relatives audit paiement (62), dont le montant dudit paiement ;

lesdits moyens de réception serveur (37) dudit serveur (9) dudit organisme (7) sont agencés pour adresser audit utilisateur (2) un message de saisie (75), notamment de type SMS, en utilisant ledit numéro d'appel (13) associé audit terminal mobile (25) ;

ledit message de saisie (75) comprenant lesdites informations relatives audit paiement (62) et une requête de saisie dudit mot de passe (68), se présentant notamment sous la forme d'un champ de saisie (19) dans ledit message de saisie (75) ;

lesdits moyens de transmission terminal mobile (74) étant agencés pour permettre audit utilisateur (2) de transmettre en retour ledit mot de passe (15) audit serveur (9) dudit organisme (7), notamment en saisissant ledit mot de passe (15) dans ledit champ de saisie (19) ;

lesdits moyens de traitement informatique serveur (33) étant agencés pour vérifier dans ladite base de données (10) que ledit mot de passe (15), transmis par ledit utilisateur (2), correspond audit numéro d'appel (13) associé audit terminal mobile (25) transmis par ledit accepteur (23) ;

lesdits moyens de traitement informatique serveur (33) étant agencés pour rechercher dans ladite base de données (10), tout ou partie desdites données d'identification (20), notamment ledit numéro et ladite date d'expiration dudit objet portable

(1), correspondant audit numéro d'appel (13) associé audit terminal mobile (25) et audit mot de passe (15) ;

lesdits moyens de traitement informatique serveur (33) étant agencés pour faire débiter ou débiter un compte bancaire associé audit objet portable (1) du montant dudit paiement et de faire créditer ou créditer ledit accepteur (23) dudit montant ;

lesdits moyens de traitement informatique serveur (33) étant agencés pour confirmer auprès dudit accepteur (23) ledit paiement à distance dudit utilisateur (2) ;

de sorte que le paiement est acquitté à distance par l'utilisateur (2) sans qu'il ait eu à communiquer à l'accepteur (23) les données d'identification (20) de l'objet portable (1), notamment le numéro et de la date d'expiration de la carte bancaire (5) de l'utilisateur (2).

9. Système selon la revendication 8 ; ledit système étant tel que pour déterminer si ledit paiement peut être effectué selon ledit mode avancé ou s'il doit être effectué selon ledit mode de base, lesdits moyens de traitement informatique serveur (33) dudit organisme (7) détectent si une clé publique de signature (50) est associée audit numéro d'appel (13) soit que cette information provienne dudit opérateur de téléphonie (69) soit qu'elle provienne dudit terminal mobile (25) ;

de sorte que ledit organisme (7) peut, selon les options qu'il entend privilégier :

soit inviter ledit utilisateur (2) à demander un certificat (55) de manière qu'il puisse accéder audit mode avancé,

soit accepter que ledit utilisateur (2) puisse continuer à effectuer des paiements à distance selon ledit mode de base.

10. Système selon la revendication 9 ; ledit système étant tel que ladite détection par lesdits moyens de traitement informatique serveur (33) intervient, au cours de ladite phase de paiement en mode de base, lors de la transmission par ledit

accepteur (23) audit organisme (7) dudit numéro d'appel (13) associé audit terminal mobile (25).

11. Système selon l'une quelconque des revendications 9 ou 10 ; lesdits moyens de traitement informatique serveur (33) comprenant en outre des moyens de verrouillage (72) pour bloquer la mise en œuvre dudit mode de base dans le cas où ledit organisme (7) détecte qu'une clé publique de signature (50) est associée audit numéro d'appel (13) ;

de sorte que ledit utilisateur (2) n'a pas d'autre solution pour effectuer des paiements à distance que de demander un certificat (55) selon ledit mode avancé.

12. Système selon la revendication 11 ; lesdits moyens de traitement informatique serveur (33) comprenant en outre des moyens de contrôle (73) pour contrôler qu'un utilisateur (2) demandant un certificat (55) n'utilise pas un mot de passe (15) ayant déjà été utilisé en paiement en mode de base en association avec ledit numéro d'appel (13) dudit utilisateur (2) ;

de sorte que les risques de compromission de mots de passe sont réduits ;

de sorte que le niveau de sécurité est optimisé en mode avancé.

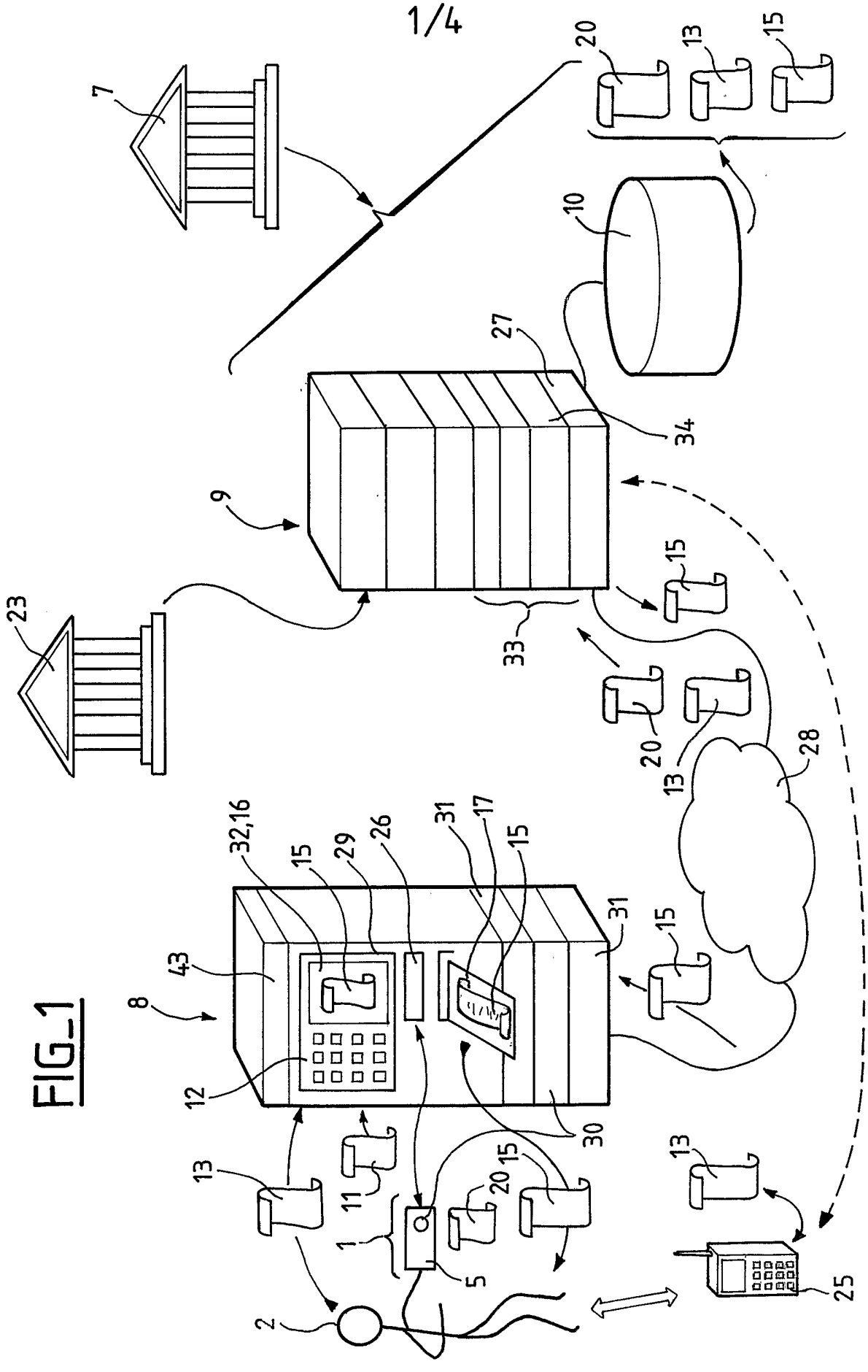


FIG_1

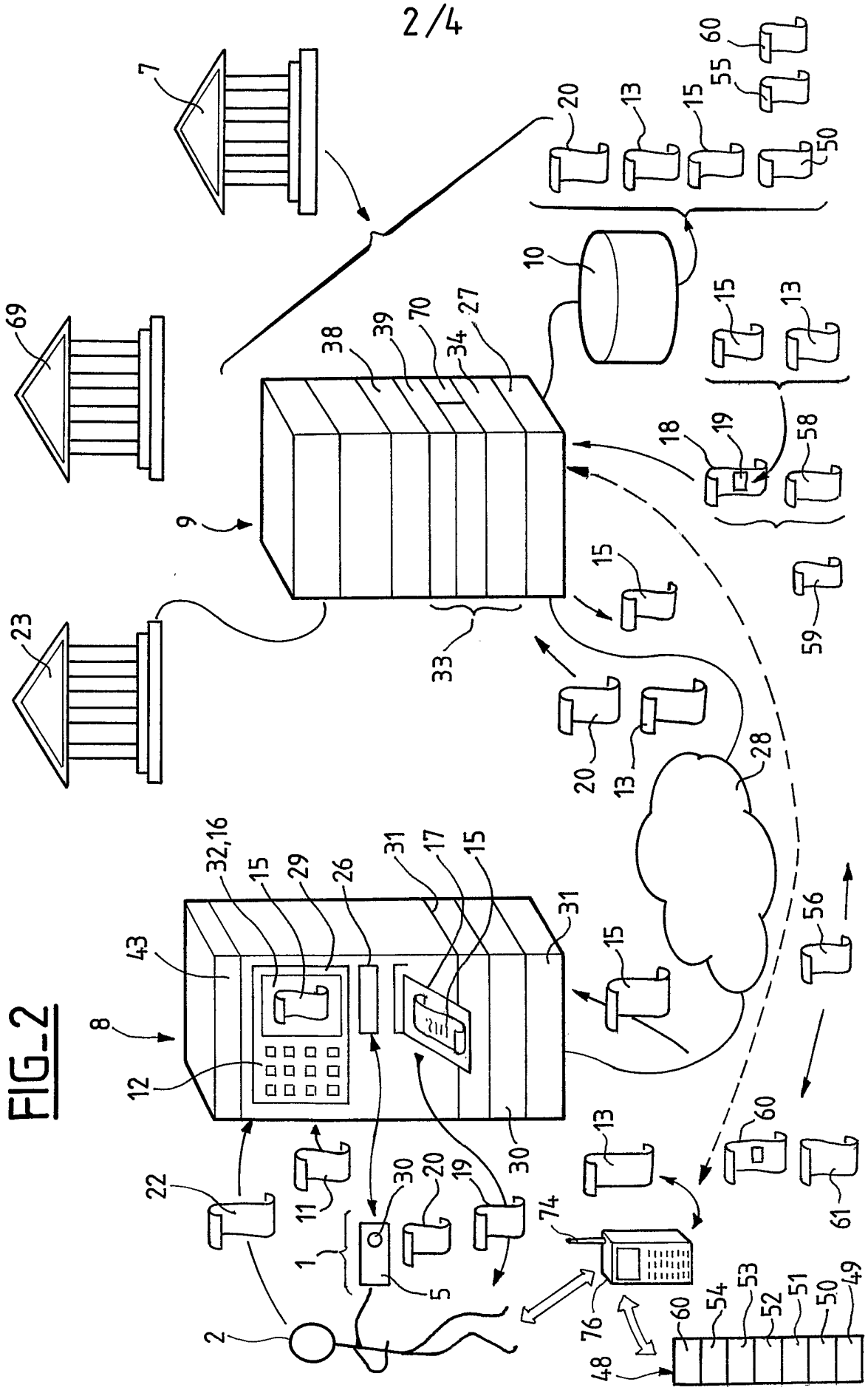
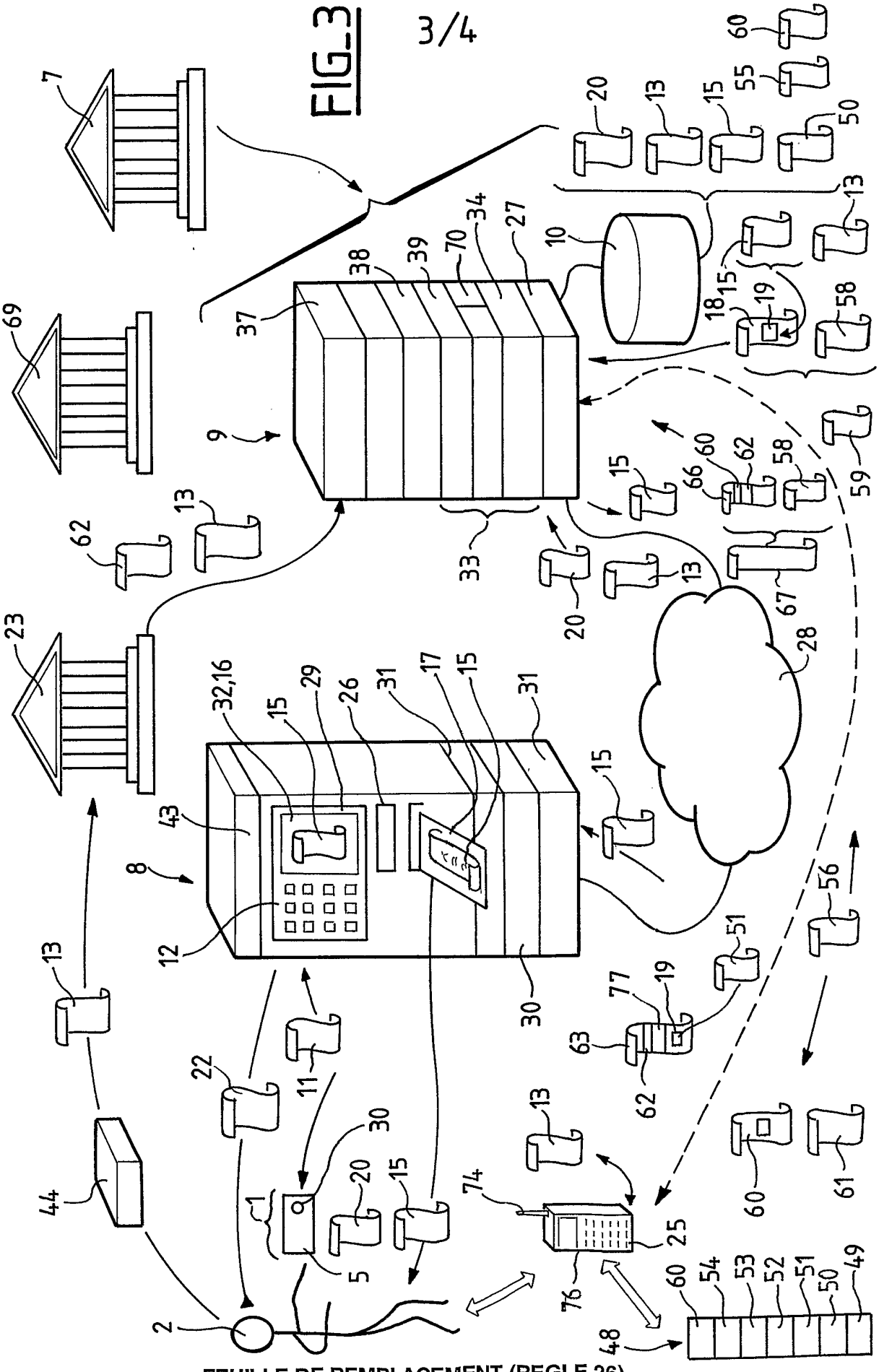

7
69
23
9
38
39
70
34
27
10
20
13
15
55
60
50
18
19
58
59
33
28
56
32,16
29
26
31
17
43
8
12
22
11
30
1
5
74
76
48
54
53
52
51
49
61

FIG_2

FIG_3

3/4



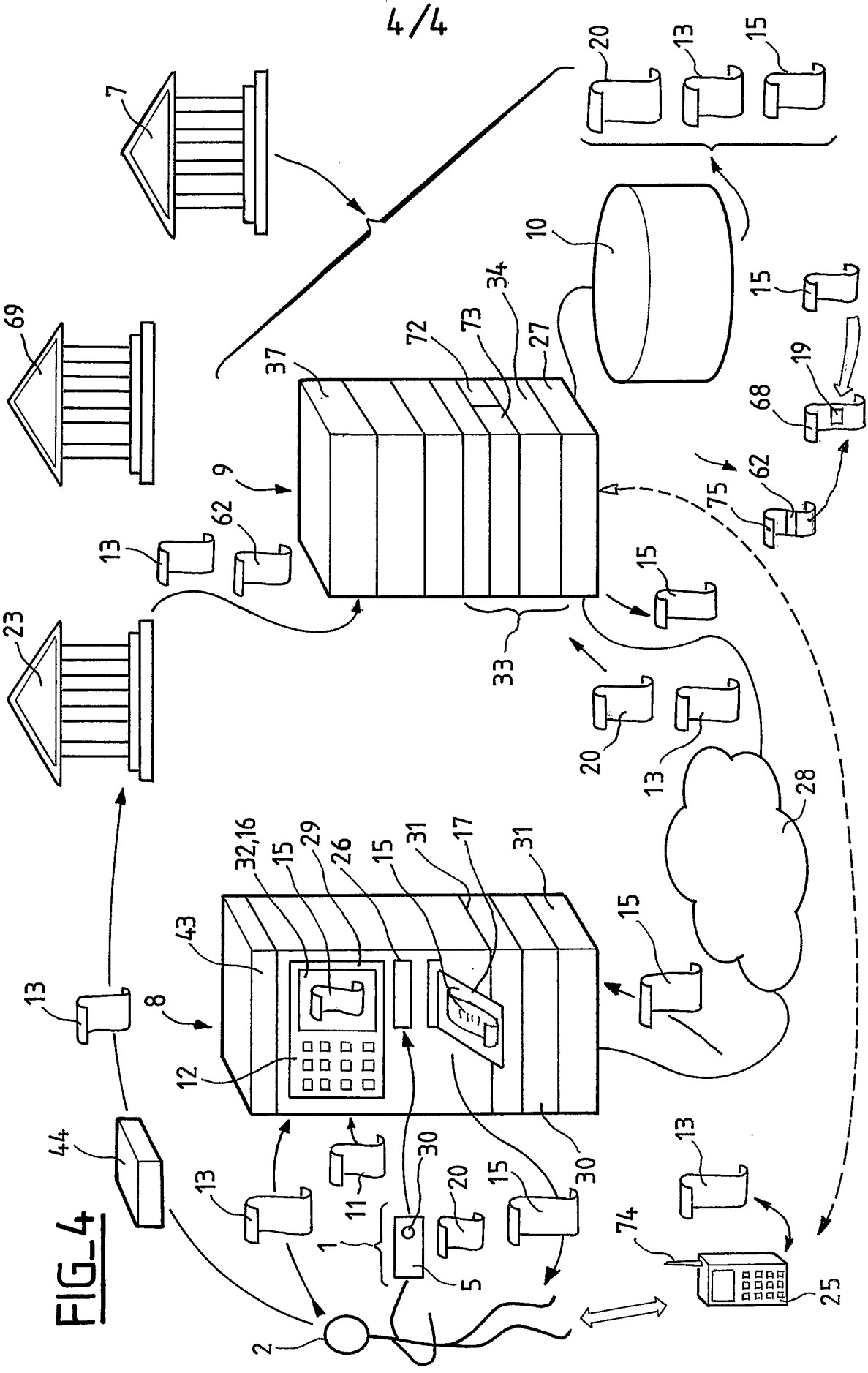

7
69
23
20
13
15
10
34
72
73
27
37
9
62
33
19
68
75
28
32,16
29
26
31
17
43
12
8
44
11
1
5
30
2
74
25

FIG_4