(19) RÉPUBLIQUE FRANÇAISE

INSTITUT NATIONAL
DE LA PROPRIÉTÉ INDUSTRIELLE

PARIS

(11) **N° de publication :** **2 904 902**
(à n'utiliser que pour les commandes de reproduction)

(21) **N° d'enregistrement national :** **06 53362**

(51) Int Cl[8] : **H 04 L 9/32** (2006.01), H 04 L 12/58, G 06 F 21/00, G 06 K 9/00, H 04 Q 7/32

(12) DEMANDE DE BREVET D'INVENTION A1

(22) **Date de dépôt :** 11.08.06.

(30) **Priorité :**

(43) **Date de mise à la disposition du public de la demande :** 15.02.08 Bulletin 08/07.

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

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

(71) **Demandeur(s) :** *FRANCE TELECOM Société anonyme* — FR.

(72) **Inventeur(s) :** BRUN ARNAUD et FLORE ELIAS CARLOS.

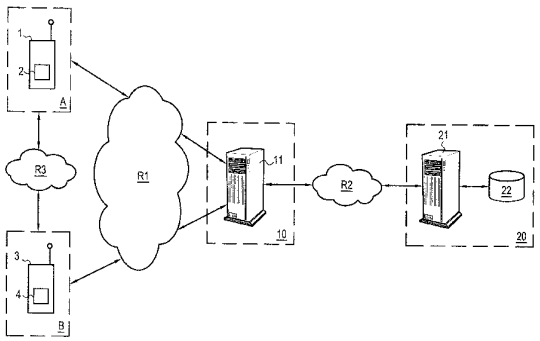
(73) **Titulaire(s) :**

(74) **Mandataire(s) :** CABINET BEAU DE LOMENIE.

(54) PROCEDE ET SYSTEME D'AUTHENTIFICATION D'UTILISATEURS DANS UN RESEAU DE COMMUNICATION.

(57) L'invention concerne un procédé d'authentification comprenant une étape de demande d'accès à un réseau de communication (R1; R3) par un utilisateur (A) équipé d'un premier terminal (1) apte à établir une communication avec au moins un deuxième terminal (3). Le procédé comprend en outre:

- une étape de création d'un message MMS, ledit message comprenant un corps et un en-tête, ledit corps comprenant au moins une page contenant une donnée biométrique d'authentification de l'utilisateur (A) du premier terminal (1),
- une étape d'insertion d'un champ d'authentification dans l'entête du message,
- une étape d'envoi dudit message à destination du deuxième terminal (3),
- une étape d'envoi du message MMS vers un serveur d'authentification (21) en réponse à une détection du champ d'authentification, et
- une étape d'authentification dans laquelle le serveur d'authentification (21) compare la donnée biométrique d'authentification reçue avec une donnée biométrique de référence préenregistrée.



FR 2 904 902 - A1

Domaine de l'invention

La présente invention se rapporte aux réseaux de communication dans lesquels des utilisateurs équipés d'un terminal de communication (fixe, mobile, ou hybride) peuvent envoyer des messages ou émettre des appels téléphoniques. Elle concerne plus particulièrement l'authentification des utilisateurs de tels réseaux lors de l'envoi d'un message ou de l'émission d'un appel téléphonique.

Art antérieur

Actuellement, lorsque le terminal d'un utilisateur reçoit un message de type message multimédia MMS, message SMS, email, etc. ou un appel téléphonique, le numéro ou le nom de l'émetteur du message ou de l'appel téléphonique peut être affiché sur l'écran du terminal. Cette fonctionnalité permet à l'utilisateur qui reçoit le message ou l'appel d'identifier l'émetteur.

Cependant, rien ne permet de garantir à l'utilisateur destinataire du message ou de l'appel que cette identité a été vérifiée par l'opérateur du réseau de communication et, par conséquent, que le message ou l'appel émis provient d'un utilisateur authentifié. En d'autres termes, les opérateurs de réseaux fixes et/ou mobiles peuvent à l'heure actuelle identifier les terminaux utilisés par leurs abonnés pour se connecter à leurs réseaux lors des communications, mais ils n'ont pas de moyens qui leur permettent d'authentifier les utilisateurs qui utilisent ces terminaux.

Il existe des procédés et systèmes permettant à un utilisateur de s'authentifier avec un niveau de sécurité important en utilisant comme donnée d'authentification une donnée biométrique telle qu'une empreinte digitale, iridienne ou vocale. Toutefois, l'authentification basée sur une donnée biométrique est utilisée dans des domaines très différents de ceux des communications. Elle est principalement utilisée pour permettre

l'accès à certain type de machines tels que des ordinateurs ou à des lieux (systèmes d'ouverture de porte).

Objet et description succincte de l'invention

La présente invention a pour objet de pallier ces inconvénients en proposant une solution permettant une authentification sûre des utilisateurs dans un réseau de communication lors de l'envoi d'un message ou de l'émission d'un appel téléphonique.

A cet effet l'invention concerne un procédé d'authentification d'utilisateurs dans un réseau de communication, ledit procédé comprenant une étape de demande d'accès au réseau de communication par un utilisateur équipé d'un premier terminal pour établir une communication vers au moins un deuxième terminal,

caractérisé en ce que le procédé comprend en outre:

- une étape de création d'un message MMS dont le corps comprend au moins une page ("slide") contenant une donnée biométrique d'authentification de l'utilisateur du premier terminal,
- une étape d'insertion d'un champ d'authentification dans l'en-tête du message,
- une étape d'envoi dudit message à destination du deuxième terminal,
- une étape de redirection automatique du message MMS vers un serveur d'authentification en réponse à la détection du champ d'authentification, et
- une étape d'authentification dans laquelle le serveur d'authentification compare la donnée biométrique d'authentification reçue avec une donnée biométrique de référence préenregistrée.

Ainsi, grâce au procédé de l'invention, un utilisateur peut s'authentifier auprès de ses correspondants dans le réseau de communication. En effet, par l'envoi d'un message MMS contenant une donnée biométrique de l'utilisateur qui est comparée par un serveur d'authentification avec une donnée biométrique de référence, l'opérateur du réseau de communication peut réaliser une authentification forte de ses abonnés. L'émetteur d'un message ou d'un appel téléphonique peut

ainsi être authentifié de manière sûre à la fois par l'opérateur et le ou les destinataires du message ou de l'appel, et ce pour chaque demande d'accès au réseau de communication.

Selon un aspect de l'invention, lorsque la demande d'accès au réseau de communication est initiée par l'envoi d'un message MMS par l'utilisateur à partir du premier terminal à destination du deuxième terminal, une valeur d'authentification d'émetteur de message est attribuée au champ d'authentification, le corps du message MMS comprenant en outre les éléments multimédias du message MMS que l'utilisateur souhaite envoyer.

Dans ce cas, le message MMS envoyé par l'utilisateur est enrichi d'un champ d'authentification auquel est attribué une valeur spécifique permettant l'authentification de l'émetteur du message MMS au moyen de la donnée biométrique transmise avec ce message.

Selon un autre aspect de l'invention, en cas d'authentification positive, le serveur d'authentification renvoie le message MMS à un centre MMS qui achemine ledit message MMS jusqu'au deuxième terminal qui notifie l'authentification de l'émetteur dudit message MMS reçu en réponse à la détection de la valeur d'authentification d'émetteur de message attribuée au champ d'authentification présent dans l'en-tête du message. Le destinataire du message est ainsi informé que l'émetteur du message a bien été authentifié.

Lorsque la demande d'accès au réseau de communication est initiée par l'émission d'un appel téléphonique à partir du premier terminal à destination du deuxième terminal, une valeur d'authentification d'émetteur d'appel est attribuée au champ d'authentification.

Il est ainsi possible, grâce à l'invention, d'authentifier par donnée biométrique un appel téléphonique d'un utilisateur.

Dans le cas d'une authentification positive, le serveur d'authentification renvoie le message MMS à un centre MMS qui achemine ledit message jusqu'aux premier et deuxième terminaux, le premier terminal émet l'appel téléphonique vers le deuxième terminal en réponse à la réception du message et le deuxième terminal notifie l'authentification de l'émetteur de l'appel téléphonique en réponse à la détection de la

valeur d'authentification d'émetteur d'appel attribuée au champ d'authentification présent dans l'en-tête du message MMS.

L'émission effective de l'appel téléphonique est ainsi subordonnée à l'authentification préalable de l'utilisateur émetteur de l'appel.

La présente invention concerne également un système d'authentification d'utilisateurs dans un réseau de communication comprenant au moins un premier terminal et un second terminal en liaison avec un centre MMS,

caractérisé en ce que ledit système comprend en outre un serveur d'authentification en liaison avec le centre MMS,

et en ce qu'au moins le premier terminal comprend des moyens pour, lors d'une demande d'accès au réseau de communication pour établir une communication avec le deuxième terminal, créer un message MMS dont le corps comprend au moins une page ("slide") contenant une donnée biométrique d'authentification de l'utilisateur du premier terminal et pour insérer un champ d'authentification dans l'en-tête du message,

le centre MMS comprenant des moyens pour rediriger automatiquement le message MMS vers le serveur d'authentification en réponse à la détection du champ d'authentification, et

le serveur d'authentification comprenant des moyens pour comparer la donnée biométrique reçue avec le message MMS avec une donnée biométrique de référence préenregistrée.

Comme pour le procédé décrit précédemment, le système de l'invention apporte une solution à l'émetteur d'un message ou d'un appel téléphonique pour s'authentifier de manière sûre auprès de ses correspondants.

Lorsque la demande d'accès au réseau de communication est initiée par l'envoi d'un message MMS à partir du premier terminal à destination du deuxième terminal, le premier terminal comprend des moyens pour attribuer une valeur d'authentification d'émetteur de message au champ d'authentification, le corps du message MMS comprenant en outre les éléments multimédias du message MMS à envoyer.

En cas d'authentification positive, le serveur d'authentification comprend des moyens pour renvoyer le message MMS au centre MMS de manière à permettre l'acheminement dudit message MMS jusqu'au

deuxième terminal qui comprend des moyens pour notifier l'authentification de l'émetteur dudit message MMS reçu en réponse à la détection de la valeur d'authentification d'émetteur de message attribuée au champ d'authentification présent dans l'en-tête du message.

Lorsque la demande d'accès au réseau de communication est initiée par l'émission d'un appel téléphonique à partir du premier terminal à destination du deuxième terminal, le premier terminal comprend des moyens pour générer un message MMS (dans lequel sera inclus la donnée biométrique qui sera utilisée pour l'authentification) et attribuer dans celui-ci une valeur d'authentification d'émetteur d'appel au champ d'authentification.

En cas d'authentification positive, le serveur d'authentification comprend des moyens pour renvoyer le message MMS au centre MMS de manière à acheminer ledit message jusqu'aux premier et deuxième terminaux, le premier terminal comprenant des moyens pour émettre l'appel téléphonique vers le deuxième terminal en réponse à la réception du message, le deuxième terminal comprenant des moyens pour notifier l'authentification de l'émetteur de l'appel téléphonique en réponse à la détection de la valeur d'authentification d'émetteur d'appel attribuée au champ d'authentification présent dans l'en-tête du message MMS.

La présente invention concerne encore un programme client MMS destiné à être embarqué sur un terminal comprenant des instructions pour permettre la composition, l'envoi et la réception de messages MMS, caractérisé en ce qu'il comprend en outre des instructions pour, lors d'une demande d'accès au réseau de communication pour établir une communication avec un autre terminal, créer un message MMS dont le corps comprend au moins une page ("slide") contenant une donnée biométrique d'authentification de l'utilisateur du terminal et pour insérer un champ d'authentification dans l'en-tête du message.

Un tel client MMS, une fois embarqué dans un terminal, offre à son utilisateur les outils pour s'authentifier auprès de ses correspondants lorsqu'il accède au réseau pour leur envoyer un message ou émettre un appel téléphonique.

Lorsque la demande d'accès au réseau de communication est initiée par l'envoi d'un message MMS, le programme comprend en outre des

instructions pour attribuer une valeur d'authentification d'émetteur de message au champ d'authentification.

Le programme peut comprendre en outre des instructions pour notifier l'authentification de l'émetteur d'un message MMS en réponse à la détection d'une valeur d'authentification d'émetteur de message du champ d'authentification présent dans l'en-tête dudit message.

Lorsque la demande d'accès au réseau de communication est initiée par l'émission d'un appel téléphonique, le programme comprend en outre des instructions pour attribuer une valeur d'authentification d'émetteur d'appel au champ d'authentification.

Le programme peut comprendre en outre des instructions pour, lors de la réception du message MMS, émettre l'appel téléphonique en réponse à la détection de la valeur d'authentification d'émetteur d'appel du champ d'authentification présent dans l'en-tête dudit message et des instructions pour notifier l'authentification de l'émetteur d'un appel téléphonique en réponse à la détection d'une valeur d'authentification d'émetteur d'appel du champ d'authentification présent dans l'en-tête dudit message.

Enfin, l'invention se rapporte aussi à un terminal mobile ou fixe comprenant un programme client MMS tel que décrit précédemment.

Brève description des dessins

Les caractéristiques et avantages de la présente invention ressortiront mieux de la description suivante, faite à titre indicatif et non limitatif, en regard des dessins annexés sur lesquels :

- la figure 1 est une vue schématique d'une architecture réseau dans laquelle sont mis en œuvre un système et un procédé d'authentification conformément à l'invention,
- la figure 2 montre la structure d'un message multimédia MMS,
- la figure 3 est un ordinogramme d'un mode de mise en œuvre d'un procédé d'authentification lors de l'envoi d'un message MMS conformément à un mode de réalisation de l'invention,

- la figure 4 est un ordinogramme montrant les étapes réalisées lors de l'émission d'un message MMS avec authentification à partir du terminal de l'émetteur conformément à l'invention,
- la figure 5 est un ordinogramme montrant les étapes réalisées par un centre MMS lors de la transmission d'un message MMS avec authentification conformément à l'invention,
- la figure 6 est un ordinogramme montrant les étapes réalisées par un centre d'authentification MMS lors de la réception d'un message MMS conformément à l'invention,
- la figure 7 est un ordinogramme d'un mode de mise en œuvre d'un procédé d'authentification lors de l'émission d'un appel téléphonique conformément à un autre mode de réalisation de l'invention,
- la figure 8 est un ordinogramme montrant les étapes réalisées lors de l'émission d'un appel téléphonique avec authentification à partir du terminal de l'émetteur conformément à l'invention,
- la figure 9 est un ordinogramme montrant les étapes réalisées par un centre MMS lors de la transmission d'un message MMS d'authentification d'émetteur d'appel téléphonique conformément à l'invention,
- la figure 10 est un ordinogramme montrant les étapes réalisées par un centre d'authentification MMS lors de la réception d'un message MMS d'authentification d'émetteur d'appel téléphonique conformément à l'invention.

Description détaillée des modes de réalisation de l'invention

La présente invention propose une solution pour permettre à un utilisateur d'un réseau fixe et/ou mobile de communication (GSM, GPRS, UMTS, Internet, etc.) de s'identifier auprès de l'opérateur du réseau et, ainsi, de s'authentifier auprès des correspondants auxquels il souhaite envoyer un message (message MMS, SMS, email, etc.) ou vers lequel il souhaite émettre un appel vocal téléphonique.

Conformément à l'invention, lors d'une demande d'accès à un réseau de communication initiée par l'envoi d'un message ou d'un appel téléphonique depuis son terminal (téléphone mobile, Smartphone, PDA,

etc.), l'utilisateur envoie une donnée d'authentification biométrique qui permet à son opérateur de l'identifier de manière unique et, par conséquent, d'authentifier son message ou son appel auprès du ou des destinataires.

A cet effet, comme décrit plus loin en détail, l'invention utilise la technologie connue du service de messagerie multimédia dite MMS ("Multimedia Messaging Service") pour l'envoi de la donnée d'authentification biométrique de l'utilisateur. Par souci de simplification, la plupart des éléments utilisés dans la présente invention et relevant de cette technologie seront qualifiés avec le terme MMS (ex. message MMS).

La donnée biométrique d'authentification DBn considérée dans la présente invention correspond à toute information biométrique permettant d'identifier de façon unique une personne. Cette donnée peut être, par exemple, une empreinte digitale, iridienne ou vocale. Selon la donnée biométrique utilisée par l'opérateur pour l'authentification, le terminal de l'utilisateur sera équipé de moyens de saisie de cette donnée. Par exemple, le terminal de l'utilisateur pourra être équipé d'un capteur d'empreinte digitale, d'un capteur permettant la capture d'une photo de son iris, ou d'un enregistreur vocal permettant à l'utilisateur d'enregistrer une phrase type et du logiciel de biométrie associé. Les moyens de saisie biométriques sont biens connus et ne seront pas décrit plus en détail.

La figure 1 illustre une architecture dans laquelle l'invention peut être mise en œuvre. Cette architecture comprend un terminal 1 d'un utilisateur A, un terminal 3 d'un utilisateur B, un centre MMS 10 et un centre d'authentification 20. Le centre MMS 10 permet l'échange de messages MMS entre le terminal 1 de l'utilisateur A et le terminal 3 de l'utilisateur B à travers un réseau de communication R1 (ex. réseau GSM, GPRS ou UMTS). Le centre MMS 10 peut également échanger des messages MMS avec le centre d'authentification 20 via un réseau R2. Les terminaux 1 et 2 peuvent établir des communications téléphonique via un réseau R3. Les réseaux R1, R2 et R3 peuvent être des réseaux de communication fixes ou mobiles gérés par des opérateurs différents ou identiques.

Dans la suite de la description, l'utilisateur A sera considéré comme l'émetteur du message ou de l'appel téléphonique et l'utilisateur B le destinataire du message ou de l'appel.

Le centre MMS 10 gère le routage des messages MMS aussi bien dans l'environnement MMS auquel il appartient que vers d'autres environnements MMS ou d'autres serveurs de messagerie. De façon connue, le centre MMS est constitué d'un ou plusieurs serveurs comprenant des modules (logiciels) permettant le traitement des messages MMS (ex. routage, stockage, adaptation).

Le centre MMS est en outre en liaison avec des services à valeur ajoutée ("VAS Applications"), une base de données pour la gestion des abonnés et de leur localisation (par exemple : HLR pour "Home Location Register" pour le réseau mobile), des systèmes de facturation, et des bases de données d'informations sur les utilisateurs MMS (ex. informations de présence) (non représentés sur la figure 1).

Ces éléments réseau sous le contrôle d'un fournisseur de service de messagerie multimédia ("MMS content provider") permettent l'accès aux services MMS à des utilisateurs abonnés via un réseau de télécommunication.

Les différentes entités d'un système d'échange de messages MMS communiquent à travers un ensemble d'interfaces dédiées, à savoir:

- L'interface MM1 qui permet l'échange entre un client MMS embarqué sur un terminal et un centre MMS;
- L'interface MM2 est l'interface utilisée entre les entités de routage (MMS relay) et de stockage (MMS server) du centre MMS. La plupart des solutions des fournisseurs intègrent les deux entités dans le même équipement rendant cette interface propriétaire (i.e. non normalisée);
- L'interface MM3 permet à un centre MMS d'échanger des messages avec d'autres serveurs de messagerie;
- L'interface MM4 permet l'échange de messages MMS entre deux centres MMS appartenant à deux environnements MMS différents;
- L'interface MM5 permet au centre MMS d'interroger la base de données de gestion des abonnés;

- L'interface MM6 permet au centre MMS d'accéder à la base de données d'informations sur les usagers MMS;
- L'interface MM7/SOAP permet le transfert de messages MMS d'un centre MMS vers des services à valeur ajoutée (fournisseur de contenus) et inversement;
- L'interface MM8 permet au centre MMS d'interagir avec les systèmes de facturation.

L'architecture d'un système d'échange de messages MMS est bien connue en soi et ne sera pas décrit plus en détail pour ne pas alourdir inutilement la présente description. On pourra toutefois se reporter notamment aux documents publiés par l'organisme de standardisation pour les systèmes mobiles de troisième génération 3GPP (www.3gpp.org).

Concernant les terminaux 1 et 3, ceux-ci doivent être équipés d'un client MMS 2, respectivement 4 qui est embarqué dans le terminal. Le client MMS (encore appelé MMS-UA pour "MMS User Agent") est un logiciel d'application utilisateur embarqué sur le terminal qui permet la composition, la présentation, l'envoi et la réception des messages MMS. Les clients MMS 2 et 4 sont attachés à un environnement MMS correspondant au réseau R1 (ex. GSM, GPRS ou UMTS) d'abonnement du terminal émetteur et récepteur.

Conformément à l'invention, les clients MMS 2 et 4 des terminaux 1 et 3 comprennent en outre des instructions pour intégrer une donnée biométrique d'authentification dans un message MMS et envoyer ce message MMS en intégrant un champ d'authentification dans l'en-tête du message.

En effet, l'authentification d'un utilisateur par transmission d'une donnée biométrique dans un message MMS selon la présente invention doit pouvoir s'intégrer dans des environnements MMS existants. A cet effet, comme décrit plus loin en détail, on ajoute un champ spécifique "Authentification Mode" dans les messages MMS qui, en fonction de sa valeur, va permettre au centre MMS 10 et au centre d'authentification 20 de traiter de façon particulière ce message pour réaliser l'authentification de l'utilisateur.

De façon connue et tel qu'illustré sur la figure 2, un message MMS comporte un en-tête MMS-H et un corps MMS-B. L'en-tête MMS-H du

message MMS contient des informations relatives au transport du message, telles que, par exemple, l'identification du destinataire, de l'émetteur et des informations relatives au message envoyé (date d'envoi, date de validité du message, objet du message, etc.). Les informations de l'en-tête MMS-H sont organisées selon des champs auxquels sont attribuées des valeurs.

Le corps MMS-B du message peut contenir une ou plusieurs pages SL1 à SLn couramment appelés "slides". Dans un message, les pages ("slides") sont en général définis en langage "SMIL" (Synchronized Multimedia Integration Language) normalisé, ce langage permettant la synchronisation des différents éléments contenus dans le message. Les "slides" peuvent éventuellement être définis par un langage spécifique au terminal.

Chacune des pages SL1 à SLn du corps d'un message MMS contient un ou plusieurs éléments multimédia tels qu'un son, une image, un texte, etc. Le corps d'un message MMS est, par conséquent, composé d'une succession de pages SL1 à SLn chacune comprenant un ou plusieurs éléments multimédia (son, image, texte, etc.), la nature de chacun étant déterminée par un identifiant.

La donnée biométrique d'authentification DBn de l'utilisateur est insérée dans une page déterminée du message MMS (par exemple la dernière).

Enfin, comme expliqué plus loin, le client MMS de chaque terminal comprend conformément à l'invention, des instructions pour, en fonction de la valeur du champ d'authentification présent dans l'en-tête du message MMS reçu, informer l'utilisateur destinataire du message ou de l'appel téléphonique de l'authentification de l'utilisateur émetteur.

Le centre d'authentification 20 comprend des moyens de traitement, comme par exemple un serveur 21, en liaison avec le réseau de communication R2 et une unité de stockage 22 dans laquelle sont mémorisées les données biométriques de références de tous les utilisateurs enregistrés auprès du service d'authentification. Le serveur 21 est programmé pour, lorsqu'il reçoit un message MMS avec une donnée biométrique d'authentification DBn, comparer cette donnée avec la donnée

biométrique de référence DBref correspondant à l'identité de l'utilisateur indiquée comme émetteur du message MMS.

On décrit maintenant en relation avec la figure 3 un premier exemple de mise en œuvre du procédé d'authentification d'un utilisateur conformément à l'invention dans le cas où ce dernier souhaite envoyer un message MMS à un autre utilisateur. Dans cet exemple, l'utilisateur A de la figure 1 envoie un message MMS à l'utilisateur B.

La première étape (étape S1) consiste à composer et à envoyer un message MMS.

Plus précisément et tel qu'illustré sur la figure 4, l'utilisateur A compose de manière classique sur son terminal un message MMS M1 qu'il souhaite envoyer à l'utilisateur B (étape S11). Cette opération consiste pour l'utilisateur à renseigner l'adresse de l'utilisateur destinataire du message et à éditer les éléments multimédias qu'il souhaite transmettre avec le message.

Après cette composition, lors de la demande d'accès au réseau de communication (par exemple le réseau R1), c'est-à-dire lorsque l'utilisateur A décide d'envoyer son message (lorsqu'il appuie sur le bouton "*Envoyer*" par exemple), le terminal 1 effectue automatiquement les actions/traitements suivants:

- saisie de la donnée biométrique d'authentification DBn de l'utilisateur A (par exemple empreinte digitale, iridienne ou vocale) (étape S12),
- ajout d'une nouvelle page ("slide") SLn dans le message MMS M1 (ici en dernière position dans le corps du message) et insertion dans cette page de la donnée biométrique d'authentification DBn (étape S13),
- ajout, dans l'en-tête du message MMS M1 du champ "Authentification-Mode" à la valeur 1 (étape S14),
- envoie du message MMS M1 ainsi constitué à destination du terminal 3 de l'utilisateur B en utilisant l'architecture MMS, c'est-à-dire l'interface MM1 entre le terminal 3 et centre MMS 10 de l'opérateur par lequel transite le message (étape S15).

La figure 5 décrit les étapes de traitement réalisées par le centre MMS lorsqu'il reçoit le message MMS M1. Une fois le message MMS M1

reçu par le centre MMS 10 (étape S21), ce dernier détermine si un champ d'authentification ("Authentification-Mode") est présent dans l'en-tête du message (étape S22). Si ce n'est pas le cas, le message MMS M1 sera traité comme un message MMS classique (étape S23), c'est-à-dire directement acheminé à son destinataire, ici l'utilisateur B. Si un champ d'authentification est présent dans l'en-tête du message MMS M1, le centre MMS 10 vérifie la valeur attribuée à ce champ (étape S24). Si la valeur indique qu'il n'y a pas de page contenant une donnée biométrique d'authentification (ex. champ "Authentification-Mode"=0), le message MMS M1 sera traité comme un message MMS classique (étape S23). Si, au contraire, la valeur du champ correspond à une indication qu'une page SLn contenant une donnée biométrique est présente dans le message (ex. champ "Authentification-Mode"=1), le centre MSS 10 transmet le message au serveur 21 du centre d'authentification 20 via l'interface MM7/SOAP (étape S25 et étape S2 de la figure 3).

A la réception du message MMS M1, le serveur 21 du centre d'authentification effectue les traitements spécifiques à l'authentification de l'utilisateur A.

Plus précisément et tel qu'illustré sur la figure 6, une fois le message reçu (étape S31), le serveur 21 extrait la donnée biométrique DBn contenue dans la dernière page (slide) du message MMS M1 (étape S32). Il extrait également à partir de l'identifiant de l'émetteur (cet identifiant peut être soit son numéro de téléphone si l'émetteur est utilisateur d'un réseau de téléphonie mobile ou fixe, soit son adresse e-mail si l'émetteur est utilisateur d'un réseau internet) indiqué dans le message MMS M1 la donnée biométrique de référence DBref enregistrée au nom de l'utilisateur A dans l'unité de stockage 22 (étape S33).

Le serveur 21 détermine ensuite par comparaison si ces deux données biométriques proviennent du même utilisateur (étape S34). Si les deux données biométriques correspondent (DBn=DBref), l'utilisateur A est identifié et le serveur 21 supprime la dernière page SLn du message MMS M1 contenant la donnée biométrique (étape S35) puis renvoie le message au centre MMS 10 (étape S36 et étape S3 sur la figure 3). Dans l'autre cas, c'est-à-dire si la donnée biométrique d'authentification reçue ne correspond pas à la donnée biométrique de référence enregistrée pour

l'utilisateur A, le serveur 21 envoie un message SMS à l'utilisateur A lui signalant l'échec de son authentification et bloque le message MMS M1 (étape S37). Les traitements du serveur 21 pour le message MMS M1 sont alors terminés (étape S38)

Comme indiqué précédemment, dans le cas d'une authentification positive, le centre MMS 10 reçoit le message MMS M1 renvoyé par le serveur 21 du centre d'authentification 20 (étape S3). Le centre MMS 10 achemine alors le message MMS M1 vers le terminal 4 de l'utilisateur B (étape S4). Le client MMS 4 du terminal 3 détecte le champ "Authentification-Mode" présent à la valeur 1 dans l'en-tête du message et informe l'utilisateur B que l'émetteur du message, l'utilisateur A, a bien été authentifié par l'opérateur (par exemple en affichant une icône spécifique à l'écran du terminal) (étape S5). Le message MMS M1 est ensuite joué de façon classique sur le terminal 3 de l'utilisateur B (étape S6).

Le champ d'authentification "Authentification-Mode" inséré dans l'en-tête du message MMS peut prendre trois valeurs, à savoir 0, 1 (valeurs spécifiques aux messages MMS) ou 2 (valeur spécifique aux appels téléphoniques).

En fonction de la valeur de ce champ le réseau de l'opérateur, c'est-à-dire le centre MMS 10 et le centre d'authentification 20, et le terminal du destinataire effectuent des actions différentes sur les messages MSS qui sont respectivement indiquées dans les deux tableaux ci-dessous.

Valeur du champ "Authentification-Mode"	***Traitements du message par le réseau de l'opérateur de l'émetteur du message (utilisateur A)***
0	Cas d'un message MMS "classique" : le centre MMS de l'opérateur traite le message de manière classique (comme défini dans les normes MMS), c'est-à-dire en acheminant le message directement au destinataire (utilisateur B).
1	Le centre MMS envoie automatiquement le message au centre d'authentification qui effectue les traitements nécessaires à l'authentification tels que décrits précédemment en relation avec la figure 5, puis, en cas d'authentification positive, renvoie le message au centre MMS qui l'achemine à son destinataire.

Valeur du champ "Authentification-Mode"	***Traitements du message par le terminal du destinataire (utilisateur B)***
0	Cas d'un message MMS "classique" : le message est joué sur le terminal.
1	Le terminal destinataire informe son utilisateur que l'émetteur (utilisateur A) a été authentifié. Le message MMS est ensuite joué sur le terminal.

Lorsque le champ "Authentification-Mode" est absent de l'en-tête du message MMS, ce dernier est traité de manière classique par le centre MMS et le terminal du destinataire.

On décrit maintenant en relation avec la figure 7 un deuxième exemple de mise en œuvre du procédé d'authentification d'un utilisateur conformément à l'invention dans le cas où ce dernier souhaite émettre un

appel téléphonique vers un autre utilisateur. Dans cet exemple, l'utilisateur A de la figure 1 appelle l'utilisateur B.

Lorsque l'utilisateur A initie une demande d'accès au réseau de communication (par exemple le réseau R3) pour établir une communication téléphonique avec l'utilisateur B en composant, par exemple, de manière classique sur son terminal le numéro d'appel téléphonique de B et en appuyant sur le bouton *"Appeler"* (étape S10), le terminal 1 effectue automatiquement, comme indiqué sur la figure 8, les actions/traitements suivants:

- saisie de la donnée biométrique d'authentification DBn de l'utilisateur A (par exemple empreinte digitale, iridienne ou vocale) (étape S41),
- création d'un message MMS M2 contenant une seule page (SL1) (étape S42),
- insertion dans cette page de la donnée biométrique d'authentification DBn (étape S43),
- ajout, dans l'en-tête du message MMS M2 du champ "Authentification-Mode" à la valeur 2 (étape S44),
- envoie du le message MMS M2 ainsi constitué à destination du terminal 3 de l'utilisateur B en utilisant l'architecture MMS, c'est-à-dire l'interface MM1 entre le terminal 3 et centre MMS 10 de l'opérateur par lequel transite le message (étape S45 et S20 de la figure 7).

La figure 9 décrit les étapes de traitement réalisées par le centre MMS lorsqu'il reçoit le message MMS M2. Une fois le message MMS M2 reçu par le centre MMS 10 (étape S51), ce dernier détecte la présence du champ d'authentification "Authentification-Mode" présent dans l'en-tête du message ainsi que la valeur 2 attribuée à ce champ (étape S52) et transmet le message au serveur 21 du centre d'authentification 20 via l'interface MM7/SOAP (étape S53 et étape S30 de la figure 7).

A la réception du message MMS M2, le serveur 21 du centre d'authentification effectue les traitements spécifiques à l'authentification de l'utilisateur A.

Plus précisément et tel qu'illustré sur la figure 10, une fois le message reçu (étape S61), le serveur 21 extrait la donnée biométrique

DBn contenue dans la page SL1 (slide) du message MMS M2 (étape S62). Il extrait également à partir de l'identifiant de l'émetteur (cet identifiant peut être soit son numéro de téléphone si l'émetteur est utilisateur d'un réseau de téléphonie mobile ou fixe, soit son adresse e-mail si l'émetteur est utilisateur d'un réseau internet) indiqué dans le message MMS M2 la donnée biométrique de référence DBref enregistrée au nom de l'utilisateur A dans l'unité de stockage 22 (étape S63).

Le serveur 21 détermine ensuite par comparaison si ces deux données biométriques proviennent du même utilisateur (étape S64). Si les deux données biométriques correspondent, l'utilisateur A est identifié et le serveur 21 supprime la page SL1 du message MMS M2 contenant la donnée biométrique (étape S65) puis renvoie le message MMS 2 au centre MMS 10 (étape S66 et étape S40 sur la figure 3). Dans l'autre cas, c'est-à-dire si la donnée biométrique d'authentification reçue ne correspond pas à la donnée biométrique de référence enregistrée pour l'utilisateur A, le serveur 21 envoie un message SMS à l'utilisateur A lui signalant l'échec de son authentification et bloque le message MMS M2 (étape S67). Les traitements du serveur 21 du message MMS M2 sont alors terminés (étape S68).

Lorsque l'authentification est positive (DBn=DBref), deux cas se distinguent:

- dans le cas où le champ d'authentification "Authentification-Mode" de l'en-tête du message est positionné à 1 (cas où l'utilisateur A souhaite envoyé un message MMS authentifié): le serveur 21 envoie le message MMS M1 débarrassé de la page SLn, à destination de B et ayant comme champ origine le numéro de A (étape S3, figure 3).
- dans le cas où le champ d'authentification "Authentification-Mode" de l'en-tête du message est positionné à 2 comme dans l'exemple considéré ici (cas où l'utilisateur A souhaite émettre un appel téléphonique authentifié): le serveur 21 envoie le message MMS M2 débarrassé de la page SL1, à destination de B et ayant comme champ origine le numéro de A (étape S40). Le

serveur 21 envoie également un second message MMS M2 débarrassé de la page SL1, à destination de A et ayant comme champ origine le numéro de B (étape S40').

Le centre MMS 10 achemine le premier message MMS M2 vers le terminal 4 de l'utilisateur B (étape S50) et le second message MMS M2 vers le terminal 1 de l'utilisateur A (étape S60).

Lorsqu'il reçoit le message MMS M2, le client MMS 2 du terminal 1 déclenche l'émission de l'appel téléphonique vers le terminal 3 de l'utilisateur B (étape S70) (le message MMS M2 reçu par A a le champ "Authentification-Mode" dans son en-tête positionné à 2 et l'émetteur du message indiqué est B)

De son côté, le terminal 3 de l'utilisateur B reçoit le message MMS M2 et la demande d'appel provenant du terminal 1 de l'utilisateur A. Le terminal 3 informe l'utilisateur B qu'il a une demande d'appel (en sonnant par exemple) tandis que le client MMS 4 du terminal 3, qui a détecté le champ "Authentification-Mode" présent à la valeur 2 dans l'en-tête du message, informe en même temps l'utilisateur B que l'émetteur du message, l'utilisateur A, a bien été authentifié par l'opérateur (par exemple en affichant une icône spécifique à l'écran du terminal) (étape S80). L'utilisateur B peut alors prendre l'appel téléphonique de façon classique sur son terminal 3 (étape S90).

Dans le cas de l'émission d'un appel téléphonique, le champ d'authentification "Authentification-Mode" inséré dans l'en-tête du message MMS ne peut prendre que la valeur 2.

Les trois tableaux ci-dessous indiquent les actions réalisées par respectivement le réseau de l'opérateur (c'est-à-dire le centre MMS et le centre d'authentification), le terminal de l'émetteur de l'appel et le terminal du destinataire de l'appel lors de la réception d'un message avec un champ "Authentification-Mode" positionné à 2.

Valeur du champ "Authentification-Mode"	***Traitements du message par le réseau de l'opérateur de l'émetteur du message (utilisateur A)***
2	Le centre MMS envoie automatiquement le message au centre d'authentification qui effectue les traitements nécessaires à l'authentification tels que décrits précédemment en relation avec la figure 10, puis, en cas d'authentification positive, renvoie le message au centre MMS qui l'achemine à son émetteur et à son destinataire.

Valeur du champ "Authentification-Mode"	***Traitements du message par le terminal de l'émetteur (utilisateur A)***
2	Lorsqu'il reçoit le message, le terminal de l'émetteur (utilisateur A) émet l'appel vers le destinataire (utilisateur B).

Valeur du champ "Authentification-Mode"	***Traitements du message par le terminal du destinataire (utilisateur B)***
2	Lorsqu'il reçoit le message et la demande d'appel téléphonique, le terminal destinataire informe son utilisateur (utilisateur B) qu'il a une demande d'appel et que son émetteur (utilisateur A) a été authentifié.

Le processus d'authentification étant initié par l'envoi d'un message MMS par le client MMS du terminal de l'émetteur d'un message ou d'un appel téléphonique, le client MMS peut comprendre en outre des moyens pour activer/désactiver cette fonctionnalité, par exemple en permettant à

l'utilisateur de sélectionner/désélectionner cette fonctionnalité dans un menu affiché à l'écran. Lorsque cette fonctionnalité n'est pas activée, le client MMS n'envoie pas de message MMS avec une donnée biométrique d'authentification et un champ d'authentification et son utilisateur ne sera pas authentifié.

Par ailleurs, lorsqu'il s'inscrit au service d'authentification de la présente invention, l'utilisateur doit fournir à son opérateur une donnée biométrique qui sera enregistrée en tant que donnée biométrique de référence dans l'unité de stockage du centre d'authentification de l'opérateur. Cette donnée biométrique de référence peut être, par exemple, envoyée par l'utilisateur par message MMS au serveur du centre d'authentification lors de son inscription au service.

La présente invention est décrite en relation avec des systèmes d'échange de messages MMS comprenant des terminaux mobiles. Toutefois, ces systèmes peuvent aussi comprendre des terminaux fixes aptes à envoyer/recevoir des messages MMS. A cet effet, il suffit que le terminal fixe soit équipé d'un client MMS similaire à celui embarqué sur les terminaux mobiles.

Dans le cas d'une authentification lors de l'envoi d'un message, le procédé et le système de l'invention ne sont pas limités seulement au cas d'envoi d'un message MMS comme décrit précédemment mais à l'envoi de tout type de message et en particulier les messages SMS et les courriels ou emails.

Dans le cas de l'envoi d'un message SMS, le terminal de l'émetteur du message envoie un message MMS composé de deux pages:

- une première page contenant le texte que souhaite envoyer l'émetteur correspondant au message SMS, et
- une seconde page contenant la donnée biométrique d'authentification (le message MMS contenant en outre dans son en-tête un champ "Authentification-Mode" positionné à 1 comme décrit précédemment).

Dans le cas de l'envoi d'un email, le terminal de l'émetteur du message envoie un message MMS composé de deux pages:

- les N-1 premières pages contenant les différents éléments contenus dans l'email à transmettre (en particulier, le texte de l'email est contenu dans la première page), et
- la $N^{ième}$ page contenant la donnée biométrique d'authentification (le message MMS contenant en outre dans son en-tête un champ "Authentification-Mode" positionné à 1 comme décrit précédemment).

Enfin, de manière optionnelle, le serveur du centre d'authentification peut être dotée d'un compteur d'échecs successifs d'authentification pour un même utilisateur et comprendre des instructions pour, au-delà d'un nombre successif d'échecs déterminé, interdire systématiquement tout message ou appel pour cet utilisateur et inviter ce dernier à contacter son service client dans un message SMS.

REVENDICATIONS

1. Procédé d'authentification comprenant une étape de demande d'accès à un réseau de communication (R1; R3) par un utilisateur (A) équipé d'un premier terminal (1) apte à établir une communication avec au moins un deuxième terminal (3),

caractérisé en ce que le procédé comprend en outre:

- une étape de création d'un message MMS (M1; M2), ledit message (M1; M2) comprenant un corps et un en-tête, ledit corps comprenant au moins une page (SLn) contenant une donnée biométrique d'authentification (DBn) de l'utilisateur (A) du premier terminal (1),
- une étape d'insertion d'un champ d'authentification dans l'en-tête du message (M1; M2),
- une étape d'envoi dudit message (M1; M2) à destination du deuxième terminal (3),
- une étape d'envoi du message MMS (M1; M2) vers un serveur d'authentification (21) en réponse à une détection du champ d'authentification, et
- une étape d'authentification dans laquelle le serveur d'authentification (21) compare la donnée biométrique d'authentification (DBn) reçue avec une donnée biométrique de référence préenregistrée (DBrefn).

2. Procédé selon la revendication 1, caractérisé en ce que, lorsque la demande d'accès au réseau de communication (R1) est initiée par l'envoi d'un message MMS par l'utilisateur (A) à partir du premier terminal (1) à destination du deuxième terminal (3), une valeur d'authentification d'émetteur de message est attribuée au champ d'authentification, le corps du message MMS (M1) comprenant en outre les éléments multimédias du message MMS que l'utilisateur souhaite envoyer.

3. Procédé selon la revendication 2, caractérisé en ce que, en cas d'authentification positive, le serveur d'authentification (21) renvoie le message MMS (M1) à un centre MMS (10) qui achemine ledit message MMS jusqu'au deuxième terminal (3) et en ce que ledit deuxième terminal

notifie l'authentification de l'émetteur dudit message MMS (M1) reçu en réponse à la détection de la valeur d'authentification d'émetteur de message attribuée au champ d'authentification présent dans l'en-tête du message MMS (M1).

4. Procédé selon la revendication 1, caractérisé en ce que, lorsque la demande d'accès au réseau de communication (R3) est initiée par l'émission d'un appel téléphonique à partir du premier terminal (1) à destination du deuxième terminal (3), une valeur d'authentification d'émetteur d'appel est attribuée au champ d'authentification.

5. Procédé selon la revendication 4, caractérisé en ce que, en cas d'authentification positive, le serveur d'authentification (21) renvoie le message MMS (M2) à un centre MMS (10) qui achemine ledit message jusqu'aux premier et deuxième terminaux (1, 3), et en ce que ledit premier terminal (1) émet l'appel téléphonique vers le deuxième terminal (3) en réponse à la réception dudit message, le deuxième terminal (3) notifiant l'authentification de l'émetteur de l'appel téléphonique en réponse à la détection de la valeur d'authentification d'émetteur d'appel attribuée au champ d'authentification présent dans l'en-tête du message MMS (M2).

6. Système d'authentification d'utilisateurs dans un réseau de communication (R1; R2) comprenant au moins un premier terminal (1) et un second terminal (3) en liaison avec un centre MMS (10),

caractérisé en ce que ledit système comprend en outre un serveur d'authentification (21) en liaison avec le centre MMS (10),

et en ce qu'au moins le premier terminal (1) comprend des moyens pour, lors d'une demande d'accès au réseau de communication (R1; R3) pour établir une communication avec le deuxième terminal (3), créer un message MMS (M1; M2) dont le corps comprend au moins une page (SLn) contenant une donnée biométrique d'authentification (DBn) de l'utilisateur du premier terminal et pour insérer un champ d'authentification dans l'en-tête du message,

le centre MMS (10) comprenant des moyens pour rediriger automatiquement le message MMS vers le serveur d'authentification (21) en réponse à la détection du champ d'authentification, et

le serveur d'authentification (21) comprenant des moyens pour comparer la donnée biométrique reçue (DBn) avec le message MMS (M1; M2) avec une donnée biométrique de référence préenregistrée (DBref).

7. Système selon la revendication 6, caractérisé en ce que le premier terminal (1) comprend des moyens pour, lorsque la demande d'accès au réseau de communication (R1) est initiée par l'envoi d'un message MMS à partir du premier terminal (1) à destination du deuxième terminal (3), attribuer une valeur d'authentification d'émetteur de message au champ d'authentification, le corps du message MMS (M1) comprenant en outre les éléments multimédias du message MMS à envoyer.

8. Système selon la revendication 7, caractérisé en ce que le serveur d'authentification (21) comprend des moyens pour, en cas d'authentification positive, renvoyer le message MMS (M1) au centre MMS (10) de manière à permettre l'acheminement dudit message MMS jusqu'au deuxième terminal (3) et en ce que ledit deuxième terminal comprend des moyens pour notifier l'authentification de l'émetteur dudit message MMS (M1) reçu en réponse à la détection de la valeur d'authentification d'émetteur de message attribuée au champ d'authentification présent dans l'en-tête du message MMS (M1).

9. Système selon la revendication 6, caractérisé en ce que le premier terminal (1) comprend des moyens pour, lorsque la demande d'accès au réseau de communication (R3) est initiée par l'émission d'un appel téléphonique à partir du premier terminal (1) à destination du deuxième terminal (3), attribuer une valeur d'authentification d'émetteur d'appel au champ d'authentification.

10. Système selon la revendication 9, caractérisé en ce que, le serveur d'authentification (21) comprend des moyens pour, en cas

d'authentification positive, renvoyer le message MMS (M2) au centre MMS (10) de manière à acheminer ledit message jusqu'aux premier et deuxième terminaux (1, 3), et en ce que ledit premier terminal (1) comprend des moyens pour émettre l'appel téléphonique vers le deuxième terminal (3) en réponse à la réception dudit message, le deuxième terminal (3) comprenant des moyens pour notifier l'authentification de l'émetteur de l'appel téléphonique en réponse à la détection de la valeur d'authentification d'émetteur d'appel attribuée au champ d'authentification présent dans l'en-tête du message MMS (M2).

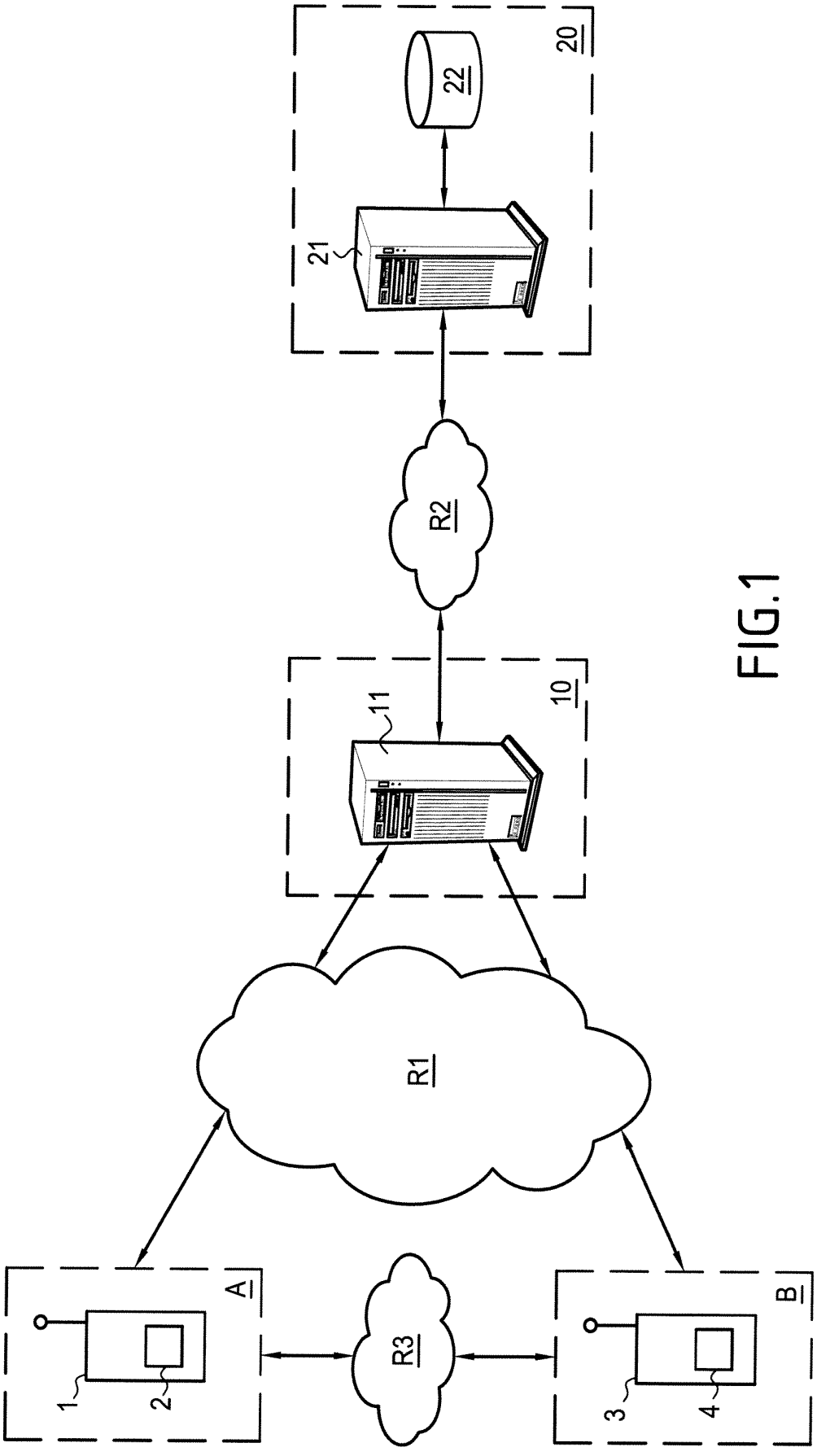


FIG.1

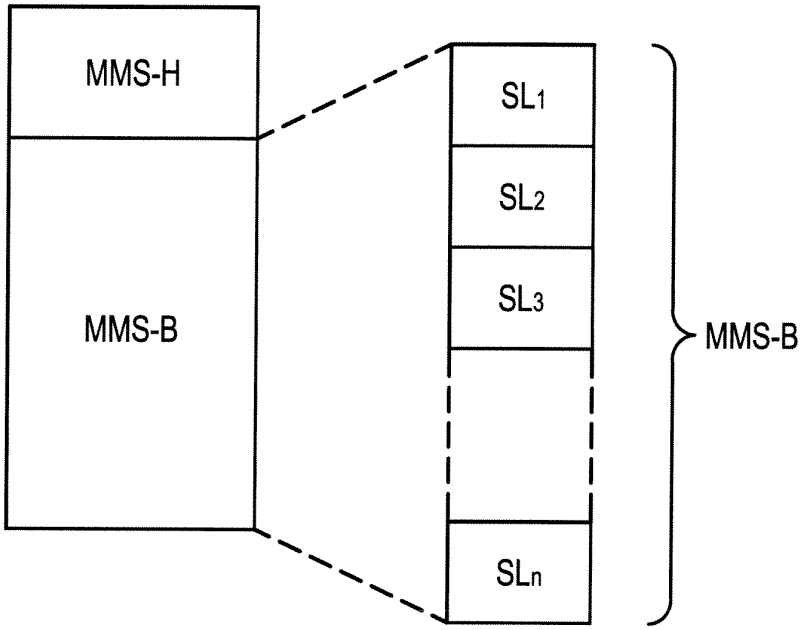


FIG.2

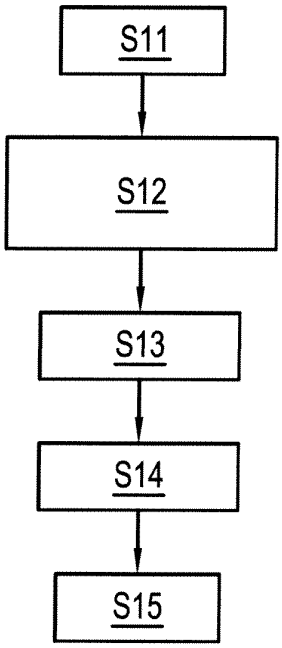


FIG.4

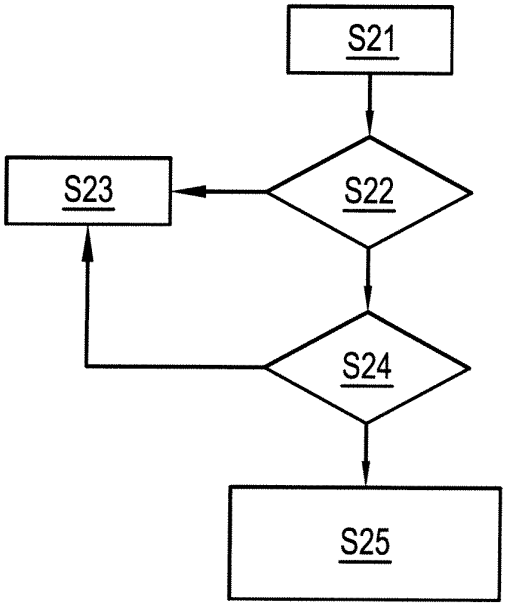


FIG.5

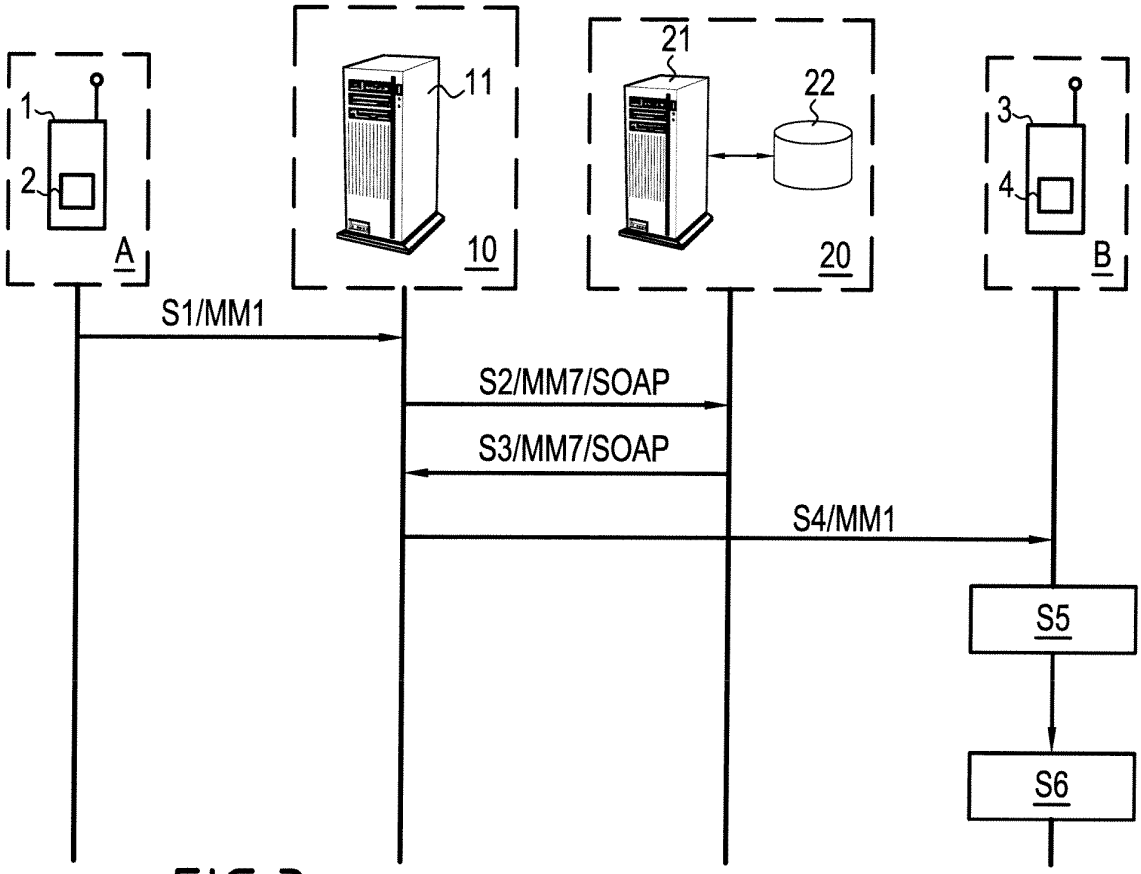
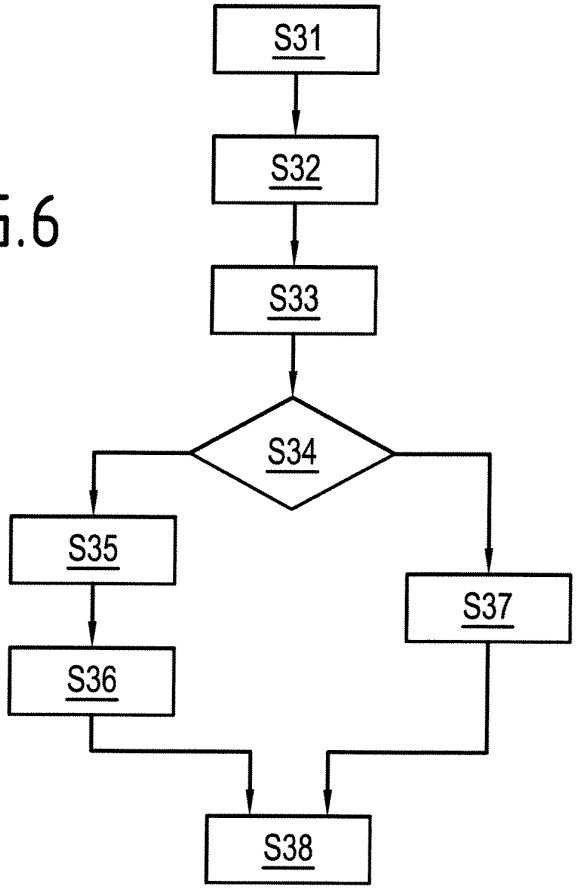

1
2
A
11
10
21
22
20
3
4
B
S1/MM1
S2/MM7/SOAP
S3/MM7/SOAP
S4/MM1
S5
S6

FIG.3

FIG.6


S31
S32
S33
S34
S35
S36
S37
S38

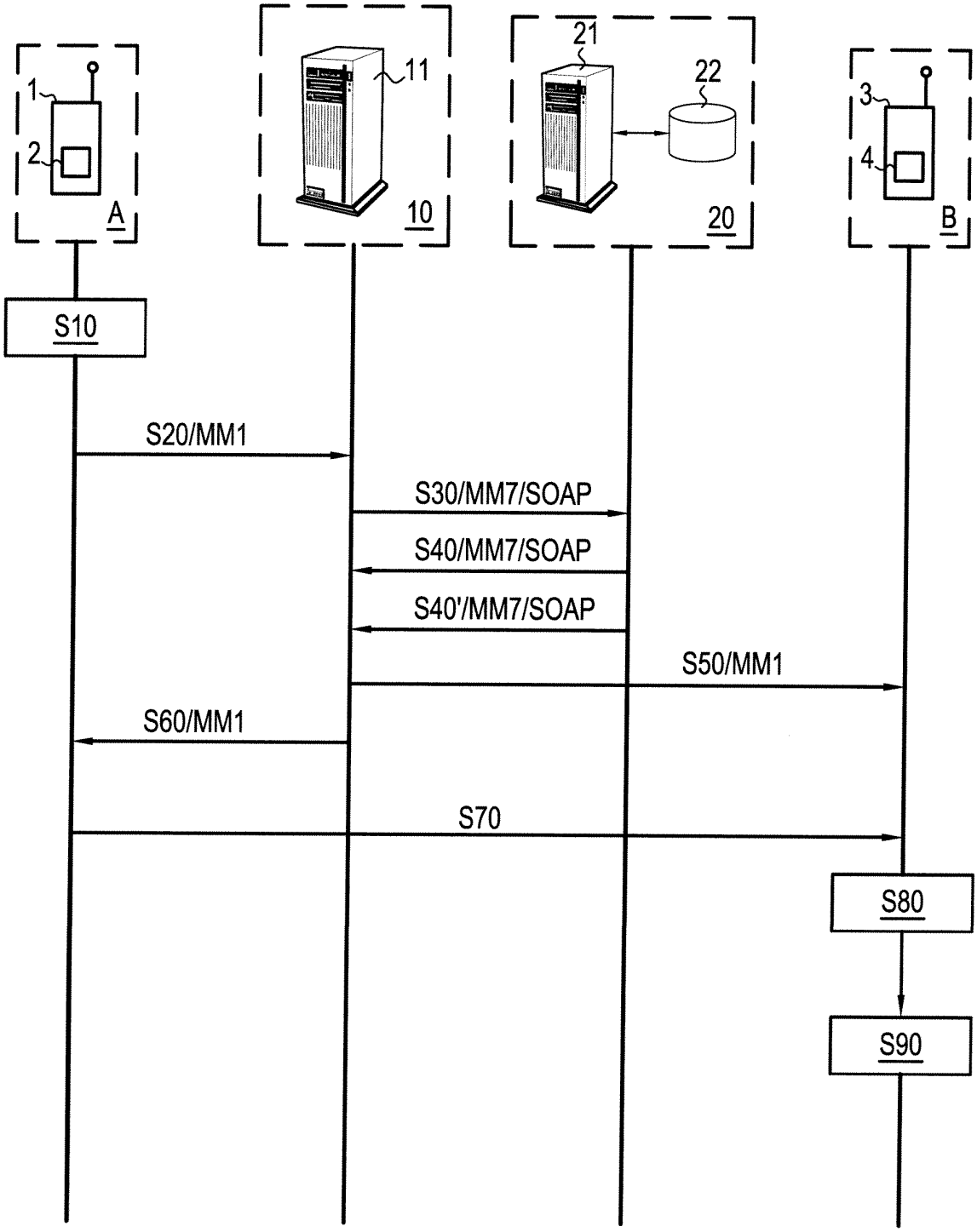

1
2
A
11
10
21
22
20
3
4
B
S10
S20/MM1
S30/MM7/SOAP
S40/MM7/SOAP
S40'/MM7/SOAP
S50/MM1
S60/MM1
S70
S80
S90

FIG.7

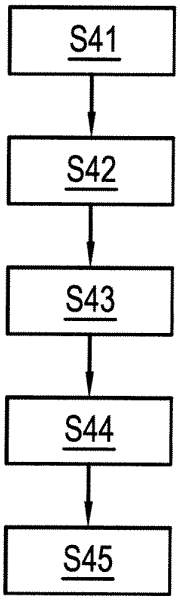


FIG.8

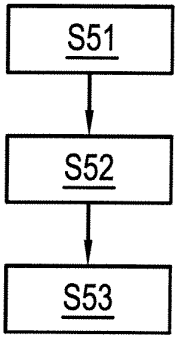
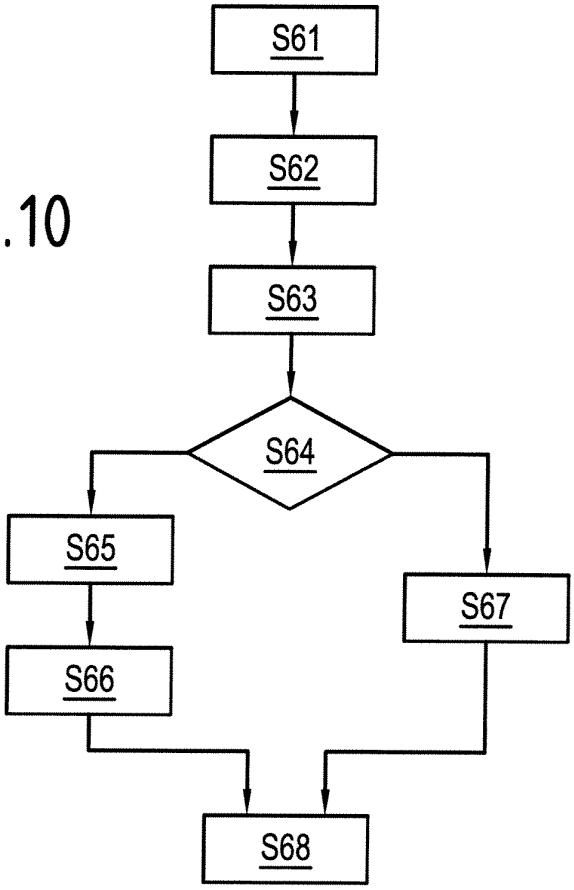


FIG.9

FIG.10



RÉPUBLIQUE FRANÇAISE

2904902

INSTITUT NATIONAL DE LA PROPRIÉTÉ INDUSTRIELLE

RAPPORT DE RECHERCHE PRÉLIMINAIRE

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

N° d'enregistrement national

FA 683786
FR 0653362

DOCUMENTS CONSIDÉRÉS COMME PERTINENTS		Revendication(s) concernée(s)	Classement attribué à l'invention par l'INPI
Catégorie	Citation du document avec indication, en cas de besoin, des parties pertinentes		
X	GB 2 398 707 A (SCHLUMBERGER HOLDINGS [VG]) 25 août 2004 (2004-08-25) * abrégé * * page 4, ligne 3 - page 5, ligne 22 * * figures 1,2 *	1-17	H04L9/32 H04L12/58 G06F21/00 G06K9/00 H04Q7/32
A	US 2004/225878 A1 (COSTA-REQUENA JOSE [FI] ET AL) 11 novembre 2004 (2004-11-11) * abrégé * * alinéa [0064] - alinéa [0071] *	1-17	
A	US 2006/048212 A1 (TSURUOKA YUKIO [JP] ET AL) 2 mars 2006 (2006-03-02) * abrégé * * alinéa [0047] - alinéa [0049] *	1-17	
A	AJIT JAOKAR: "Multimedia Messaging and SMIL" SMIL EUROPE 2003, [Online] 12 février 2003 (2003-02-12), - 14 février 2003 (2003-02-14) XP002434658 Paris Extrait de l'Internet: URL:http://www.aristote.asso.fr/SMIL2002/P/Jackar.pdf> [extrait le 2007-05-23] * le document en entier *	1-17	

DOMAINES TECHNIQUES RECHERCHÉS (IPC)

H04L

Date d'achèvement de la recherche	Examinateur
23 mai 2007	Bertolissi, Edy

CATÉGORIE DES DOCUMENTS CITÉS

X : particulièrement pertinent à lui seul
Y : particulièrement pertinent en combinaison avec un autre document de la même catégorie
A : arrière-plan technologique
O : divulgation non-écrite
P : document intercalaire

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

.....

& : membre de la même famille, document correspondant

EPO FORM 1503 12.99 (P04C14)

ANNEXE AU RAPPORT DE RECHERCHE PRÉLIMINAIRE RELATIF A LA DEMANDE DE BREVET FRANÇAIS NO. FR 0653362 FA 683786

La présente annexe indique les membres de la famille de brevets relatifs aux documents brevets cités dans le rapport de recherche préliminaire visé ci-dessus.
Les dits membres sont contenus au fichier informatique de l'Office européen des brevets à la date du 23-05-2007
Les renseignements fournis sont donnés à titre indicatif et n'engagent pas la responsabilité de l'Office européen des brevets, ni de l'Administration française

Document brevet cité au rapport de recherche	Date de publication	Membre(s) de la famille de brevet(s)	Date de publication
GB 2398707 A	25-08-2004	US 2004209597 A1	21-10-2004
US 2004225878 A1	11-11-2004	AUCUN	
US 2006048212 A1	02-03-2006	CN 1701561 A	23-11-2005
		EP 1646177 A1	12-04-2006
		WO 2005011192 A1	03-02-2005

EPO FORM P0465