(19) OFICINA ESPAÑOLA DE PATENTES Y MARCAS

ESPAÑA

(11) Número de publicación: **2 349 626**

(51) Int. Cl.:
H04L 29/06 (2006.01)

(12) TRADUCCIÓN DE PATENTE EUROPEA T3

(96) Número de solicitud europea: **02785497 .5**
(96) Fecha de presentación : **13.09.2002**
(97) Número de publicación de la solicitud: **1428372**
(97) Fecha de publicación de la solicitud: **16.06.2004**

(54) Título: **Sistema de comunicación con confidencialidad mejorada.**

(30) Prioridad: **17.09.2001 FR 01 12022**

(45) Fecha de publicación de la mención BOPI:
07.01.2011

(45) Fecha de la publicación del folleto de la patente:
07.01.2011

(73) Titular/es: **SAGEM MOBILES**
Ponant de Paris
27, rue Leblanc
75015 Paris, FR

(72) Inventor/es: **Charbonnier, Philippe**

(74) Agente: **Aznárez Urbieta, Pablo**

Aviso: En el plazo de nueve meses a contar desde la fecha de publicación en el Boletín europeo de patentes, de la mención de concesión de la patente europea, cualquier persona podrá oponerse ante la Oficina Europea de Patentes a la patente concedida. La oposición deberá formularse por escrito y estar motivada; sólo se considerará como formulada una vez que se haya realizado el pago de la tasa de oposición (art. 99.1 del Convenio sobre concesión de Patentes Europeas).

Venta de fascículos: Oficina Española de Patentes y Marcas. Pº de la Castellana, 75 – 28071 Madrid

SISTEMA DE COMUNICACIÓN CON CONFIDENCIALIDAD MEJORADA

Descripción

La presente invención se refiere a un sistema de telecomunicación que incluye:

- Un primer medio de comunicación apto para comunicar con una red de transferencia de datos y destinado a estar a disposición de un usuario del sistema, y
- Un segundo medio de comunicación apto para comunicar con dicha red perteneciente a un interlocutor del usuario.

En este tipo de sistema, el primer medio de comunicación puede estar constituido por un terminal conectado a una red de tipo Internet, a disposición del usuario en un cibercafé, un hotel o una sala de aeropuerto.

El segundo medio de comunicación podrá ser un servidor conectado a una base de datos perteneciente al interlocutor que será, según la elección del usuario, un banco o una empresa de comercio en línea.

El documento WO 01/65340, publicado el 7 de septiembre de 2001, divulga un sistema de telecomunicación que incluye: un primer medio de comunicación apto para comunicar con una red de transferencia de datos y destinado a estar a disposición de un usuario del sistema, y un segundo medio de comunicación apto para comunicar con dicha red, perteneciente a un interlocutor del usuario. El sistema incluye además un objeto denominado personal, en posesión del usuario del sistema.

En tal sistema, el usuario no controla la confidencialidad de sus propios datos. Si, en el transcurso de un intercambio con el interlocutor, éste solicita al usuario su identificación o un código de acceso o incluso una contraseña, la información provista por el usuario circulará por el primer medio de

comunicación donde el usuario ejerce un control limitado, generalmente solo de funciones de interfaz. En particular, el usuario no puede tener la certeza de que el primer medio de comunicación no memorizará en un registro caché la información confidencial que lo atravesará, en vista a una futura utilización ilícita de dicha información por parte de una persona no autorizada que tendrá acceso al registro caché.

Tal situación crea una sensación de inseguridad entre los usuarios que es desfavorable para el desarrollo del comercio en línea a través de medios de comunicación de los cuales no son propietarios, y también perjudicial no solamente para los comerciantes en línea, sino también para los operadores de la red y para los fabricantes de equipos destinados a dichas redes.

La presente invención tiene como objetivo remediar en gran medida dichos inconvenientes, proponiendo un sistema de telecomunicación que garantiza al usuario un mayor control de la confidencialidad de sus propios datos.

Para ello, la invención incluye un sistema según la reivindicación 1.

El objeto personal puede ser un radioteléfono, un organizador de bolsillo o cualquier otro dispositivo, preferentemente de tipo portátil, donde el usuario habrá memorizado datos confidenciales propios, tales como números de identidad, códigos de acceso y otras contraseñas o datos bancarios o médicos.

El objeto personal estará provisto a menudo de capacidades de menor importancia que las ofrecidas al usuario por el primer medio de comunicación en términos de rendimiento y de interfaz hombre/máquina.

El objeto personal y el primer medio de comunicación podrán comunicar vía una unión por cable o radio.

En el sistema según la invención, el primer medio de comunicación ya no tiene la posibilidad material de manipular o de memorizar los datos que lo

atraviesan en cuanto ha sido colocado en modo de funcionamiento transparente. De este modo, si en el transcurso de un intercambio entre el interlocutor y el usuario, éste último es invitado a producir un dato confidencial, el primer modo de comunicación será colocado en modo de funcionamiento transparente antes de que el dato confidencial sea efectivamente emitido por el objeto personal.

Tal medida, una vez comunicada al usuario tendrá por efecto tranquilizar a los usuarios en lo referente a la preservación de la confidencialidad de sus propios datos y contribuirá al desarrollo del comercio en línea.

La configuración del primer medio de comunicación en modo de funcionamiento transparente podrá, según el caso, producirse mediante una señal de mando emitida por el objeto personal, por ejemplo después de la recepción de una solicitud de datos confidenciales, o por el segundo medio de comunicación, por ejemplo, simultáneamente o inmediatamente después de haber emitido tal solicitud.

El objeto personal podrá generar tal señal de mando automáticamente antes de la emisión de un dato confidencial o después de haber recibido la orden por parte del usuario.

En una variante ventajosa de la invención, el objeto personal será apto para comunicar directamente con el segundo medio de comunicación, por ejemplo por vía de ondas radioeléctricas si el objeto personal y el segundo medio de comunicación disponen ambos de recursos de emisión/recepción radio, por ejemplo compatibles con los estándares GSM o UMTS. En el sistema de telecomunicación según dicha variante, una comunicación directa se establece entre el objeto personal y el segundo medio de comunicación cuando el primer medio de comunicación está configurado en modo transparente.

Tal comunicación directa permite garantizar, teniendo apartado el primer medio de comunicación, que éste no pueda hacer peligrar la confidencialidad

de los datos intercambiados entre el objeto personal y el segundo medio de comunicación.

En un modo de realización particularmente ventajoso de la invención, un sistema de telecomunicación como el descrito anteriormente incluye medios de cifrado de los datos que circulan entre el objeto personal y el segundo medio de comunicación. Dichos medios de cifrado están destinados a ser activados cuando el primer medio de comunicación está configurado en modo transparente.

Los medios de cifrado ofrecen una garantía suplementaria al usuario en cuanto al carácter confidencial de la comunicación de sus propios datos al segundo medio de comunicación.

La invención se refiere también a un aparato emisor/receptor de señales radioeléctricas según la reivindicación 7, apto para cumplir las funciones del objeto personal incluido en un sistema de telecomunicación tal como está descrito anteriormente.

De un modo más general, la invención se refiere además a un procedimiento de transmisión de datos según la reivindicación 8.

En una variante de este procedimiento, se establece una comunicación directa entre el objeto personal y el segundo medio de comunicación cuando el primer medio de comunicación está configurado en modo transparente.

En un modo de realización particularmente ventajoso de tal procedimiento, los datos que circulan entre el objeto personal y el segundo medio de comunicación están cifrados cuando el primer medio de comunicación está configurado en modo transparente.

Tal como está expuesto anteriormente, este procedimiento permite garantizar al usuario una mayor confidencialidad de sus propios datos y contribuye al desarrollo del comercio electrónico.

Las características de la invención mencionadas anteriormente, así como otras surgirán con mayor claridad con la lectura de la descripción siguiente de un ejemplo de realización, descripción realizada con referencia a los dibujos adjuntos, donde:

- La figura 1, es un esquema funcional que describe un sistema de telecomunicación según la invención.
- La figura 2, es un esquema funcional que describe una variante de tal sistema de telecomunicación.
- La figura 3, es un organigrama que describe un procedimiento de transmisión de datos utilizado en tales sistemas, y:
- La figura 4, es un organigrama que describe una variante de tal procedimiento.

La figura 1 representa esquemáticamente un sistema de telecomunicación que incluye:

- Un objeto denominado personal OBJ, destinado a ser usado por el usuario del sistema.

- Un primer medio de comunicación M1 apto para comunicar con el objeto personal OBJ, por una parte, y con una red de transferencia de datos NETW, por otra parte, y destinado a estar a disposición del usuario, y:

- Un segundo medio de comunicación M2 apto para comunicar con dicha red NETW perteneciente a un interlocutor INT del usuario.

El objeto personal OBJ es, en este ejemplo, un organizador de bolsillo, el primer medio de comunicación M1 es un terminal multimedia a disposición del usuario en un cibercafé o en una sala de aeropuerto, y el segundo medio de comunicación M2 es un servidor perteneciente al interlocutor INT.

En este sistema, el primer medio de comunicación M1 es apto para ser configurado en un modo de funcionamiento transparente en el transcurso del cual el primer medio M1 es incapaz de actuar en los datos que circulan entre el objeto personal OBJ y el segundo medio de comunicación M2. La configuración en modo de funcionamiento transparente del primer medio de comunicación M1 puede ser activado, según los casos, ya sea mediante una señal de mando SC(OBJ) emitida por el objeto personal OBJ, o bien mediante una señal de mando SC (M2) emitida por el segundo medio de comunicación M2.

Por ejemplo, si el interlocutor INT es una institución bancaria y emite una solicitud en dirección al usuario para obtener de su parte códigos confidenciales, como un número de cuenta y una contraseña que permite consultar dicha cuenta, tal solicitud le será comunicada al usuario quien podrá dar la orden al objeto personal de emitir hacia el primer medio de comunicación M1 la señal de mando SC(OBJ) para colocar dicho primer medio M1 en modo de funcionamiento transparente antes de enviar efectivamente los datos confidenciales al interlocutor INT. Tal envío podrá ser realizado en una forma cifrada mediante medios de cifrado no representados en la figura, que serán por ejemplo según las especificaciones SSL (del inglés Secure Sockets Layer).

El envío de la señal de mando SC(OBJ) por parte del objeto personal puede ser realizado automáticamente por dicho objeto si previamente ha sido programado para enviar tal señal a partir de la identificación de una solicitud de datos confidenciales.

También es posible que el segundo medio de comunicación M2 esté configurado de modo tal que emita una señal de mando SC(M2) para colocar el primer medio de comunicación M1 en modo de funcionamiento transparente simultáneamente o inmediatamente después de la emisión de una solicitud de datos confidenciales por parte del segundo medio de comunicación, lo que evita toda intervención del objeto personal OBJ y/o del usuario mismo.

Tal señal de mando SC(OBJ) o SC(M2) puede tomar la forma, por ejemplo, de una secuencia de escape particular inserta en un flujo de datos enviado al primer medio de comunicación M1.

El modo de funcionamiento transparente puede ser obtenido de diversas maneras: el primer medio de comunicación M1 podrá ser configurado, por ejemplo, de modo que, durante este modo de funcionamiento, le estará prohibido a dicho primer medio M1 ejecutar funciones por encima de un nivel OSI predeterminado, correspondiente por ejemplo a actividades de recuperación de errores. Toda función de un nivel OSI superior, como operaciones de lectura, de memorización o de alteración de datos, será entonces momentáneamente inhibida, garantizando así la confidencialidad de los datos que circulan a través del primer medio de comunicación M1 así configurado. Con mayor motivo, si estos datos están cifrados, el primer medio de comunicación M1 será incapaz de descifrarlos, y aún menos de alterarlos de modo indetectable por parte del interlocutor INT.

La figura 2, es un esquema funcional que representa una variante del sistema de telecomunicación anteriormente descrito. Los elementos comunes a los dos sistemas están provistos con los mismos signos de referencia y no se describirán nuevamente. En este sistema, el objeto personal OBJ es un radioteléfono y el segundo medio de comunicación M2 está provisto de recursos ANT de emisión/recepción que lo hacen apto para comunicar con el objeto personal OBJ, por ejemplo mediante una red celular de tipo GSM o UMTS. En este sistema de telecomunicación, se establece una comunicación directa entre el objeto personal OBJ y el segundo medio de telecomunicación M2 cuando el primer medio de comunicación está configurado en modo transparente. Tal modo de realización de la configuración en modo de funcionamiento transparente del primer medio de comunicación M1 permite garantizar, manteniendo dicho medio M1 ajeno al intercambio de datos entre el objeto personal OBJ y el segundo medio de comunicación M2, que el primer medio de comunicación M1 no pueda poner en peligro la confidencialidad de los datos así intercambiados entre el objeto personal OBJ y el segundo medio de comunicación M2.

La figura 3, es un organigrama que ilustra el desarrollo de un procedimiento de transmisión de datos según la invención. Según este procedimiento, en el transcurso de una primera etapa CONM1, el usuario se

conecta al primer medio de comunicación M1, eventualmente por la vía de su objeto personal OBJ. En el transcurso de una etapa siguiente NAV, el usuario lanza un navegador que sirve de interfaz con la red de transferencia de datos. En el transcurso de una etapa siguiente URL, compone una dirección a los efectos de establecer una conexión con el interlocutor elegido. En el transcurso de una etapa siguiente CNM2.INFO, la conexión se establece y el interlocutor INT informa al usuario que el intercambio de datos se efectuará mediante un sistema de telecomunicación o de un procedimiento según la invención, a los efectos de convencer al usuario de que la transmisión de todo dato sensible que podría proveer a su interlocutor beneficiará de condiciones de confidencialidad óptimas. En el transcurso de una etapa siguiente REQM2, el interlocutor INT requiere por parte del usuario datos que le son propios. Por ejemplo, si el interlocutor es un comerciante en línea, podrá ser llevado, en el transcurso de una transacción, a solicitar al usuario un número de tarjeta bancaria para extraer de una cuenta bancaria asociada el importe de la transacción. Tal solicitud puede estar asociada a una señal de mando SC(M2) enviada, simultáneamente o inmediatamente después de dicha solicitud, por el segundo medio de comunicación M2 al primer medio de comunicación M1, en las condiciones descritas anteriormente, destinada a configurar el primer medio de comunicación M1 en modo de funcionamiento transparente. Caso contrario, el objeto personal OBJ puede, en cuanto recibe dicha solicitud, emitir, automáticamente o siguiendo una orden del usuario, una señal de mando SC(OBJ) destinada a idénticos fines. El carácter alternativo posible de dichos hechos se indica mediante la transición SC(M2)+SC(OBJ), donde hay que considerar el signo “+” en su sentido “O” booleano. En el transcurso de una etapa siguiente DISM1, el primer medio de comunicación M1 se configura en modo transparente y es incapaz de actuar en los datos que lo atraviesan en el transcurso de dicho modo de funcionamiento, garantizando de este modo la confidencialidad del intercambio que tiene lugar entonces entre el segundo medio de comunicación M2 y el objeto personal OBJ. En el transcurso de una etapa siguiente GRNTOBJ, el objeto personal OBJ accede a la solicitud del interlocutor INT y transmite los datos confidenciales requeridos por él. En una etapa siguiente RECM2, el segundo medio de comunicación recibe dichos datos y elimina la

inhibición impuesta al primer medio de comunicación. En una etapa siguiente ENM1, dicho primer medio de comunicación M1 abandona el modo de funcionamiento transparente y retoma un régimen de funcionamiento normal e inseguro, hasta que un nuevo intercambio de datos sensibles sea necesario, por ejemplo en el marco de una nueva transacción entre el usuario y el mismo interlocutor INT, posibilidad materializada por la transición NEWTR, u otra transacción con un nuevo interlocutor, posibilidad materializada por la transición NEWINT.

Se entiende que, una vez informado el usuario en el transcurso de la etapa CONM2+INFO de la seguridad, posible gracias a la invención, del intercambio de datos que deben intervenir en el transcurso de la transacción que piensa llevar a cabo, dicho usuario estará más propenso a proceder efectivamente a dicha transacción. Es totalmente posible confiar al primer medio de comunicación M1 el hecho de informar con mayor anterioridad al usuario de dicha ventaja a los efectos de instaurar lo antes posible un clima de confianza, por ejemplo al inicio de la etapa CONM1 después de la cual el usuario está conectado al primer medio de comunicación M1.

La figura 4 ilustra una variante del procedimiento descrito anteriormente, destinado a la realización en un sistema de telecomunicación donde el segundo medio de comunicación M2 es solidario al primer medio de comunicación M1. En tal caso, el segundo medio de comunicación M2 podrá ser por ejemplo el servidor de una base de datos central propia a una cadena de cibercafés o de salas de aeropuerto, para retomar los ejemplos anteriores, cadena a la cual pertenece el primer medio de comunicación M1. El usuario puede en efecto querer crear y guardar un perfil, es decir un conjunto de direcciones de red y/o de contraseñas y códigos de acceso y correspondientes, y desear que su identidad real no pueda estar asociada a dicho perfil por el terminal local por medio del cual comunica con dicha base de datos central, a los efectos de preservar localmente un anonimato cibernético. Un procedimiento de telecomunicación según esta variante de la invención comprenderá entonces ventajosamente una primera etapa CONM1.INFO, durante la cual el usuario se conecta al primer medio de comunicación M1, eventualmente por la vía de su

objeto personal OBJ. En el transcurso de esta misma etapa, el usuario es informado del hecho de que, gracias al uso de un sistema de telecomunicación o de un procedimiento según la invención, tiene la posibilidad de crear un perfil personal o de extraer un perfil personal de su objeto personal y de grabarlo en la base de datos central sin que ningún rastro de su identidad real pueda permanecer localmente asociado con dicho perfil. En el transcurso de una etapa siguiente PROT(M1), se activa un protocolo de intercambio de informaciones entre el objeto personal OBJ y el primer medio de comunicación M1 para permitir a dicho objeto enviar una señal de mando SC(OBJ) al primer medio para configurarlo en modo de funcionamiento transparente después de que el usuario haya producido su perfil. Durante una etapa siguiente DISM1, el primer medio de comunicación M1 está configurado en modo transparente y es incapaz de actuar sobre los datos que lo recorren en el transcurso de dicho modo de funcionamiento, garantizando de este modo la confidencialidad de todo intercambio que ocurre entre el objeto personal OBJ y el segundo medio de comunicación M2. En el transcurso de una etapa siguiente S(PROF.ID.ALIAS)M2, el objeto personal OBJ transmite el perfil producido por el usuario, acompañado por su identidad real y un alias elegido por el usuario, al segundo medio de comunicación M2. En una etapa siguiente R(PROF.ID.ALIAS)M2, el segundo medio de comunicación acusa recibo de dicho perfil al objeto personal OBJ, lo que inicia una interrupción de la inhibición impuesta al primer medio de comunicación M1. En una etapa siguiente ENM1, dicho primer medio de comunicación M1 abandona el modo de funcionamiento transparente y reinicia un régimen de funcionamiento normal inseguro. En una etapa siguiente ALIAS, el usuario da su alias al primer medio de comunicación M1, para instalar su perfil en dicho primer medio de comunicación M1. En una etapa siguiente INSTPROF, el segundo medio de comunicación M2 provee al primer medio de comunicación M1, ante su solicitud, el perfil anteriormente definido por el usuario. Dicho perfil se instala efectivamente entonces en el primer medio de comunicación M1. En el transcurso de una etapa siguiente NAV, el usuario puede lanzar un navegador que sirve de interfaz con la red de transferencia de datos. Dicha etapa puede ser seguida de las etapas que siguen a la etapa homónima en la figura anterior.

De la descripción anterior, surge con claridad que la invención, al mejorar las condiciones de seguridad de los intercambios de datos electrónicos, tendrá como consecuencia dar seguridad a los actores de tales intercambios, sólo con haberlos informado de las ventajas de la invención. La invención contribuirá de este modo al desarrollo del comercio electrónico y al respeto de la privacidad de los usuarios de las redes de transferencia de datos.

REIVINDICACIONES

1. Sistema de telecomunicación que incluye:

- un primer medio de comunicación apto para comunicar con una red de transferencia de datos y destinado a estar a disposición de un usuario del sistema y,

- un segundo medio de comunicación apto para comunicar con dicha red, perteneciente a un interlocutor del usuario,

sistema caracterizado porque incluye además un objeto denominado personal, destinado al usuario del sistema y porque el primer medio de comunicación es apto para ser configurado en un modo de funcionamiento transparente en el transcurso del cual dicho primer medio es incapaz de actuar sobre datos que circulan entre el objeto personal y el segundo medio de comunicación garantizando de este modo la confidencialidad de los datos que circulan por el primer medio de comunicación así configurado.

2. Sistema de comunicación según la reivindicación 1, donde la configuración en modo de funcionamiento transparente del primer medio de comunicación se inicia mediante una señal de mando emitida por el objeto personal.

3. Sistema de telecomunicación según la reivindicación 1, donde la configuración en modo de funcionamiento transparente del primer medio de comunicación se inicia mediante una señal de mando emitida por el segundo medio de comunicación.

4. Sistema de telecomunicación según una de las reivindicaciones 1 a 3, donde como el objeto personal es apto además para comunicar con el segundo medio de comunicación, se establece una comunicación directa entre el objeto personal y el segundo medio de comunicación cuando el primer medio de comunicación está configurado en modo transparente.

5. Sistema de telecomunicación según una de las reivindicaciones 1 a 4, que incluye medios de cifrado de los datos que circulan entre el objeto personal y el segundo medio de comunicación, estando dichos medios de cifrado destinados a ser activados cuando el primer medio de comunicación está configurado en modo transparente.

6. Sistema de telecomunicación según una de las reivindicaciones 1 a 5, donde el objeto personal es un radioteléfono.

7. Aparato emisor/receptor de señales radioeléctricas apto para cumplir funciones del objeto personal incluido en un sistema de telecomunicación según una de las reivindicaciones 1 a 5, caracterizado porque comprende medios para configurar dicho primer medio de comunicación en un modo de funcionamiento transparente durante el cual dicho primer medio es incapaz de actuar en datos que circulan por dicho primer medio entre el objeto personal del usuario y el segundo medio de comunicación.

8. Procedimiento de transmisión de datos entre:

- un primer medio de comunicación apto para comunicar con una red de transferencia de datos y destinado a ser puesto a disposición de un usuario del procedimiento, y

- un segundo medio de comunicación apto para comunicar con dicha red, perteneciente a un interlocutor del usuario,

procedimiento que incluye una etapa de configuración del primer medio de comunicación en un modo de funcionamiento transparente durante el cual el primer medio es incapaz de actuar sobre datos que circulan por el primer medio entre un objeto personal del usuario y el segundo medio de comunicación.

9. Procedimiento de transmisión de datos según la reivindicación 8, donde la etapa de configuración se inicia mediante una señal de mando emitida por el objeto personal.

10. Procedimiento de transmisión de datos según la reivindicación 8, donde la etapa de configuración se inicia mediante una señal de mando emitida por el segundo medio de comunicación.

11. Procedimiento de transmisión de datos según una de las reivindicaciones 8 a 10, donde entre el objeto personal y el segundo medio de comunicación se establece una comunicación directa cuando el primer medio de comunicación está configurado en modo transparente.

12. Procedimiento de transmisión de datos según una de las reivindicaciones 8 a 11, donde los datos que circulan entre el objeto personal y el segundo medio de comunicación están cifrados cuando el primer medio de comunicación está configurado en modo transparente.

13. Procedimiento de transmisión de datos según una de las reivindicaciones 8 a 12 caracterizado porque comprende además una etapa durante la cual al menos uno de los medios de comunicación está informado del hecho de que dicha transmisión se realizará mediante un sistema de telecomunicación según la reivindicación 1.

14. Procedimiento de transmisión de datos según una de las reivindicaciones 8 a 12 caracterizado porque comprende además una etapa durante la cual al menos uno de los medios de comunicación está informado del hecho de que dicha transmisión se realizará mediante un procedimiento de transmisión de datos según la reivindicación 8.

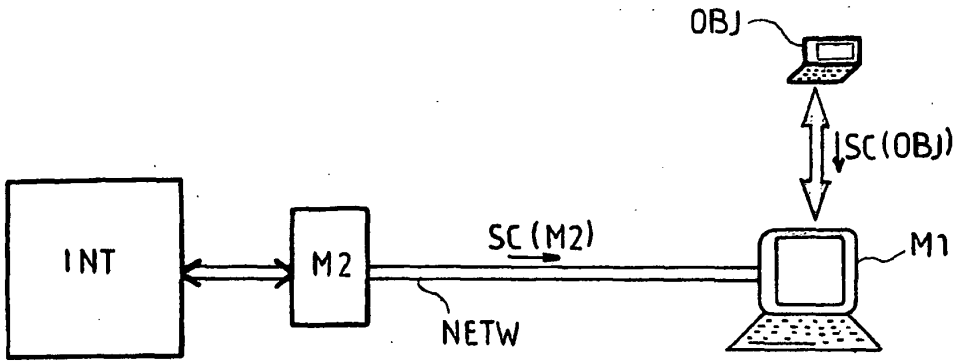

FIG. 1

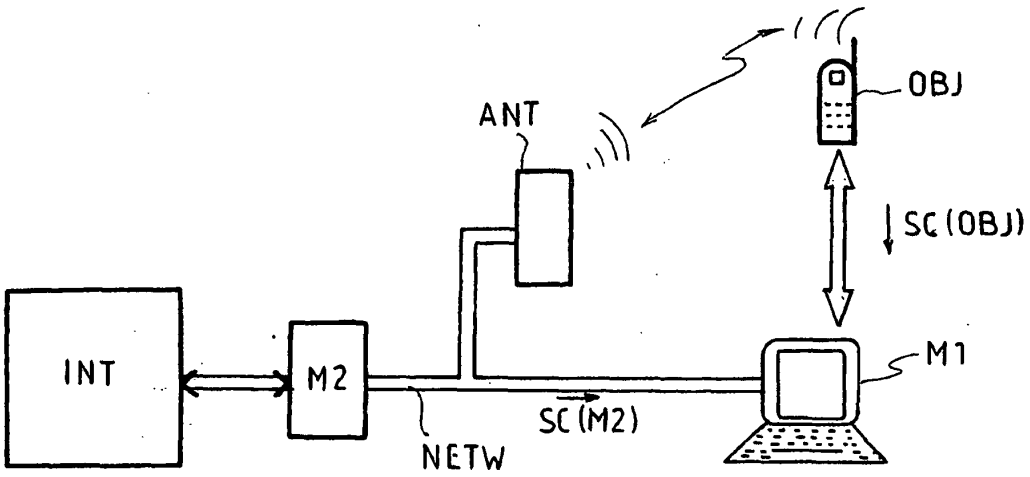

FIG. 2

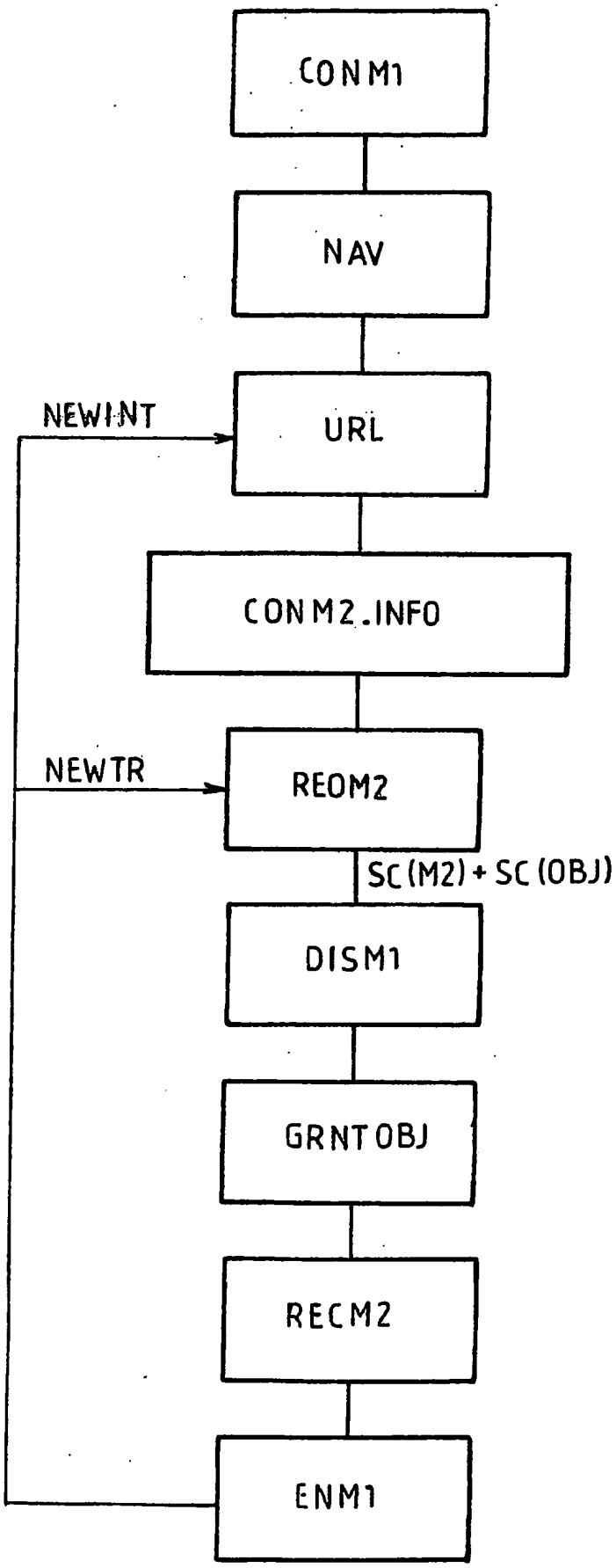
CONM1
NAV
NEWINT
URL
CONM2.INFO
NEWTR
REOM2
SC(M2) + SC(OBJ)
DISM1
GRNTOBJ
RECM2
ENM1

FIG.3

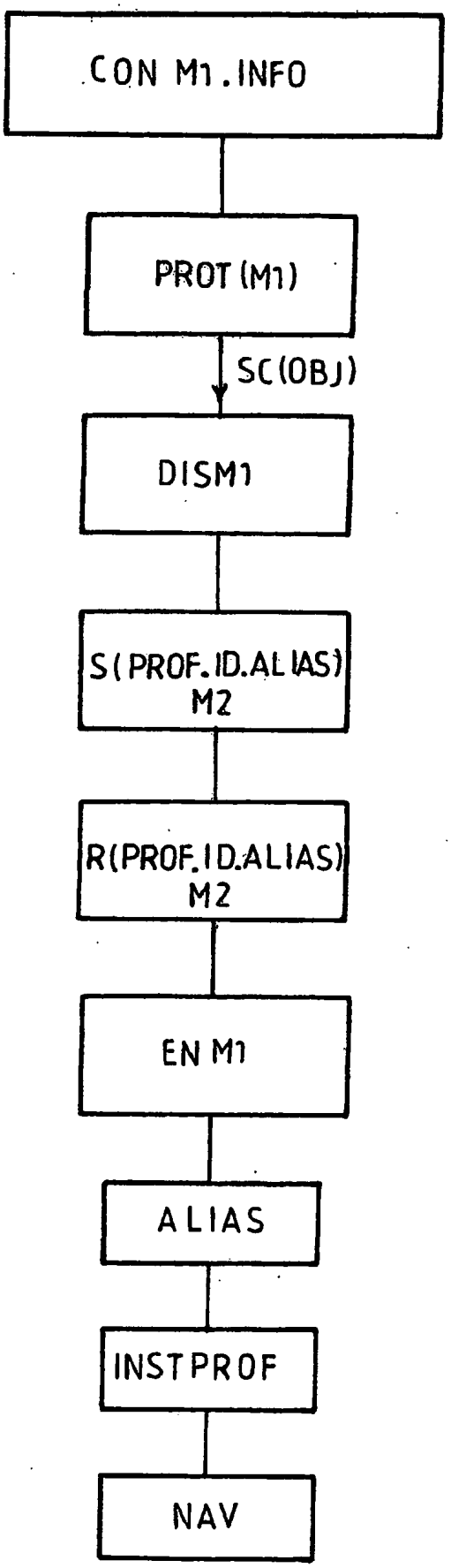
CON M1.INFO
PROT(M1)
SC(OBJ)
DISM1
S(PROF.ID.ALIAS) M2
R(PROF.ID.ALIAS) M2
EN M1
ALIAS
INSTPROF
NAV

FIG.4