(19) OFICINA ESPAÑOLA DE PATENTES Y MARCAS

ESPAÑA

(11) Número de publicación: **2 581 333**

(51) Int. CI.:

H04N 5/00 (2011.01)

(12) TRADUCCIÓN DE PATENTE EUROPEA T3

(96) Fecha de presentación y número de la solicitud europea: **19.06.2006 E 06778955 (2)**

(97) Fecha y número de publicación de la concesión europea: **06.04.2016 EP 1894407**

(54) Título: **Procedimiento y dispositivo de seguridad para la gestión de acceso a contenidos multimedia**

(30) Prioridad:

20.06.2005 FR 0506233

(45) Fecha de publicación y mención en BOPI de la traducción de la patente:
05.09.2016

(73) Titular/es:

ORANGE (100.0%)
78, rue Olivier de Serres
75015 Paris, FR

(72) Inventor/es:

TALAOUIT, VINCENT y
ANNIC, ETIENNE

(74) Agente/Representante:

ISERN JARA, Jorge

DESCRIPCIÓN

Procedimiento y dispositivo de seguridad para la gestión de acceso a contenidos multimedia

Campo de la invención

La presente invención se refiere al campo de los terminales de comunicación (por ejemplo teléfonos portátiles, unas PDA con comunicación, PC, etc.) equipados con un dispositivo de seguridad (por ejemplo una tarjeta de microchips) y que se refiere más particularmente el acceso a contenidos multimedia propuestos por los operadores a través de una red de comunicaciones.

Técnica antecedente

Para un gran número de terminales de comunicación, tales como los teléfonos móviles, es necesario para el funcionamiento del terminal un dispositivo de seguridad gestionado por un tercero de confianza (por ejemplo operador). Un dispositivo de seguridad de ese tipo es por ejemplo la tarjeta UICC (por "UMTS Integrated Circuit Card") (también denominada tarjeta SIM por "Subscriber Identity Module" o incluso tarjeta USIM por "Universal Subscriber Identity Module"). Este dispositivo permite entre otros la autentificación del abonado en una red móvil de telecomunicaciones, el filtrado de los intercambios (de voz o de datos) así como la personalización del terminal móvil. Permite también el acceso a servicios de valor añadido tales como correo, el seguimiento del consumo, el servicio cliente, el directorio personal del usuario, el envío de llamadas, mini mensajes, etc…. Estos servicios se almacenan en la tarjeta de abonado y se implementan en ella bajo la forma de llamadas telefónicas. En efecto, en el caso por ejemplo de un servicio de mensajería, la selección de este servicio sobre el menú se convierte en una llamada telefónica en GSM en modo circuito de voz hacia un número de teléfono (tipo E-164) que corresponde en general al de un servidor local.

Con la llegada de sistemas de telecomunicación móvil de nuevas generaciones (3G) acompañados de nuevas normas de alta velocidad tales como las normas UMTS o GPRS que permiten unas transmisiones de datos en modo paquetes, los operadores desean poder proponer unos servicios o contenidos multimedia cada vez más sofisticados.

Las soluciones actuales para implementar dichos servicios necesitan previamente la parametrización de los abscesos del terminal por parte del usuario. A título de ejemplo, en el marco de una configuración GPRS/UMTS de un acceso a "Internet" en un terminal comercial, el procedimiento siguiente es el siguiente:

etapa 1: acceder al menú "conexiones";
etapa 2: acceder a submenú "comunicación de datos";
etapa 3: acceder a submenú "acceso de datos";
etapa 4: seleccionar entre una lista, el acceso de datos correspondiente al (a los) servicio(s) a parametrizar;
etapa 5: seleccionar el (los) parámetro(s) a modificar entre la lista de parámetros presentados y proceder a su modificación.

Los parámetros mencionados son "*APN*", "*dirección IP*", "*dirección DNS*", "*compresión de encabezado*", "*compresión de datos*", "*parámetros de calidad de servicio*", "*aplicación por defecto*", "*nombre de usuario*", "*contraseña*",…

Es claro que la parametrización del acceso a "Internet" a través de una red de acceso GPRS/UMTS que da acceso a un contenido tal como un correo electrónico requiere unos conocimientos tecnológicos que no están al alcance de un simple usuario no experto o no especializado.

Para remediar esto, los operadores han solicitado a los constructores de terminales móviles parametrizar en fábrica los terminales con una parametrización que tenga en cuenta los principales contenidos del operador. Pero esta solución está limitada por las capacidades de parametrización propias de cada terminal, lo que limita el número de servicios que pueden ser parametrizados por el operador así como el tipo de contenido parametrizable.

Esta solución no tiene en cuenta la modificación de la parametrización que puede evolucionar en el curso del tiempo y que es necesario modificar en el terminal para continuar accediendo al servicio.

Además, no permite garantizar ya la seguridad de los contenidos parametrizados, no dispone de medios para asegurar la modificación o la creación de la parametrización del acceso a los contenidos, pudiendo ser hechos a espaldas de su usuario por una aplicación maliciosa del terminal móvil. A título de ejemplo, han hecho su aparición los primeros virus sobre terminales móviles. El virus "Warrior A" tiene como consecuencia modificar la parametrización y el envío a espaldas del usuario de mensajes electrónicos con recargo. El usuario no puede más que constatar posteriormente un importe de factura exagerado y no justificado.

Al ser realizada previamente esta etapa de parametrización, el usuario es invitado a elegir la funcionalidad "acceso a una red de comunicación" en el menú del constructor del terminal pulsando, por ejemplo, sobre la tecla específica "tecla de acceso a una red de comunicación". El terminal presenta la lista de las redes de comunicación accesibles

por el terminal entre las que el usuario debe seleccionar aquella que permite alcanzar el contenido. Solo después de establecida la conexión con la plataforma, es cuando el usuario puede consultar un conjunto de contenidos disponibles. Y solo a continuación de una búsqueda del servicio, por ejemplo, mediante un motor de búsqueda, es cuando el usuario accede efectivamente al servicio deseado.

Se observa también que el acceso al contenido deseado necesita previamente su conocimiento por el usuario. Si el usuario no tiene conocimiento, este último tendrá pocas oportunidades de acceder al servicio y beneficiarse de sus ventajas.

Dado que una red de acceso GPRS/UMTS-PS da acceso a varias redes de comunicación, el usuario debe en consecuencia conocer previamente la red de comunicación a partir de la que se puede acceder al contenido, porque las redes de comunicación son disjuntas dos a dos, impidiendo que un contenido que se encuentre en una red de comunicación pueda ser accedido a partir de otra.

En consecuencia, el acceso a los contenidos multimedia (por ejemplo servicios de tipo GPRS y/o UMTS) con este tipo de solución es relativamente largo, complicado y aleatorio para el usuario, lo que penaliza el desarrollo de tales servicios.

Además, la consulta y la selección de los servicios o contenidos multimedia se realizan a partir de una interfaz de usuario propietaria del constructor del terminal, como se describe por ejemplo por la solicitud de patente europea EP 0 719 045 A2.

No hay posibilidad de que el operador ante el que el usuario ha suscrito un abono uniformice o personalice el menú en el que propone unos servicios.

Objeto y descripción sucinta de la invención

La presente invención tiene por objeto paliar estos inconvenientes proponiendo poner a disposición del usuario un medio simple y que no necesite ningún conocimiento tecnológico para acceder a unos contenidos multimedia que necesiten habitualmente unos conocimientos tecnológicos elevados para su implementación y su parametrización sobre el terminal. Los contenidos multimedia pueden ser de cualquier naturaleza y particularmente unos contenidos multimedia ricos tales como unas páginas web, unos videos, etc.

Este objetivo se alcanza mediante un procedimiento de gestión de contenidos multimedia, según la reivindicación 1.

De ese modo, gracias al procedimiento de la invención, la consulta, la selección y el lanzamiento de contenido multimedia se simplifica grandemente para el usuario del terminal. En efecto, los contenidos se presentan al usuario en la forma de un menú que corresponde a un documento electrónico, lo que permite ofrecer numerosas posibilidades de presentación de los contenidos (por ejemplo, iconos, nombres comerciales etc.) en una forma fácilmente inteligible para el usuario. Además las operaciones a efectuar para el lanzamiento de contenido multimedia por el usuario se reducen al mínimo, a saber, en la mayor parte de los casos, a la simple selección de un contenido presentado en la pantalla del terminal.

Con la solución propuesta por la invención, el operador tiene la posibilidad de reagrupar y de organizar (“empaquetar”) en el seno del dispositivo de seguridad todos los datos necesarios para el acceso y para la publicación de los contenidos multimedia de manera que se disminuyan las dificultades de accesibilidad que impedirían al usuario acceder simplemente y de manera intuitiva a estos contenidos de alta tecnicidad.

Gracias a la invención, el operador puede también liberarse de las operaciones de mantenimiento ordinario necesarias durante una modificación de la parametrización para acceso a los contenidos, lo que asegura la accesibilidad a los contenidos incluso en el caso de cambio de la parametrización. En efecto, con los sistemas actuales, cualquier cambio de parámetros necesita la intervención del usuario que realice por sí mismo estas modificaciones de mantenimiento y que puedan convertirse muy rápidamente en fastidiosas porque reclaman unos conocimientos tecnológicos o de parametrización complejos.

El procedimiento de la invención aporta también al usuario una garantía de “operador” para los contenidos a los que accede, garantizando que dichos contenidos han sido aprobados por el operador tanto en el plano técnico (buen funcionamiento, acceso de seguridad, etc.) como en el plano de las tarifas (facturación fácilmente estimable y sin sorpresas). Los contenidos multimedia están sometidos a un fuerte pirateo y a malversaciones, como sobre la Internet hoy en día. La falta de confianza en el acceso a los contenidos perjudica muy grandemente los desarrollos comerciales, teniendo el comercio la necesidad de un enlace de confianza para establecerse. Utilizando un dispositivo de seguridad, tal como la tarjeta UICC, gestionada por el tercero de confianza que es el operador, la invención permite poner en práctica un acceso de confianza a los contenidos de datos, lo que facilita su desarrollo comercial.

En la etapa f) del procedimiento de la invención, el dispositivo de seguridad transmite al sistema operativo del terminal una orden de apertura de conexión hacia la red de comunicación identificada en el conjunto de los datos del contenido multimedia seleccionado y, en respuesta a la confirmación de la conexión a la red de comunicación, una orden de publicación del contenido multimedia en el terminal.

De ese modo, todas las acciones necesarias para el acceso y el lanzamiento de un contenido son gestionadas automáticamente por el dispositivo de seguridad que envía al terminal unas órdenes de ejecución completas a partir de los datos registrados en el dispositivo de seguridad. Esta orden puede tener en cuenta particularmente todos los parámetros técnicos (de hardware y de la red) necesarios para la implementación del contenido así como el nivel de derechos (autentificación) del que debe beneficiarse al usuario para acceder a ellos.

Según un aspecto de la invención, el procedimiento comprende además una etapa de descarga de nuevos conjuntos de datos y una etapa de verificación de dichos conjuntos de datos descargados, actualizando el dispositivo de seguridad la base de datos de los contenidos con estos nuevos conjuntos de datos en caso de verificación positiva. Esta actualización puede consistir en modificar unos datos de uno o varios conjuntos de datos relativos a uno o varios contenidos multimedia ya presentes en la base, y/o en registrar uno o varios conjuntos de datos que corresponden a nuevos contenidos multimedia, y/o en suprimir uno o varios conjuntos de datos de la base.

De ese modo, los operadores tienen la posibilidad de actualizar los contenidos multimedia que proponen a sus clientes independientemente del tipo de terminal móvil utilizado, y esto de manera fiable porque el dispositivo de seguridad verifica previamente cualquier nueva descarga de datos relativos a un contenido antes de proponerlo al usuario a través del menú de contenidos.

El objeto de la invención se alcanza igualmente gracias a un dispositivo de seguridad según la reivindicación 8.

Según un aspecto de la invención, el dispositivo de seguridad comprende además unos medios para verificar los conjuntos de datos descargados en el dispositivo de seguridad y para actualizar una base de datos de los contenidos con estos nuevos conjuntos de datos en caso de verificación positiva, consistiendo la actualización de la base de datos de los contenidos en modificar unos datos de uno o varios conjuntos de datos relativos a uno o varios contenidos multimedia ya presentes en la base, y/o en registrar uno o varios conjuntos de datos correspondientes a nuevos contenidos multimedia, y/o en suprimir uno o varios conjuntos de datos de la base.

La invención se refiere igualmente a un terminal móvil equipado con una interfaz de usuario que comprende al menos unos medios de presentación y de selección, caracterizado por que comprende un dispositivo de seguridad tal como el descrito anteriormente.

Los datos de un conjunto de datos para cada contenido multimedia se registran en el dispositivo de seguridad bajo el formato o clasificación de niveles siguiente:

- nivel 0 que comprende los datos de identificación del contenido;
- nivel 1 que comprende el tipo de red de acceso al contenido multimedia;
- nivel 2 que comprende el identificador de la red de comunicación para acceder al contenido multimedia;
- nivel 3 que comprende las informaciones sobre la autentificación requerida para el acceso a dicha red;
- nivel 4 que comprende los recursos requeridos para la publicación del contenido multimedia;
- nivel 5 que comprende el identificador de acceso del contenido multimedia;
- nivel 6 que comprende la identificación de la aplicación a ejecutar para la publicación del contenido multimedia en el terminal.

Breve descripción de los dibujos

Las características y ventajas de la presente invención surgirán mejor de la descripción siguiente, realizada a título indicativo y no limitativo, en relación con los dibujos adjuntos en los que:

- la figura 1 es una vista esquemática de la arquitectura del hardware y software de los elementos del sistema que implementa el procedimiento de gestión de acceso a los contenidos multimedia según la invención,
- la figura 2 es un ordinograma de un modo de implementación de un procedimiento de publicación de menús de contenido de acuerdo con un modo de realización de la invención,
- la figura 3 es un ordinograma de un modo de implementación del procedimiento de ejecución de acuerdo con un modo de realización de la invención,
- la figura 4 es un ordinograma de un modo de implementación del procedimiento de verificación de acuerdo con un modo de realización de la invención.

Descripción detallada de los modos de realización de la invención

La presente invención propone una solución para permitir a un usuario del terminal seleccionar y lanzar de manera simple y rápida unos servicios (por ejemplo servicios GPRS y UMTS o equivalentes) y que se denominará en lo que sigue del texto simplemente “contenido multimedia”. En la presente descripción, un contenido multimedia hace referencia a cualquier tipo de intercambio de información que conduzca a una comunicación tales como una llamada telefónica, fax, una página que contiene unas informaciones (tal como una página web), un mensaje electrónico, un video o una película, un software descargado (tal como un juego, una herramienta de mapas de carretera, un software de pago…), unos datos transmitidos en transmisión continua (denominada también streaming) tal como la televisión, la radio, unos datos difundidos tales como la televisión, una publicidad, el teletexto…

Por otro lado, la invención se aplica a cualquier terminal que disponga de un dispositivo de seguridad gestionado por un tercero de confianza que tenga la propiedad o el disfrute. Este elemento de seguridad puede ser la tarjeta UICC del teléfono móvil (también denominada tarjeta SIM o tarjeta USIM), un componente electrónico, extraíble o no, dispuesto en un terminal tal como, por ejemplo, un teléfono portátil, un teléfono fijo, una televisión, un vehículo (automóvil, tren,…), un equipo de acceso a una red de servicios como un decodificador audiovisual, equipos electrodomésticos, etc.

Por razones de simplificación, en lo que sigue de la descripción, se tomará un ejemplo en el que el terminal del usuario es un teléfono portátil, el dispositivo de seguridad es una tarjeta UICC, el tercero de confianza es un operador de telecomunicaciones (por ejemplo Orange™) y la red accedida es una red de datos GPRS/UMTS.

La figura 1 ilustra una arquitectura en la que puede implementarse la invención. Esta arquitectura comprende particularmente:

- un terminal 10,
- un dispositivo de seguridad 20,
- una red de acceso 30, accesible por el terminal y que da acceso a las redes de comunicación,
- una(s) red(es) de comunicación 40, 50, 60 que dan respectivamente acceso a unos contenidos multimedia 41, 51, 52, 61 y 62.

El terminal 10 y el dispositivo de seguridad 20 comunican a través de una interfaz 16, 26. Por ejemplo en el caso del móvil, esa interfaz es normalizada por el ETSI (Instituto Europeo de Normas de Telecomunicación). Su acceso a través de unas API (interfaces de aplicación) está también normalizado, se dará en el ejemplo la recomendación JSR177 definida por el Java™ Forum.

El dispositivo de seguridad 20 comprende tres aplicaciones: una aplicación “menú” 21 (publicación del menú), una publicación “verificador” 22 y una aplicación “ejecutor” 23 (publicación del contenido multimedia) que pueden ser implementadas en la forma de un componente electrónico programado. Comprende además un espacio de memoria 24 para la transferencia de archivos y una base de datos de los contenidos 25 (pudiendo ser la base de datos un archivo). La realización de las tres aplicaciones puede realizarse por ejemplo en Java™ para los dispositivos de seguridad que dispongan de una máquina virtual Java™.

El terminal 10 comprende una interfaz de usuario 11, un sistema operativo 12, una interfaz de red de acceso 13 y eventualmente unas aplicaciones 14, 15 que permiten la publicación de contenidos.

La red de acceso 30 es la red que permite al terminal acceder a la(s) red(es) de comunicación 40, 50, 60.

En ciertas tecnologías de red, la red de acceso y la red de comunicación están reunidas en una única y misma red: es el caso por ejemplo de las redes telefónicas fijas (RTC).

En las otras tecnologías de red, la red de acceso y la(s) red(es) de comunicación son disjuntas: es el caso por ejemplo de la red GPRS.

Finalmente, cada contenido multimedia es accesible desde la red de comunicación correspondiente, por ejemplo, a través de un servidor de aplicación en el caso de contenidos web o a través de un terminal telefónico en el caso de una llamada telefónica.

El procedimiento de la invención implementa tres procedimientos principales: un procedimiento de publicación del menú, un procedimiento de ejecución del contenido multimedia y un procedimiento de verificación.

El procedimiento de publicación se implementa mediante la aplicación “menú” 21 en el dispositivo de seguridad 20 y produce un documento informático denominado “menú de contenidos”, que puede ser presentado por la interfaz de usuario del terminal y que permite la selección de un contenido por el usuario entre los publicados en el menú de contenidos. La selección conduce a la ejecución de dicho contenido seleccionado. La aplicación “menú” ejecuta el procedimiento de publicación descrito en el presente documento a continuación.

El procedimiento de ejecución o de publicación del contenido multimedia es implementado por la aplicación “ejecutor” 23 en el dispositivo de seguridad 20 y lanza el procedimiento de ejecución del contenido que permite que dicho contenido sea accesible por el usuario. El procedimiento de ejecución se describe en el presente documento a continuación.

El procedimiento de verificación consiste en descargar nuevos datos relativos a los contenidos con el fin de enriquecer el menú de contenidos. La llegada de nuevos datos activa la aplicación “verificador” 22 que tiene por objeto validar la coherencia de los datos y realizar el mantenimiento de la base de datos de los contenidos 25 en la que se almacenan los datos de contenidos necesarios para la fabricación del menú de contenidos.

En la presente invención, se define un contenido multimedia a partir de un conjunto de datos que se clasifican o formatean por “niveles”:

• el nivel 0 describe los datos comerciales del contenido, tales como su nombre comercial, su logotipo, su video o su señal representativa de una marca o de su utilización, su firma sonora representativa de una marca o de su utilización, un identificador del contenido independiente de su nombre, el tipo de contenido (bancario, ocio,…) etc. El nivel 0 puede contener unos datos en la forma de datos brutos o de archivo (por ejemplo archivo de imagen, sonido, etc.).
• el nivel 1 describe el tipo de red de acceso que permite el acceso al contenido. Los tipos de red de acceso son muy numerosos, se pueden citar por ejemplo el acceso por circuitos RTC (teléfono fijo), el acceso de datos ADSL, el acceso por circuito GSM, el acceso por circuito UMTS, el acceso de datos GSM-Data (GSM-CSD), el acceso de datos GPRS/UMTS-PS, el acceso de datos Irda (infrarrojo), el acceso de datos Bluetooth™ (tecnología de enlace serie vía radio), etc.
• el nivel 2 describe el identificador de la red de comunicación para acceder al contenido. La información de este nivel está condicionada por el valor del nivel 1 porque la mayor parte de los tipos de red de acceso no permiten el acceso más que a una única red de comunicación: es por ejemplo el caso de la redes de circuitos (RTC, GSM) y de la redes serie (Irda…). De ese modo para estos tipos de acceso de red, el nivel 2 no está completo. Los tipos de acceso de red que permiten el acceso a varias redes son, por ejemplo, la GPRS/UMTS-PS que identifica una red de comunicaciones del conjunto accesible por un identificador denominado “*APN*”, la GSM-Data que identifica la red por un identificador de tipo número de teléfono E164, etc.
• el nivel 3 describe la autentificación requerida para el acceso a la red. La información de este nivel está condicionada por el valor del nivel 1 porque la mayor parte de los tipos de acceso de red no gestionan la autentificación al acceso. En efecto, el acceso a ciertas redes puede estar condicionado a una autentificación fuerte de tipo (identificador/contraseña). Lo que es el caso por ejemplo para ciertos accesos a unas redes de comunicación identificadas por un APN.
• el nivel 4 describe los recursos requeridos para la ejecución del contenido. Estos recursos se refieren al terminal y la red que permite el acceso al contenido.
• el nivel 5 describe el identificador del contenido. El contenido se identifica mediante una dirección que depende de la red de comunicación que permite el acceso al contenido. Por ejemplo, en RTC o GSM, el contenido se identifica por un número telefónico E164. En GPRS/UMTS-PS y para un APN que reclame un direccionado IP, el contenido puede ser identificado mediante una dirección física IP (“Internet Protocol” normalizado por el IETF (Internet Engineering Task Force)) o una dirección lógica URI (“Uniform Resource Identifier” normalizado por el IETF), etc.
• el nivel 6 describe el identificador de la aplicación a ejecutar que permite el lanzamiento o la publicación del contenido en el terminal. Por ejemplo, si el contenido es una película, la aplicación será un lector de películas. Si el contenido es una página web, la aplicación será un navegador web, etc. La información de este nivel es facultativa porque la mayor parte de los sistemas operativos saben seleccionar automáticamente la aplicación de publicación en función del contenido que se le somete. En cualquier caso, este nivel puede ser útil cuando existe una voluntad de forzar la publicación sobre una aplicación de publicación particular, y esto para garantizar el resultado ofrecido al usuario. Porque, si se toma el único ejemplo del navegador web, cada navegador posee sus particularidades y la publicación del contenido en un navegador no válido puede conducir a una publicación parcial, incluso a ninguna publicación, lo que es muy perjudicial y puede tener consecuencias contractuales (o comerciales) sobre todo en el caso de contenidos de pago.

Procedimiento de publicación del menú

El desarrollo del procedimiento de publicación del menú es el siguiente (véase la figura 2):

- Etapa S10: la interfaz de usuario (IU) 11 del terminal 10 muestra en el terminal un enlace que da acceso al “menú de contenidos”. Por ejemplo, este enlace puede ser un botón sobre el teclado del terminal, una etiqueta o un icono sobre el que puede hacerse clic presentado sobre la pantalla del terminal.
- Etapa S11: el usuario activa el enlace del menú de contenidos.
- Etapa S12: la IU solicita la aplicación “menú” 21 del dispositivo de seguridad 20 que le transmite los datos relativos al menú de contenidos. Estos datos están contenidos en un documento informático cuyo formato puede publicarse por la IU. Por ejemplo en el caso de una solución web, el menú de contenidos se identifica por una URI de tipo “dispositivo_de_seguridad:\menú-de-contenidos.htm”.

- Etapa S13: la aplicación “menú” 21 extrae el nivel 0 de todos los contenidos de la base de datos de los contenidos 25.
- Etapa S14: a partir de estos datos, la aplicación “menú” pone en forma y publica el menú de contenidos en la forma de un documento informático cuyo formato es publicable por la IU.
- Etapa S15: la aplicación “menú” transmite a la IU el documento informático.
- Etapa S16: la IU publica el documento informático que aparece en la forma del menú de contenidos.
- Etapa S17: el usuario selecciona el contenido en el menú de contenidos.
- Etapa S18: la IU transmite a la aplicación “menú” unas informaciones que permiten deducir la identidad del contenido seleccionado. En efecto, en un ejemplo de una solución, el contenido se definirá en el menú de contenidos mediante un elemento de navegación web de tipo “server-side-maps” que permite identificar el contenido por sus coordenadas (X, Y) en la página web. Por supuesto, según la solución de implementación, las informaciones para identificar el contenido pueden variar.
- Etapa S19: la aplicación “menú” deduce de estas informaciones el identificador del contenido.
- Etapa S20: la aplicación “menú” 21 lanza la aplicación “ejecutor” 23 transmitiendo como parámetro de ejecución el identificador del contenido. (Véase el procedimiento de ejecución).
- Etapa S21: al final de la ejecución de la aplicación “ejecutor”, la aplicación “menú” recupera la iniciativa y vuelve a presentar el menú de contenidos. El usuario puede seleccionar un nuevo contenido.

Si una de las etapas anteriores fracasa, la aplicación “menú” pone fin al procedimiento de publicación del menú (etapa S22).

Procedimiento de ejecución (publicación del contenido multimedia)

El desarrollo del procedimiento de ejecución es el siguiente (véase la figura 3):

- Etapa S30: la aplicación “menú” 21 lanza la aplicación “ejecutor” 23 en el dispositivo de seguridad 20, pasando como parámetro de ejecución la identidad del contenido.
- Etapa S31: la aplicación “ejecutor” busca los datos relativos a dicho contenido en la base de datos de contenidos 25.
- Etapa S32: la aplicación “ejecutor” deduce de los niveles 1, 2 y 3 el procedimiento y el formato de la solicitud de apertura de acceso a la red de comunicación ante la red de acceso 30.
- Etapa S33: la aplicación “ejecutor” transmite al sistema operativo 12 del terminal 10 la solicitud de apertura de acceso para inicializar el acceso a una red de comunicación.
- Etapa S34: el sistema operativo determina si se solicita una autentificación en la apertura del acceso.
- Etapa S35: si se solicita una autentificación, el sistema operativo retransmite la solicitud a la aplicación “ejecutor”.
- Etapa S36: la aplicación “ejecutor” deduce del nivel 4 la respuesta a dar a la solicitud de autentificación resultante de la demanda de apertura.
- Etapa S37: si no resulta ninguna solicitud autentificación de la solicitud de apertura mientras que el nivel 4 está completo o, por el contrario, si hay una solicitud de autentificación resultante de la solicitud de apertura mientras que el nivel 4 no está completo, la aplicación “ejecutor” va directamente a la etapa de fracaso S42 que produce un mensaje de error (etapa S43). En los otros casos, la aplicación transmite la respuesta a la solicitud de autentificación al sistema operativo que se encarga de transmitirla a la interfaz a la red de acceso 13.
- Etapa S38: como retorno de una autentificación positiva o cuando no se ha solicitado ninguna autentificación, el sistema operativo confirma a la aplicación “ejecutor” el resultado de la apertura de la conexión a la red de acceso.
- Etapa S39: la aplicación “ejecutor” deduce de los niveles 5 y 6 el procedimiento y el formato de la solicitud de publicación del contenido. Si el nivel 6 está completo, este se impone para publicación de dicho contenido. Por el contrario, si el nivel 6 no está completo entonces la aplicación “ejecutor” deja al sistema operativo la elección de la aplicación para publicar el contenido.
- Etapa S40: lanzamiento de la publicación del contenido.
- Etapa S41: el sistema operativo confirma a la aplicación “ejecutor” la publicación del contenido.

Si una de las etapas precedentes fracasa, la aplicación “ejecutor” pone fin al procedimiento de publicación del menú (etapa S42) y presenta un mensaje de error sobre la interfaz de usuario del terminal (etapa S43) precisando el fracaso de la publicación del contenido especificado por su nombre que procede del nivel 0 del conjunto de datos de este último registrados en la base de contenidos.

Procedimiento de verificación

El procedimiento de verificación se implementa durante nuevas descargas del conjunto de datos de contenidos multimedia.

La descarga de datos es bien conocida por sí misma y puede realizarse de diferentes maneras. A título de ilustrativo, se describe el ejemplo de una descarga en un entorno de red móvil. Es posible colocar una descarga desde un terminal, desde una memoria extraíble, etc.
En una red de operador que esté encargado de los servicios, una base de datos 73 (véase la figura 1) contiene los datos o conjuntos de datos de los “menús de contenidos” de todos los abonados. Cuando los datos del “menú de

contenidos" de un abonado se modifican, la base de datos actualiza sus datos y alimenta una base de datos temporal 72 que contiene los contenidos modificados.

Una aplicación de descarga 71 escruta periódicamente la base de datos temporal 72. Si ésta no está vacía, realiza a partir de los datos que están contenidos en ella un archivo a descargar para cada dispositivo de seguridad del terminal de abonado. En el mundo móvil, el abonado es identificado por su IMSI o bien su MSISDN, 2 identificadores normalizados por el ETSI e interpretables por la red de acceso móvil.

La aplicación 71 transmite el (los) archivo(s) a una plataforma de descarga 70 que envía automáticamente los archivos hacia los destinatarios.

Por ejemplo, los métodos de descarga de seguridad están normalizados en el caso de un terminal móvil cuyo dispositivo de seguridad es una tarjeta UICC; estos métodos normalizados son BIP (Bearer Independent Protocol), OTA (Over The Air), etc.

Los datos descargados son almacenados en el espacio de memoria 24 reservado a las descargas, tal como el archivo "S-SMS" para el método OTA, a la espera de ser tratados. En el caso del método OTA, la norma prevé que los campos parametrizables sobre un SMS para especificar el uso de los datos contenidos en el SMS. De ese modo, mediante este método es posible especificar que los datos se refieren al menú de contenidos. En el caso del método BIP, el archivo transferido contiene un identificador representativo de un archivo de contenidos (tal como una extensión de archivo específica).

El desarrollo del procedimiento de verificación es el siguiente (véase la figura 4):

- Etapa S50: la aplicación "verificador" 22 es una aplicación en el dispositivo de seguridad 20 a la espera de nuevas descargas. Periódicamente, la aplicación "verificador" escruta los nuevos archivos descargados en el espacio de memoria de descargas para detectar la presencia de nuevos datos de contenido. Verificar que el archivo procedente de la descarga contiene los datos de contenidos. Si es ese el caso, comienza el procedimiento de verificación.
- Etapa S51: la aplicación "verificador" extrae los datos del primer contenido no tratado del archivo.
- Etapa S52: la verificación de los datos descargados y relativos a un contenido se realiza como sigue:

- Etapa S52a: verificación del nivel 0: la aplicación "verificador verifica que el nivel 0 no está vacío y contiene como mínimo un identificador de contenido y un nombre comercial.
- Etapa S52b: verificación del nivel 1: la aplicación "verificador" extrae el tipo de red de acceso indicado. Opcionalmente, interroga al sistema operativo del terminal para saber si el tipo de red de acceso está disponible en el terminal.
- Etapa S52c: verificación del nivel 2: la aplicación "verificador" verifica que el identificador de red completado en el nivel 2 es homogéneo con el tipo de red de acceso completado en el nivel 1.
- Etapa S52d: verificación del nivel 3: la aplicación "verificador" verifica que la autentificación completada en el nivel 3 es homogénea con el tipo de acceso de red completado en el nivel 1.
- Etapa S52e: verificación del nivel 4: la aplicación "verificador" verifica que el terminal posee un dispositivo de gestión de los recursos y que los recursos solicitados por el contenido multimedia están asignados para el terminal. Esta última verificación permite retirar del menú todos los contenidos multimedia que no son publicables en el terminal por falta de recursos suficientes. Si los recursos no están completos, entonces el contenido solicita un acceso "para el mejor" (también denominado "best effort") sin garantía de resultado. En cuyo caso, la aplicación "verificador" no procede a ninguna verificación de recursos. Si los recursos requeridos para el contenido no están asignados al terminal, entonces el contenido se suprime de la base de datos.
- Etapa S52f: verificación del nivel 5: la aplicación "verificador" verifica que el identificador del contenido es homogéneo con el tipo de acceso de red completado en el nivel 1. Por ejemplo, en una red de acceso telefónico (RTC), el identificador del contenido debe tener el formato de un número telefónico E164.
- Etapa S52g: verificación del nivel 6: la aplicación "verificador" verifica que la aplicación de publicación está disponible en el terminal interrogando al sistema operativo del terminal.

- Etapa S53: si se han pasado con éxito todas las verificaciones, entonces la aplicación "verificador" actualiza la base de datos de contenidos 25, si no pasa directamente al tratamiento del contenido siguiente (etapa S54). La base de datos de los contenidos prevé 3 acciones de mantenimiento:

a. etapa de modificación: la actualización consiste en buscar en la base si existe ya un contenido que posea un identificador de contenido idéntico, suprimir los datos de este contenido de la base de datos y posteriormente rellenarlos en la base con los nuevos valores de los datos del contenido tratados anteriormente mediante el procedimiento de verificación.
b. etapa de creación: la actualización consiste en buscar en la base si existe ya un contenido que posea un identificador de contenido idéntico. Si el identificador del contenido no existe en la base de datos entonces los valores de los datos del contenido tratados anteriormente mediante el procedimiento de modificación son introducidos en la base.

c. etapa de supresión: si los nuevos datos de contenido son nulos del nivel 1 a 6, entonces la actualización consiste en buscar en la base si ya existe un contenido que posea un identificador de contenido idéntico y suprimir los datos de este contenido de la base de datos.

- Etapa S54: la aplicación “verificador” pasa a la verificación del contenido siguiente en el archivo descargado y pasa directamente a la etapa S51. Si no hay más contenido a tratar, la aplicación pasa a la etapa S55.
- Etapa S55: como resultado el tratamiento del archivo, la aplicación “verificador” suprime dicho archivo, y vuelve a la etapa S50 para esperar la llegada del próximo archivo descargado.

Si una de las etapas precedentes fracasa, la aplicación “verificador” pone fin al procedimiento de publicación del menú (etapa S56) y pasa directamente a la etapa S55.

Se describe ahora un ejemplo de viabilidad de la presente invención aplicada a un terminal provisto de un navegador (“browser”) Web de NG (nueva generación).

En un terminal que posea un navegador de NG, el navegador, que administra la parte alta del sistema operativo, sirve de interfaz entre las interfaces del terminal (en particular la interfaz a la red de acceso) y las aplicaciones que demandan el acceso. Este método de arquitectura presenta la ventaja de realizar un tipo de uniformización del comportamiento de los terminales: todos los terminales reaccionan de manera idéntica y son accesibles de la misma manera. En efecto, en tiempo normal, los terminales poseen unos sistemas operativos diferentes, lo que para acceder a ellos implica adaptar todas las solicitudes de acceso a cada sistema operativo, lo que es materialmente imposible. Por otro lado, en caso de un sistema operativo desconocido, esto no funcionaría.

La interfaz de usuario del terminal es una aplicación Web (es decir aplicación escrita con la ayuda de los lenguajes Web). Debido a esta elección de implementación, su acceso por otras aplicaciones está normalizado y por lo tanto simplificado.

El acceso a cada interfaz del terminal se realiza con la ayuda de una “DOM API”, interfaz de aplicación (API) escrita según el lenguaje Web DOM (“Document Object Model”). Como se ha indicado anteriormente, el acceso a una interfaz cualquiera del terminal se simplifica porque se normaliza a través del lenguaje DOM.

El dispositivo de seguridad es una tarjeta UICC que posee una máquina virtual Java™. Las aplicaciones “menú”, “verificador” y “ejecutor” son unas applets Java™. El espacio de memoria de descarga es un espacio de memoria flash de la UICC reservado para este uso.

La base de datos de contenidos es un archivo. Para permitir la extracción de los datos de los contenidos, la codificación de este archivo se realiza por ejemplo según el protocolo siguiente (codificación expresada en hexadecimal):

- el archivo se codifica en ASCII
- el inicio de los datos de un contenido se señaliza por el nivel 0 del contenido y se especifica a continuación mediante 2 octetos: “FF” → “00”
- el inicio de los datos de los niveles del contenido es identificado mediante 2 octetos: “FF” → “número del nivel”
- para los niveles que disponen de varios campos, el inicio de los datos de los campos se identifica mediante 2 octetos: “FF” → “número del campo”

  - el número del campo es estrictamente superior a “10”
  - por ejemplo, para el nivel 0, se tendrían los identificadores de los campos:

    - “10”: identificador del contenido
    - “11”: nombre comercial del contenido
    - “12”: logotipo o imagen del contenido
    - …

El valor de los campos introducidos no puede contener el octeto “FF”. Los archivos descargados poseen el mismo formato.

El operador descarga en el espacio de memoria de descarga del dispositivo de seguridad un archivo de actualización de los contenidos. La descarga se realiza por ejemplo mediante el protocolo BIP del ETSI.

Periódicamente, la aplicación “verificador” inspecciona la presencia de un archivo en el espacio de memoria de descarga, descubre el archivo descargado y se asegura a través de su extensión que el archivo corresponde a unos datos de contenidos. La aplicación “verificador” extrae los datos de los contenidos y actualiza la base de datos de los

contenidos del dispositivo de seguridad, posteriormente, una vez terminada la extracción, destruye el archivo y espera a la próxima descarga.

La página por defecto de la interfaz de usuario del terminal posee un enlace que da acceso al menú de los contenidos. El usuario al activar este enlace, ejecuta la aplicación “menú” en el dispositivo de seguridad. La aplicación “menú” extrae los niveles 0 de los contenidos, y produce una página web que contiene el acceso a cada uno de los contenidos y representativa del menú de contenidos. El acceso a un contenido se define, por ejemplo, por el elemento de navegación Web “server-side-maps”. La aplicación “menú” transfiere la página web a la interfaz de usuario para que la publique en el terminal. El usuario, al seleccionar uno de los elementos de navegación Web “server-side-maps” que definen los contenidos multimedia sobre la página web, ordena el envío, mediante la interfaz de usuario, de un mensaje a la aplicación “menú” que contiene las coordenadas del contenido (X, Y) en la página Web. La aplicación “menú” deduce de las coordenadas el identificador del contenido y lanza la aplicación “ejecutor” teniendo como parámetro de ejecución el identificador del contenido.
La aplicación “ejecutor” extrae de la base de datos de los contenidos los datos que corresponden al identificador del contenido que le ha sido comunicado. De los niveles 1, 2 y 3, deduce la orden para abrir una conexión hacia la red de comunicación especificada por el contenido.

La orden toma la forma de un documento informático, de tipo página Web interactiva escrita en lenguaje DOM y contiene todas las informaciones para que el navegador Web pueda interpretarlas y ejecutar el procedimiento de conexión en la “DOM API” que gestiona la interfaz de la red de acceso. Si el procedimiento de conexión reclama una autentificación, la “DOM API” reenvía, a través del navegador Web y hacia la aplicación “ejecutor”, un mensaje (por ejemplo en la forma de un mensaje SOAP (SOAP es un protocolo estandarizado)) que solicita la identificación/ contraseña. La aplicación “ejecutor” responde como retorno el identificador/contraseña contenido en el nivel 4. Como resultado del procedimiento de conexión, la “DOM API” informa, a través del navegador Web, a la aplicación “ejecutor” del resultado del procedimiento. Si la conexión ha sido realizada, la aplicación “ejecutor” deduce de los niveles 5 y 6 la orden para publicar el contenido. En la solución Web dada en este caso como ejemplo, el nivel 5 contiene la URI del contenido multimedia a publicar “www.orange.com/bourse.htm”. El nivel 6 contiene la URI de la aplicación que permite la publicación del contenido “www.outil.com/browser/browserNG.exe”. En una arquitectura de navegador web de NG, la aplicación de publicación es lo más frecuente una aplicación Web que puede no estar disponible en el terminal; en cuyo caso, se descarga previamente, antes de proceder a la publicación del contenido.

Como resultado de la publicación del contenido, el menú de contenidos reaparece para que el usuario pueda seleccionar un nuevo contenido.

El contenido multimedia contenido en el nivel 5 puede ser de cualquier tipo: una llamada telefónica, una página web, un video, un fax, etc.

Por otro lado, la utilización de un navegador web como interfaz de usuario con una dirección de tipo URI para el acceso al contenido multimedia no es más que uno de los ejemplos posibles de implementación de la invención. El acceso al contenido multimedia puede obtenerse también, por ejemplo, mediante el envío de comandos “shell” (interfaz de comandos bajo Unix™) al sistema operativo para contactar con la interfaz de la red de acceso. Igualmente, el tipo de direccionamiento depende de la naturaleza del contenido multimedia al que se desea acceder. Por ejemplo, cuando el contenido multimedia es una llamada de voz, el direccionamiento es de tipo E164 (y ya no URI).

REIVINDICACIONES

1. Procedimiento de gestión del acceso a unos contenidos multimedia (41, 51, 52, 61, 62) por un terminal (10) equipado con un dispositivo de seguridad (20) gestionado por un tercero de confianza, comprendiendo dicho terminal una interfaz de usuario (11) y una aplicación de publicación (14, 15), estando integrado dicho dispositivo de seguridad (20) en el terminal, siendo accesibles dichos contenidos multimedia por el terminal a través de una o varias redes de comunicación (40; 50; 60), estando el procedimiento caracterizado por que comprende las etapas siguientes:

a) registro, en una base de datos (25) comprendida en el dispositivo de seguridad gestionado por el tercero de confianza, de un conjunto de datos para cada contenido multimedia,
b) creación, por el dispositivo de seguridad (20) y a partir de dichos datos registrados en la base de datos (25), de un documento informático que corresponde a un menú de contenidos multimedia,
c) transmisión por el dispositivo de seguridad (20) del documento informático a la interfaz de usuario (11),
d) publicación del documento informático mediante la interfaz de usuario (11),
e) selección de un contenido multimedia por el usuario a partir del documento informático presentado,
f) publicación del contenido multimedia seleccionado por la aplicación de publicación del terminal (10) en respuesta a unas instrucciones de control del dispositivo de seguridad (20) y en función del conjunto de los datos registrados en el dispositivo de seguridad para el contenido multimedia seleccionado.

2. Procedimiento según la reivindicación 1, caracterizado por que, en la etapa a), los datos de un conjunto de datos para cada contenido multimedia se registran en el formato siguiente:

- nivel 0 que comprende los datos de identificación del contenido;
- nivel 1 que comprende el tipo de red de acceso (30) al contenido multimedia;
- nivel 2 que comprende el identificador de la red de comunicación (40; 50; 60) para acceder al contenido multimedia;
- nivel 3 que comprende las informaciones sobre la autentificación requerida para el acceso a dicha red;
- nivel 4 que comprende los recursos requeridos para la publicación del contenido multimedia;
- nivel 5 que comprende el identificador de acceso del contenido multimedia;
- nivel 6 que comprende la identificación de la aplicación a ejecutar para la publicación del contenido multimedia en el terminal.

3. Procedimiento según la reivindicación 1 o 2, caracterizado por que, en la etapa f), el dispositivo de seguridad (20) transmite al sistema operativo del terminal (12) una orden de apertura de conexión hacia la red de comunicación identificada en el conjunto de los datos del contenido multimedia seleccionado y, en respuesta a la confirmación de la conexión a la red de comunicación, una orden de publicación del contenido multimedia en el terminal (10).

4. Procedimiento según la reivindicación 3, caracterizado por que la orden de publicación comprende unos datos de identificación de una aplicación a ejecutar para la publicación del contenido multimedia en el terminal (10).

5. Procedimiento según la reivindicación 3 o 4, caracterizado por que la orden de apertura de conexión comprende además unos datos de autentificación para el acceso a la red de comunicación.

6. Procedimiento según una cualquiera de las reivindicaciones 1 a 5, caracterizado por que comprende además una etapa de descarga de nuevos conjuntos de datos y una etapa de verificación de dichos conjuntos de datos descargados, actualizando el dispositivo de seguridad (20) la base de datos (25) con estos nuevos conjuntos de datos en caso de verificación positiva, y por que la actualización de la base de datos (25) consiste en modificar unos datos de uno o varios conjuntos de datos relativos a uno o varios contenidos multimedia ya presentes en la base, y/o en registrar uno o varios conjuntos de datos que corresponden a nuevos contenidos multimedia, y/o en suprimir uno o varios conjuntos de datos de la base.

7. Procedimiento según una cualquiera de las reivindicaciones 1 a 6, caracterizado por que la interfaz de usuario (11) del terminal (10) es un navegador web y por que el documento informático que corresponde a un menú de contenidos multimedia se identifica mediante una dirección URI o URL.

8. Dispositivo de seguridad (20) gestionado por un tercero de confianza e integrado en un terminal de comunicación (10), comprendiendo dicho terminal de comunicación una interfaz de usuario (11) y una aplicación de publicación (14, 15) y siendo utilizado para acceder a unos contenidos multimedia (41, 51, 52, 61, 62) a través de una o varias redes de comunicación (40; 50; 60), estando dicho dispositivo de seguridad caracterizado por que comprende:

- una base de datos (25), para memorizar un conjunto de datos para cada contenido multimedia,
- unos medios (21) para crear a partir de los datos memorizados en la base de datos (25) un documento informático que corresponde a un menú de contenidos multimedia;
- unos medios para transmitir el documento informático a la interfaz de usuario (11) del terminal con el fin de publicar el menú de contenidos multimedia en el terminal;

- unos medios (23) para enviar unas instrucciones de control a la aplicación de publicación del terminal para una publicación del contenido multimedia seleccionado a partir del menú presentado en el terminal (10) en función del conjunto de los datos registrados en el dispositivo de seguridad para el contenido multimedia seleccionado.

9. Dispositivo según la reivindicación 8, caracterizado por que los datos de un conjunto de datos para cada contenido multimedia se memorizan bajo el formato siguiente:

- nivel 0 que comprende los datos de identificación del contenido;
- nivel 1 que comprende el tipo de red de acceso (30) al contenido multimedia;
- nivel 2 que comprende el identificador de la red de comunicación (40; 50; 60) para acceder al contenido multimedia;
- nivel 3 que comprende las informaciones sobre la autentificación requerida para el acceso a dicha red;
- nivel 4 que comprende los recursos requeridos para la publicación del contenido multimedia;
- nivel 5 que comprende el identificador de acceso del contenido multimedia;
- nivel 6 que comprende la identificación de la aplicación a ejecutar para la publicación del contenido multimedia en el terminal.

10. Dispositivo de seguridad según la reivindicación 8 o 9, caracterizado por que comprende además unos medios (22) para verificar los conjuntos de datos descargados en el dispositivo de seguridad (20) y para actualizar la base de datos (25) con estos nuevos conjuntos de datos en caso de verificación positiva, consistiendo la actualización de la base de datos en modificar unos datos de uno o varios conjuntos de datos relativos a uno o varios contenidos multimedia ya presentes en la base, y/o en registrar uno o varios conjuntos de datos que corresponden a nuevos contenidos multimedia, y/o en suprimir uno o varios conjuntos de datos de la base.

11. Terminal móvil (10) equipado con una interfaz de usuario (11) que comprende al menos unos medios de presentación y de selección, caracterizado por que integra un dispositivo de seguridad según una cualquiera de las reivindicaciones 8 a 10.

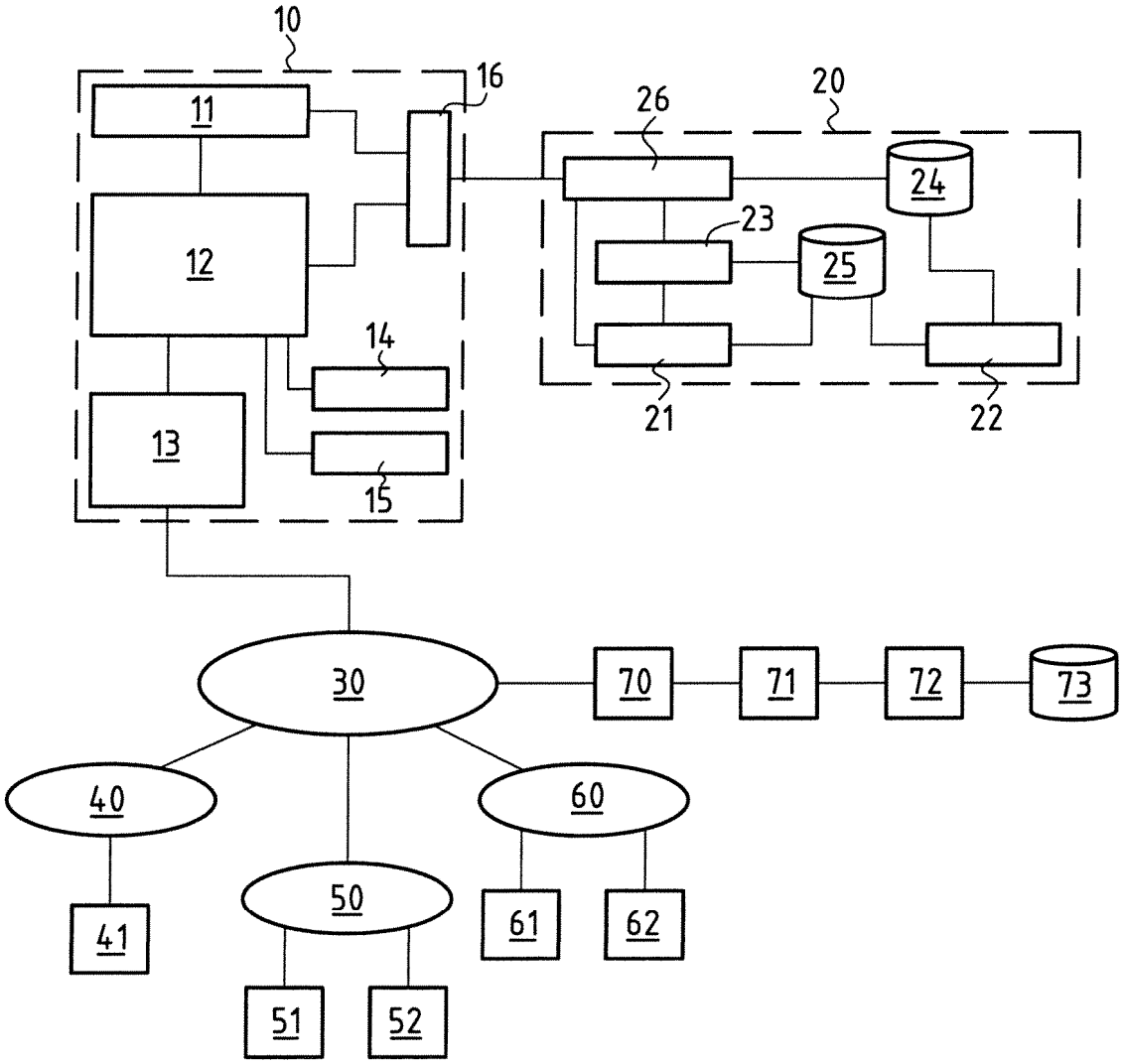
10
11
12
13
14
15
16
20
21
22
23
24
25
26
30
40
41
50
51
52
60
61
62
70
71
72
73

FIG.1

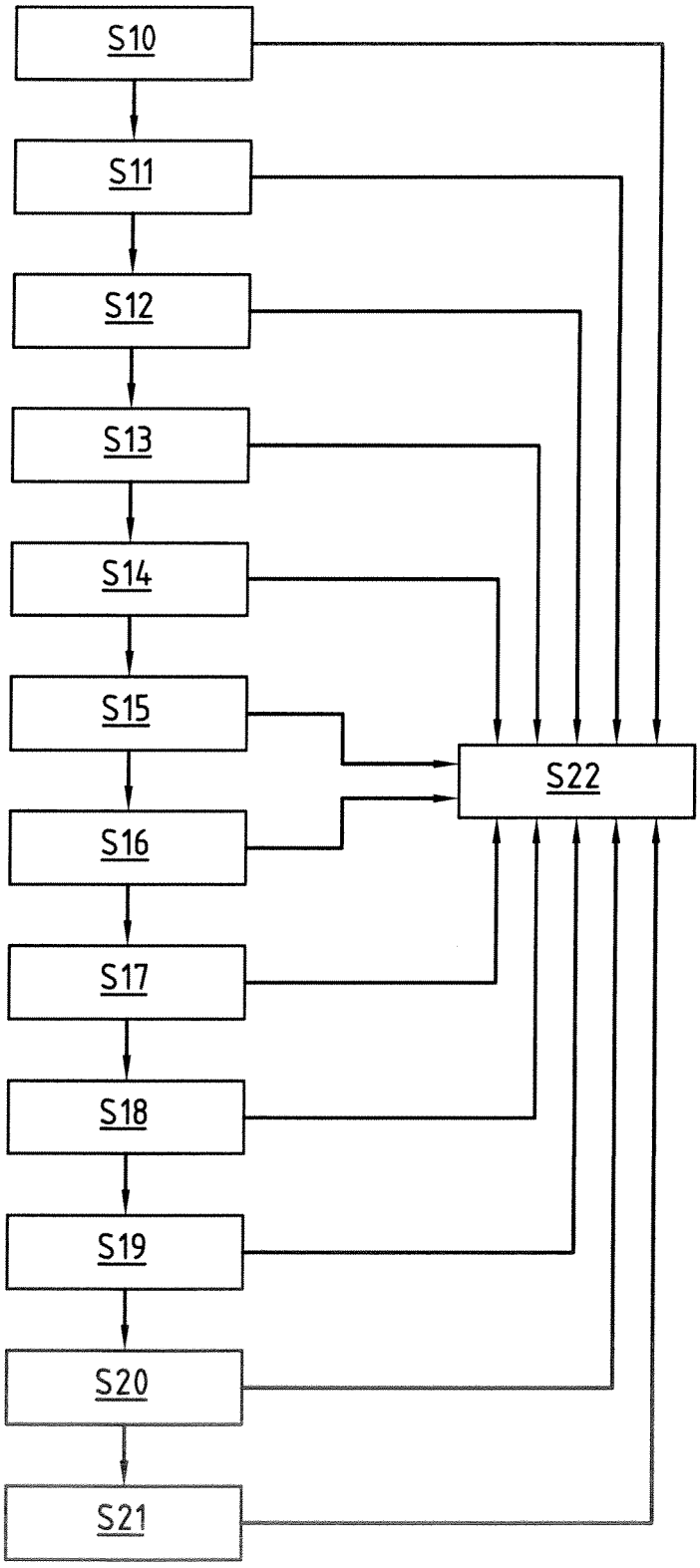

FIG.2

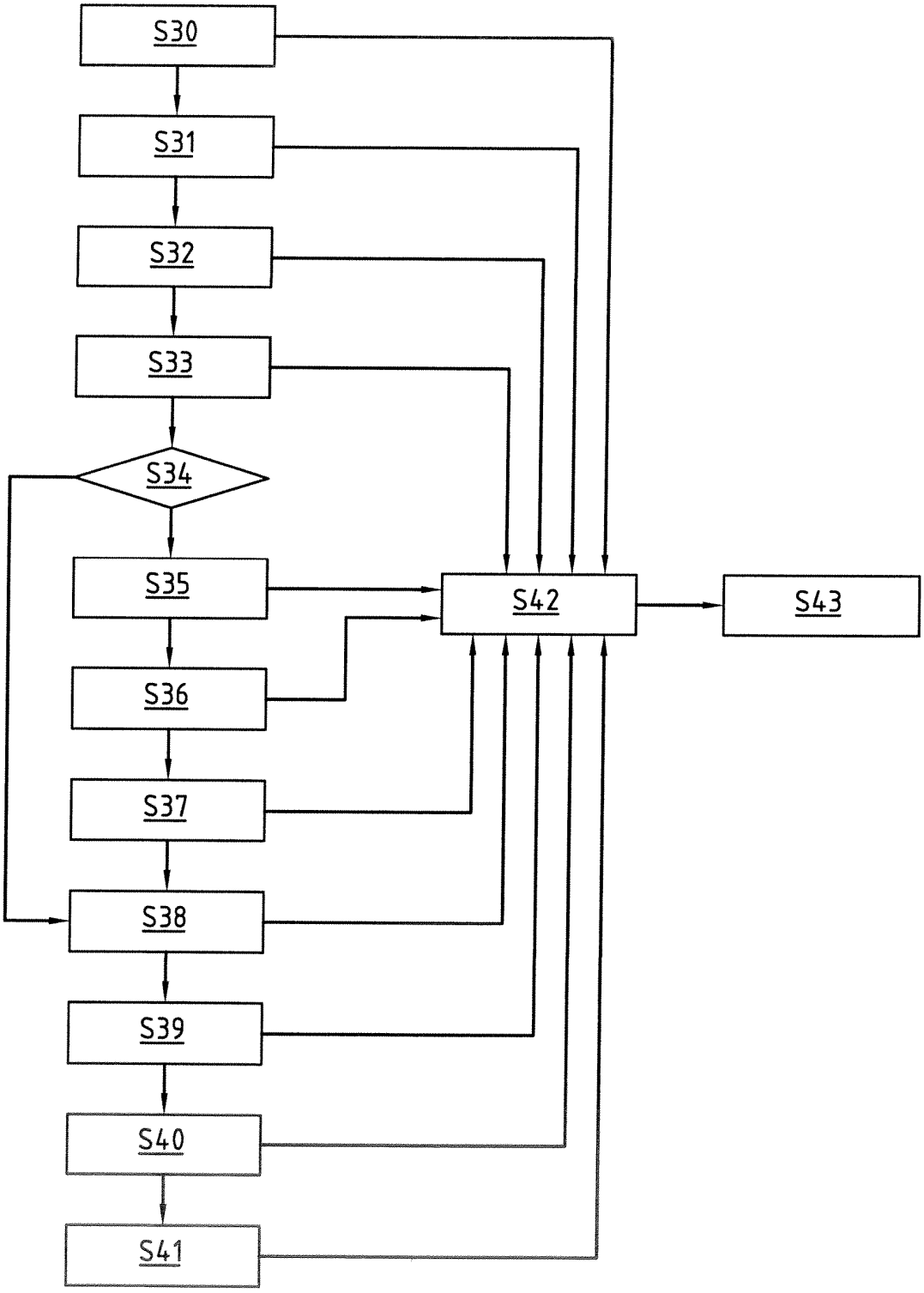

FIG.3

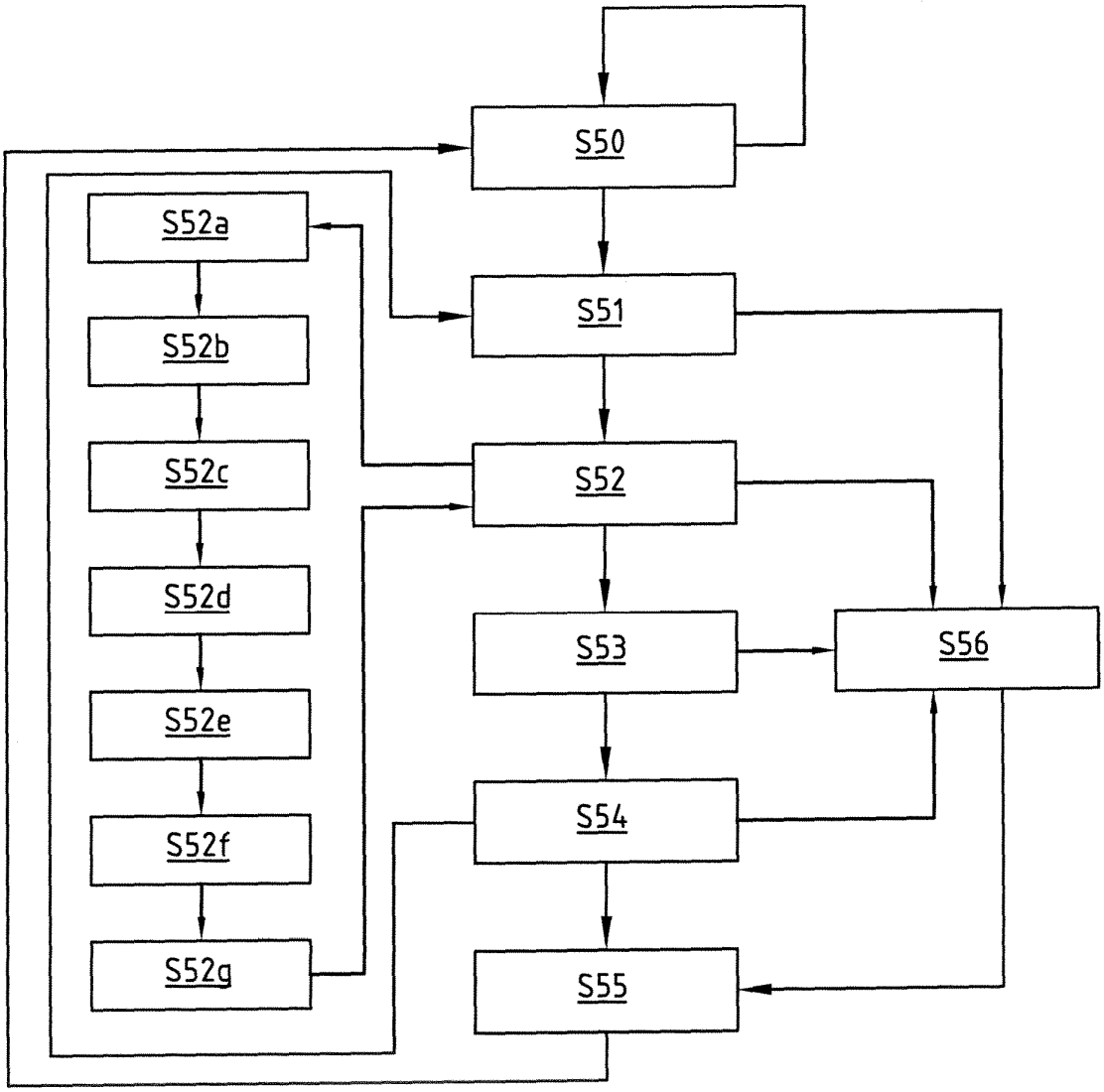

FIG.4