(19) OFICINA ESPAÑOLA DE PATENTES Y MARCAS

ESPAÑA

(11) Número de publicación: **2 749 881**

(51) Int. CI.:

***H04L 12/58*** (2006.01)
***H04L 29/08*** (2006.01)
***H04L 29/06*** (2006.01)

(12) TRADUCCIÓN DE PATENTE EUROPEA T3

(86) Fecha de presentación y número de la solicitud internacional: **07.10.2011 PCT/FR2011/052344**

(87) Fecha y número de publicación internacional: **12.04.2012 WO12045984**

(96) Fecha de presentación y número de la solicitud europea: **07.10.2011 E 11779814 (0)**

(97) Fecha y número de publicación de la concesión europea: **31.07.2019 EP 2625830**

(54) Título: **Procedimiento y dispositivo de transferencia segura de datos**

(30) Prioridad:

**07.10.2010 FR 1058134**

(45) Fecha de publicación y mención en BOPI de la traducción de la patente:
**24.03.2020**

(73) Titular/es:

**ELECTRICITÉ DE FRANCE (100.0%)**
**22-30 Avenue de Wagram**
**For all designated states, FR**

(72) Inventor/es:

**TARRAGO, ARNAUD;**
**SITBON, PASCAL y**
**NGUYEN, PIERRE**

(74) Agente/Representante:

**VEIGA SERRANO, Mikel**

## DESCRIPCIÓN

Procedimiento y dispositivo de transferencia segura de datos

**Sector de la técnica**

La invención se refiere al campo de la transmisión segura de datos, en particular en los sistemas informatizados que necesitan un alto nivel de seguridad.

**Estado de la técnica**

La protección de las redes de datos se asegura actualmente mediante unos dispositivos cuya seguridad se basa en su garantía de implementación y en el buen control de los protocolos de comunicación. Es el caso principalmente de los dispositivos "cortafuegos", de los relés de aplicación o los productos que segmentan las redes (como los productos VLAN, o la norma 802.1Q), así como de los sistemas de detección y de prevención de intrusión.

Pueden existir varios tipos de arquitecturas de seguridad. En las arquitecturas muy seguras, están prohibidas las interconexiones de redes. Los intercambios se realizan con ayuda de elementos físicos que no están conectados más que a un único sistema a la vez. Existen dispositivos de intercambio de un único sentido de comunicación pero su fiabilidad está limitada al hecho de la falta de flujo de control de intercambio y no se utilizan forzosamente en el sentido que va del sistema menos sensible en términos de seguridad hacia el sistema más sensible en términos de seguridad. Este es el caso de los dispositivos de "diodos físicos" basados, en su mayoría, en tecnologías de fibras ópticas.

Es habitual implementar una arquitectura de intercambio "ideal" por intermedio de cortafuegos sucesivos que delimitan una zona externa de intercambio, una zona interna de intercambio de primer nivel de confidencialidad y una zona interna de intercambio de segundo nivel de confidencialidad gestionadas respectivamente por servidores dedicados. La multiplicación de estas zonas de intercambio permite hacer más compleja la tarea de un eventual tercero malintencionado que desee acceder a, incluso corromper, ciertos datos de un sistema informático.

Sin embargo, se han revelado numerosos fallos de software en este tipo de arquitecturas, implicando entonces el compromiso de la red que se supone debían proteger. Las arquitecturas de intercambio "ideales" han sido, por ejemplo, sensibles a ataques sobre las aplicaciones utilizando las tecnologías web.

Independientemente de este problema de seguridad de software, una mala aplicación de la política de seguridad de una empresa o un error en la configuración de dichos dispositivos puede comprometer la seguridad de toda la red. Estos errores necesitan por tanto una supervisión y unos procedimientos de auditoría y de actualización permanente de dichos dispositivos.

Una primera solución de estos problemas se ha propuesto en la solicitud francesa FR 08 58790. En esta solicitud, la invención consiste en transferir datos de manera segura, por medio de simples comandos de tipo lectura o escritura, por intermedio de medios fijados físicamente así como de un espacio de almacenamiento central intermedio, con el fin de evitar la toma del control de un sistema conectado a uno de los puertos de acceso del sistema de transferencia segura por medio de un sistema conectado a otros de los puertos de acceso de este mismo sistema de transferencia segura.

Un dispositivo que utilice una solución así presenta sin embargo un inconveniente de depender de los sistemas que se le conectan en cuanto al final de la escritura de un archivo. Si un dispositivo de ese tipo comienza varias escrituras de archivos en paralelo, este dispositivo está entonces obligado a mantener tantas tablas de descripción como archivos hay en curso de escritura, lo que se traduce en un consumo inútil de recursos.

Además, en una implementación por omisión de un dispositivo según esta invención, el elemento de almacenamiento central de un dispositivo de ese tipo no sabe forzosamente cuándo el archivo digital transferido ha acabado de ser transmitido, lo que puede obstaculizar el desplazamiento de este archivo en este elemento a menos que se recurra a un implementación particular de este sistema, lo que complica aún más esta solución.

El documento US5878231 divulga un sistema para el filtrado de paquetes en una red de comunicación. Los paquetes se fragmentan e inspeccionan antes de que se encaminen hacia su destino, se bloquean o se toma alguna acción sobre los paquetes antes de que sean enviados.

Existe por tanto, en las soluciones de la técnica anterior, un problema de gestión de los archivos a transferir que es conveniente solucionar.

La presente invención viene a mejorar esta situación.

**Objeto de la invención**

Propone con este fin un procedimiento de transferencia segura de un archivo digital que proceda de un primer sistema informatizado hacia al menos un segundo sistema informatizado a través de un dispositivo de transferencia segura de acuerdo con el procedimiento de la reivindicación 1.

La presente invención propone además un dispositivo de transferencia segura de datos, adecuado para conectarse a un primer sistema informatizado y a un segundo sistema informatizado de acuerdo con la reivindicación de dispositivo 6.

**Descripción de las figuras**

El procedimiento y el dispositivo de transferencia segura, objetos de la invención, se comprenderán mejor con la lectura de la descripción y con la observación de los dibujos que siguen en los que:

- la figura 1 es un esquema sinóptico que ilustra un dispositivo de transferencia segura de datos según el principio de la presente invención;
- la figura 2 ilustra las etapas de un procedimiento de transferencia segura de datos según el principio de la presente invención;
- la figura 3A ilustra las etapas de un procedimiento de transferencia segura de datos según un primer modo de realización de la presente invención;
- la figura 3B ilustra las etapas de un procedimiento de transferencia segura de datos según una variante del primer modo de realización de la presente invención;
- la figura 4A ilustra las etapas de un procedimiento de transferencia segura de datos según un segundo modo de realización de la presente invención;
- la figura 4B ilustra las etapas de un procedimiento de transferencia segura de datos según una variante del segundo modo de realización de la presente invención;
- la figura 5A es un esquema sinóptico que ilustra un dispositivo de transferencia segura de datos según otro modo de realización de la presente invención; y
- la figura 5B ilustra las etapas de un procedimiento de transferencia segura de datos según un tercer modo de realización de la presente invención.

**Descripción detallada de la invención**

Se hace referencia inicialmente a la **figura 1** en la que se ilustra esquemáticamente el dispositivo de transferencia segura DISP según el principio de la presente invención.

El dispositivo de transferencia segura DISP se conecta, por un lado, a un primer sistema informatizado PC1 por medio de una primera red RED1 y, por otro lado, a un segundo sistema informatizado PC2 por medio de una segunda red RED2, con el fin de permitir el intercambio seguro de datos entre estos dos sistemas informatizados.

Se entiende en este caso por sistema informatizado cualquier tipo de sistema informático adecuado para leer o escribir un archivo digital por medio de una interfaz de red, como por ejemplo un ordenador personal, un servidor, un teléfono inteligente, un autómata industrial, un sensor, un actuador o cualquier otro objeto comunicante.

Asimismo, se entiende en este caso por red cualquier tipo de arquitectura que permita conectar físicamente unos sistemas informatizados entre ellos, por ejemplo una red local de tipo Ethernet, una red inalámbrica, la red de Internet o cualquier otro tipo de vinculación física.

El dispositivo de transferencia segura DISP incluye inicialmente un primer módulo de gestión de archivos G1 adecuado para almacenar un archivo digital F recibido desde el primer sistema informatizado PC1.

Para hacer esto, el primer módulo de gestión de archivos G1 incluye un medio de almacenamiento que permite la memorización del archivo digital F depositado desde el primer sistema informatizado PC1. Un medio así de almacenamiento puede consistir por ejemplo en un disco duro o una memoria flash.

El primer módulo de gestión de archivos G1 comprende por otro lado una interfaz de red, conectada a la primera red RED1 unida al primer sistema informatizado PC1, que permite la conexión a distancia con este primer sistema informatizado PC1 con el fin de recibir el archivo digital F. Una interfaz de red así puede ser de tipo FTP o HTTP, por ejemplo.

El primer módulo de gestión de archivos G1 comprende además un módulo de procesamiento que permite gestionar la manera en la que los archivos digitales se depositan y organizan en el medio de almacenamiento. De este modo, en particular, el medio de procesamiento gestiona la cola de espera de los archivos a transferir y da forma a estos archivos, por ejemplo asociándoles un marcado y dividiéndolas en una pluralidad de paquetes de datos, antes de transmitirles de manera secuencial hacia el módulo de verificación del dispositivo de transferencia segura.

Gracias a este primer módulo de gestión de archivos G1, puede controlarse la transmisión en paralelo de archivos digitales con el fin de evitar el consumo inútil de recursos.

Un marcado de ese tipo puede corresponder a la conversión del archivo digital a un formato específico e interno del dispositivo, por ejemplo con un encabezado que indique el tamaño y el tipo de archivo.

El módulo de procesamiento puede gestionar igualmente los archivos almacenados en el primer módulo G1 por medio de un directorio y clasificarlos en función de un parámetro tal como la fecha de depósito del archivo en el primer módulo G1 o un orden de prioridad predeterminado.

El dispositivo de transferencia segura DISP incluye por otro lado un módulo de verificación V dispuesto para recibir el archivo digital F almacenado en el primer módulo de gestión de archivos G1 y para efectuar una verificación sobre al menos una parte del archivo digital recibido.

Esta verificación y la modificación eventual de tipo sustitución o supresión de ciertos datos digitales que le puede acompañar, puede tratar sobre el conjunto del archivo digital F o, si este se divide en una pluralidad de paquetes $F_i$ en el primer módulo de gestión de archivos G1, sobre uno o varios de estos paquetes transmitidos secuencialmente desde el primer módulo de gestión de archivos G1 al módulo de verificación V, en función del tipo de verificación empleado. En particular, esta verificación puede realizarse sobre la marcha, en tiempo real, sobre unos paquetes individuales $F_i$ sobre las líneas del archivo digital F recompuestas a partir de los diferentes paquetes $F_i$ o bien sobre el archivo digital F recompuesto a partir de todos los paquetes $F_i$.

En el curso de esta verificación, pueden verificarse diversos parámetros tales como, por ejemplo, el tamaño de los paquetes $F_i$; transferidos o la sintaxis empleada en estos paquetes, el tipo de caracteres utilizados en estos paquetes o la firma electrónica estampada sobre el archivo digital F.

Con el fin de limitar al máximo las posibilidades de toma de control de este módulo de verificación V por un elemento exterior, es ventajoso fijar físicamente las funcionalidades de verificación del módulo de verificación, por ejemplo implementando este módulo en la forma de una FPGA (por Field Programmable Gate Array) que puede programarse por el software antes de ser fijada físicamente.

Cuando la verificación trata sobre unos conjuntos de paquetes individuales $F_i$, por ejemplo correspondientes a unas líneas del archivo digital F, o bien sobre el archivo digital F completo, el módulo de verificación V incluye igualmente ventajosamente una memoria tampón, por ejemplo de tipo RAM, que permite almacenar temporalmente los paquetes $F_i$; recibidos con el fin de reformar la línea del archivo digital a analizar, incluso todo el archivo digital F, a analizar. El tamaño de esta memoria tampón depende de la finura de la verificación a efectuar.

El dispositivo de transferencia segura DISP incluye igualmente un segundo módulo de gestión de archivos G2 adecuado para recibir el archivo digital del módulo de verificación, con el fin de permitir su lectura por el segundo sistema informatizado PC2 en función del resultado de la verificación efectuada en el módulo de verificación V.

Este segundo módulo de gestión de archivos G2 es similar al primer módulo de gestión de archivos G1 e incluye un medio de almacenamiento que permite la memorización del archivo digital F, en su forma completa o en una forma descompuesta en paquetes $F_i$ una vez que se ha verificado por el módulo de verificación V, permitiendo una interfaz de red la conexión a la red RED2 unida al segundo sistema informatizado PC2.

El segundo módulo de gestión de archivos G2 puede comprender además un módulo de procesamiento que permite gestionar la manera en la que los archivos digitales se depositan y organizan en el medio de almacenamiento del segundo módulo de gestión G2, así como la puesta a disposición como lectura para el segundo sistema informatizado PC2.

Por ejemplo, si el archivo digital F se descompone en el primer módulo de gestión G1 en una pluralidad de paquetes de datos $F_i$ que se verifican a continuación individualmente y secuencialmente por el módulo de verificación V, incluso se modifican eventualmente por sustitución o supresión de ciertos datos digitales que pertenecen a algunos de los paquetes de datos $F_i$, antes de llegar secuencialmente al segundo módulo de gestión G2, este módulo de tratamiento será adecuado para recomponer un archivo digital F' sobre el medio de almacenamiento del segundo módulo de gestión G2, volviendo a ensamblar los paquetes $F_i$ verificados, eventualmente modificados por sustitución o supresión de una parte de sus datos digitales, antes de darle acceso como lectura a este archivo recompuesto al segundo sistema informatizado PC2.

Es posible así controlar cuándo el archivo F transferido se pone a disposición del segundo sistema informatizado PC2, por ejemplo convirtiéndole en accesible únicamente cuando el archivo F se ha recompuesto completamente en el módulo de gestión de archivos G2, lo que permite responder a los inconvenientes que surgen en la técnica anterior.

Los módulos de gestión de archivos G1 y G2 se conectan respectivamente al módulo de verificación V del

dispositivo de transferencia segura DISP por medio de interfaces físicas B1 y B2, de tipo bus memoria, que tiene un tamaño limitado.

En un caso de este tipo, es ventajoso dividir el archivo digital F a transmitir en una pluralidad de paquetes $F_i$ cuyo tamaño es inferior a un tamaño máximo de paquetes de datos que pueden transitar en la interfaz física B1, determinado en función del tamaño limitado de la interfaz física B1. De este modo, se pueden formar por ejemplo unos paquetes $F_i$ de 256 octetos.

Se hace referencia ahora a la **figura 2** que ilustra un procedimiento 100 de transferencia segura de un archivo digital F que procede de un primer sistema informatizado PC1 hacia al menos un segundo sistema informatizado PC2 según el principio de la invención.

El procedimiento 100 comprende inicialmente una etapa 110 de escritura del archivo digital F en un primer módulo de gestión de archivos G1 de un dispositivo de transferencia segura DISP, tal como por ejemplo el descrito en la figura 1.

A continuación del depósito de este archivo digital F en este primer módulo de gestión de archivos G1, el procedimiento 100 prosigue mediante la transferencia (etapa 120) de este archivo digital F hacia un módulo de verificación V interno del dispositivo de transferencia segura DISP. Esta transferencia puede hacerse de una sola vez o por medio de la transferencia secuencial de una pluralidad de paquetes $F_i$ obtenidos por descomposición del archivo digital F en el primer módulo de gestión de archivos G1, según el tipo de verificación efectuado, como se describirá más en detalle en lo que sigue.

El procedimiento 100 incluye entonces una etapa 130 de verificación de al menos una parte del archivo digital F transferido en el módulo de verificación.

De este modo, cuando se transfiere el archivo digital F en la forma de una transferencia secuencial de una pluralidad de paquetes $F_i$ obtenidos por descomposición del archivo digital F en el primer módulo de gestión de archivos G1, la verificación puede ser de tipo "individual", es decir efectuada individualmente sobre uno de los paquetes $F_i$ transferidos, sobre varios de los paquetes $F_i$ transferidos, incluso secuencialmente sobre el conjunto de los paquetes $F_i$ transferidos.

En otro ejemplo en el que el archivo digital F se transfiere de una sola vez al módulo de verificación, la verificación puede ser de tipo "global", es decir efectuada sobre el conjunto del archivo digital F.

El procedimiento 100 se prosigue entonces mediante la transferencia (etapa 140) del archivo digital F al menos parcialmente verificado, incluso completamente verificado, hacia un segundo módulo de gestión de archivos G2 del dispositivo de transferencia segura DISP en función del resultado de la verificación efectuada en el módulo de verificación V y esto con el fin de permitir la lectura del archivo F por el segundo sistema informatizado PC2 en función del resultado de esta verificación.

La etapa de transferencia 140 puede tratar sobre el archivo digital completo o hacerse mediante transmisión de paquetes $F_i$ en función del tamaño del bus físico que conecta el módulo de verificación al segundo módulo de gestión G2.

De este modo, si todas las operaciones de verificación efectuadas durante la etapa 130 de verificación tienen un resultado positivo, el archivo digital F se encuentra almacenado en el segundo módulo de gestión de archivos G2 y disponible para lectura por el segundo sistema informatizado PC2.

A la inversa, si una o varias de las operaciones de verificación efectuadas durante la etapa 130 de verificación tienen un resultado negativo, puede interrumpirse la transferencia del archivo digital F antes de que esté disponible íntegramente en el segundo módulo de gestión PC2, con el fin de evitar que este archivo digital F se ponga a disposición del segundo sistema informatizado CP2 si no responde a los criterios de verificación, con el fin de proteger al segundo sistema informatizado PC2 de cualquier información potencialmente peligrosa o inesperada.

De manera alternativa, siempre que una o varias de las operaciones de verificación efectuadas durante la etapa 130 de verificación tengan un resultado negativo, es posible también sustituir en la parte del archivo digital F que ha provocado este resultado negativo (por ejemplo en un paquete $F_i$) unos datos de sustitución que presenten una forma bien precisa y conocida para el segundo sistema informatizado PC2, como por ejemplo unos caracteres "_" o cualquier otro marcador, compuesto de caracteres específicos previamente fijados, que pueden indicar diferentes desviaciones con relación a los criterios de verificación.

En este caso, el archivo digital F será correcto y estará disponible, en la forma modificada F' de manera que indique que no presenta ya ningún riesgo, en el segundo módulo de gestión G2, pero cuando se lea por el segundo sistema de informatizado PC2, este reconocerá que el archivo F se ha modificado en un archivo F' y que no responde a los criterios de verificación. Ventajosamente, puede incluso detectar el tipo de desviación constatada y por tanto qué

criterio de verificación no se ha respetado por el archivo original F. El sistema informatizado PC2 deduce que el archivo original F no presentaba todas las garantías en términos de seguridad detectando la presencia de los datos de sustitución.

De este modo, con el procedimiento 100 de transferencia de datos seguro, el segundo sistema informatizado CP2 tiene siempre acceso al archivo digital F en su integridad si la verificación de este archivo digital se ha desarrollado correctamente y, si esta verificación ha detectado un problema, el segundo sistema informatizado PC2 no tiene acceso a ningún archivo digital o entonces a un archivo digital modificado F' del que al menos una parte se ha sustituido de manera conocida.

En todos estos casos de figuras posibles, el segundo sistema informatizado PC2 no tendrá que gestionar una multitud de paquetes transferidos secuencialmente directamente después de su verificación, lo que representa una mejora notable con relación a la técnica anterior mencionada anteriormente.

Se hace referencia ahora a la **figura 3A** que ilustra un procedimiento 200 de transferencia segura de un archivo digital F según un primer modo de realización de la invención.

En este primer modo de realización, la verificación se denomina de tipo "de primer nivel" o "individual", porque se efectúa en cada uno de los paquetes $F_i$ de un conjunto de n paquetes dados $\{F_i\}_{1\leq i\leq n}$ correspondiente a la descomposición del archivo digital F a transferir.

El procedimiento 200 comprende por tanto una primera etapa 210 de escritura del archivo digital F en un primer módulo de gestión de archivos G1 de un dispositivo de transferencia segura DISP, de modo similar a la etapa 110 descrita anteriormente.

A continuación del depósito de este archivo digital F en este primer módulo de gestión de archivos G1, el procedimiento 200 comprende una etapa 215 de descomposición de este archivo digital F en un conjunto de n paquetes de datos $\{F_i\}_{1\leq i\leq n}$, de manera que pueda efectuar una verificación que trata sobre al menos uno de estos paquetes de datos. Estos paquetes $F_i$ tienen en la actualidad un tamaño inferior al tamaño máximo de paquetes dados permitiendo transferirles hacia el módulo de verificación, por ejemplo en función del tamaño de la interfaz física que permite esta transferencia.

Algunos de estos paquetes pueden contener unas meta-informaciones destinadas al módulo siguiente (por ejemplo el tamaño del archivo, su nombre, su extensión, su número de orden, etc.), con o sin parte del archivo original, como puede ser el caso cuando se utiliza un marcador de inicio y/o de final del archivo que contiene estas meta-informaciones.

Se transfiere a continuación un primer paquete $F_1$ (etapa 220) hacia un módulo de verificación V interna en el dispositivo de transferencia segura DISP, con el fin de que este proceda a una verificación de "primer nivel" en este paquete $F_1$, llamada de otra forma verificación "individual" en la medida en la que se efectúa sobre un único paquete.

Esta verificación puede consistir, por ejemplo, en verificar que todos los caracteres del paquete $F_1$ analizado pertenecen a un alfabeto limitado de caracteres posibles. La presencia de un único carácter que no pertenece a este alfabeto implica entonces un resultado negativo para esta verificación.

En este primer modo de realización, si el resultado de la verificación es negativo (etapa 235), entonces el paquete $F_1$ no se transfiere más adelante en el dispositivo de transferencia segura DISP (etapa 237), lo que interrumpe la transferencia del archivo digital F.

Si por el contrario el resultado de la verificación es positivo (etapa 235), entonces el paquete $F_1$ se transfiere hacia un segundo módulo de gestión de archivos G2 del dispositivo de transferencia segura DISP, accesible al segundo sistema informatizado PC2.

De este modo, en tanto que el resultado de la verificación sea positivo, las etapas 220 a 240 se repiten a continuación secuencialmente para cada paquete $F_i$ hasta el último paquete $F_n$, como se indica por el bucle de incremento (etapas 242 y 244) representado en la figura 3A. Si, por el contrario, uno de los paquetes $F_i$ da un resultado negativo en el transcurso de la etapa 230 de verificación, la transferencia del archivo digital F se interrumpe en esta fase (etapa 237) y este archivo digital F no pasa a estar accesible para el segundo sistema informatizado puesto que no se transfiere completamente al segundo módulo de gestión de archivos G2. En un caso de este tipo, puede enviarse una señal específica como por ejemplo una meta-información al módulo de gestión de archivos G2 para indicar que el archivo F es inválido y que debe ignorarse y/o suprimirse.

Si el procedimiento llega, después de n-1 iteraciones con resultado de verificación positivo, al último paquete $F_n$ y si este último paquete $F_n$ se verifica igualmente de manera positiva durante la etapa 230 que le concierne, el procedimiento 200 prosigue por una etapa 246 de recomposición del archivo digital F en el módulo de gestión de archivos G2, por ejemplo por concatenación secuencial de los archivos $F_i$ procedentes del módulo de verificación, de

manera que $F= F_1||...||F_I||...||F_n$.

En este caso, habiendo sido verificado individualmente cada uno de los paquetes $F_i$ del archivo digital F, el archivo digital F se verifica por paquetes y puede por tanto leerse, en el transcurso de una última etapa 250 de lectura, por el segundo sistema informatizado PC2.

Este procedimiento según un primer modo de realización es ventajoso cuando el segundo sistema informatizado, hacia el que se desea transferir el archivo digital F, no dispone más que de un grado limitado de autonomía y de análisis de los archivos recibidos, el filtrado de los archivos potencialmente nocivos se realiza en el dispositivo de transferencia segura en sí. En la medida en la que, con el procedimiento según un primer modo de realización, este segundo sistema informatizado no tiene acceso más que a archivos digitales íntegramente verificados y validados, no es necesario añadir elementos de decisión y de filtrado para la supresión de los archivos digitales potencialmente perjudiciales en este segundo sistema informatizado. El segundo sistema informatizado puede efectuar entonces verificaciones más simplistas o de otra naturaleza tal como la verificación de firmas digitales, volver a verificar el nombre de los archivos, verificar las extensiones, hacer una gestión de "versionning", etc.

Se hace referencia ahora a la **figura 3B** que ilustra un procedimiento 300 de transferencia segura de un archivo digital F según una variante del primer modo de realización de la invención.

En esta variante del primer modo de realización, el procedimiento 300 comprende las etapas 310 a 350 respectivamente similares a las etapas 210 a 250 descritas anteriormente en relación con la figura 3A, con la excepción de la etapa 337 que se aplica en caso de resultado negativo de la verificación individual de los paquetes de datos $F_i$ transmitidos secuencialmente.

En esta variante, si la etapa 330 de verificación de un paquete de datos $F_i$ da un resultado negativo, el paquete $F_i$ en cuestión se transforma por un paquete de sustitución $F_i'$ sustituyendo una parte, incluso el conjunto, de sus caracteres por caracteres de sustitución específicos, durante una etapa 337 de sustitución, antes de transmitirse (340) al segundo módulo de gestión G2 de un dispositivo de transferencia segura.

El paquete de sustitución presenta de ese modo una forma indicadora del resultado negativo de la verificación, pudiendo reconocerse como tal por el segundo sistema informatizado con el fin de que este último pueda detectar que una parte al menos del archivo digital F' leído en el segundo módulo de gestión G2 presenta una verificación que ha dado un resultado negativo.

Por ejemplo, los caracteres de sustitución pueden tomar la forma de una serie de caracteres "_".

De este modo, en esta variante, todos los paquetes de datos $F_i$ se transmiten sistemáticamente, después de la verificación y en secuencia, al segundo módulo de gestión G2, contrariamente al modo de realización ilustrado anteriormente en la figura 3A en el que la transferencia de los paquetes de datos $F_i$ se interrumpe a partir de que uno de los paquetes $F_i$ conduzca a un resultado negativo durante su verificación individual.

Se deriva de esta variante que el archivo digital F puede siempre recomponerse en el segundo módulo de gestión G2, puesto que todos los paquetes $F_i$ que lo componen se transfieren sistemáticamente hacia este módulo de gestión y por tanto que el archivo digital F' está disponible, después de la verificación individual de cada uno de sus paquetes, para lectura por el segundo sistema informatizado PC2.

Esta variante del procedimiento según un primer modo de realización es ventajosa puesto que el sistema informatizado hacia el que se desea transferir el archivo digital dispone de un cierto grado de autonomía y de análisis de los archivos recibidos y es capaz de gestionar por sí mismo unos archivos digitales en el que los elementos que pueden representar un riesgo se han convertido en inofensivos, detectándoles gracias a los datos de sustitución insertados por el procedimiento de la presente invención y suprimiéndoles eventualmente o considerando un diario de eventos en el que se anota la llegada de un archivo digital de ese tipo potencialmente nocivo.

Se hace referencia ahora a la **figura 4A** que ilustra un procedimiento 300 de transferencia segura de un archivo digital F según un segundo modo de realización de la invención.

En este segundo modo de realización, la verificación es de tipo "de segundo nivel", para distinguirse de la verificación individual de primer nivel descrita en las figuras 3A y 3B, en la medida en que esta verificación se efectúa sobre al menos una parte del archivo digital F a transferir correspondiente a varios paquetes de datos, incluso el conjunto, de este archivo digital.

A este respecto, el procedimiento 400 comprende una primera etapa 410 de escritura del archivo digital F en un primer módulo de gestión de archivos G1 de un dispositivo de transferencia segura DISP, de modo similar a la etapa 110 descrita anteriormente.

A continuación del depósito de este archivo digital F en este primer módulo de gestión de archivos G1, el

procedimiento 400 comprende una etapa 415 de descomposición de este archivo digital F en un conjunto de n paquetes de datos $\{F_i\}_{1\leq i\leq n}$, similar a la etapa 215 anterior.

Los n paquetes de datos $F_i$ se transfieren a continuación (etapa 420) hacia un módulo de verificación V interna en el dispositivo de transferencia segura DISP, con el fin de efectuar ahí una etapa 430 de verificación.

Contrariamente a la verificación individual de los paquetes del primer modo de realización descritos en las figuras 3A y 3B, la verificación del segundo modo de realización se efectúa sobre un conjunto de paquetes de datos $F_i$ entre los paquetes transferidos, incluso sobre la totalidad de los paquetes transferidos, es decir sobre el archivo digital recompuesto a partir de la totalidad de los paquetes transferidos.

En particular, esta verificación de segundo nivel puede designarse como una verificación "intermedia" si se refiere a una pluralidad de paquetes de datos entre los paquetes de datos transferidos y esta verificación puede designarse como una verificación llamada "global" si se refiere a todos los paquetes de datos transferidos en el segundo submódulo de verificación.

A modo de ejemplo, una verificación de ese tipo de segundo nivel puede tomar entonces las siguientes formas:

- si un conjunto de paquetes $F_i$ correspondientes a una línea del archivo digital F se verifica conjuntamente, lo que corresponde a la verificación intermedia, se puede verificar la presencia de un carácter específico correspondiente a un retorno de línea al final de este conjunto de paquetes o la cumplimentación de un motivo de línea específico. En ausencia de tal carácter específico o si el motivo de línea específico no se ha cumplimentado, el resultado de esta verificación de segundo nivel es negativo.
- si el conjunto del archivo digital F se recompone para analizarse totalmente, lo que corresponde a una verificación global, la verificación puede consistir entonces en verificar la presencia de una firma bien específica. En ausencia de una firma específica de ese tipo, el resultado de esta verificación de segundo nivel es negativo.
- siempre si el conjunto del archivo digital F se recompone para analizarse totalmente (verificación global del archivo), la verificación puede tratar sobre el formato de datos del archivo con el fin de verificar que este formato corresponde correctamente a un tipo de archivo que puede transferirse. Una verificación de ese tipo puede hacerse por medio de "magie numbers", por control del encabezado del archivo F para verificar un tipo de codificación particular (por ejemplo la codificación UTF8: BOM UTF-8) o controlando los primeros caracteres del archivo F indicativos del tipo de archivo en ciertos casos (GIF, JPEG, etc.).

Si el resultado de esta verificación de segundo nivel es negativo (etapa 435), es decir si el conjunto de paquetes verificado no es validado durante la etapa de verificación, entonces el procedimiento 400 de transferencia segura se interrumpe en esta fase (etapa 437) y el archivo digital F no pasa a estar accesible para el segundo sistema informatizado puesto que ninguno de sus paquetes de datos $F_i$ se transfiere al segundo módulo de gestión de archivos G2.

Por el contrario, si el resultado de esta verificación de tipo "global" es positivo (etapa 435), es decir si el conjunto de paquetes verificado es validado durante la etapa de verificación, entonces el procedimiento 400 de transferencia segura es seguido por la transferencia (etapa 440) del archivo digital F hacia el segundo módulo de gestión de archivos G2 a través de un conjunto de n paquetes de datos $\{F_i\}_{1\leq i\leq n}$ correspondiente a la descomposición del archivo digital F a transferir.

Algunos de estos paquetes $F_i$ pueden contener unas meta-informaciones destinadas al módulo siguiente (por ejemplo el tamaño del archivo, su nombre, su extensión, su número de orden, etc.), con o sin parte del archivo original, como puede ser el caso cuando se utiliza por ejemplo un marcador de inicio y/o de final del archivo que contiene dichas meta-informaciones.

En un modo de realización ventajoso, el módulo de verificación dispone de medios de almacenamiento temporal (por ejemplo de tipo RAM) que permiten el almacenamiento de los paquetes $F_i$ recibidos del primer módulo de gestión G1 y verificados en el módulo de verificación, así como su reensamblaje, después de la verificación 430, para reformar el archivo digital F en el módulo de verificación V. En dicho caso, es el archivo digital F en sí el que se transfiere durante la etapa 440 de transferencia.

Este último modo de realización es ventajoso en la medida en la que permite efectuar una verificación de tipo "global" sobre el archivo digital F en sí (como por ejemplo la verificación de una firma del archivo) mientras se efectúa una transferencia del archivo digital por paquetes, con el fin de tener en cuenta por ejemplo limitaciones de capacidad de la interfaz física situada entre el primer módulo de gestión G1 y el módulo de valoración V y, simétricamente, entre V y G2.

De este modo, en este modo de realización, el archivo digital F es recibido tal cual y almacenado por el segundo módulo de gestión G2, si se valida durante la etapa de verificación 430, con el fin de permitir su lectura por el segundo sistema informatizado.

En otra alternativa en la que el módulo de verificación no dispone de dichos medios de almacenamiento temporal, el conjunto de los paquetes $F_i$ recibidos del primer módulo de gestión G1 se transfieren al segundo módulo de gestión G2 durante la etapa 440 de transferencia, después de la validación de al menos una pluralidad de estos paquetes, incluso del conjunto de los paquetes, durante la etapa 430 de verificación.

En esta alternativa, los paquetes de datos $F_i$ recibidos por el segundo módulo de gestión G2 se reensamblan por este último con el fin de reconstituir el archivo digital F y poner este archivo a disposición del segundo sistema informatizado.

Se hace referencia ahora a la **figura 4B** que ilustra un procedimiento 500 de transferencia segura de un archivo digital F según una variante del segundo modo de realización de la invención.

De manera similar a lo que distingue la variante del primer modo de realización descrita en la figura 3B del primer modo de realización descrito en la figura 3A, el procedimiento 500 comprende las etapas 510 a 550 respectivamente similares a las etapas 410 a 450 descritas anteriormente en relación con la figura 4A, con la excepción de la etapa 537 que se aplica en caso de resultado negativo de la verificación (etapa 530) de un conjunto de paquetes entre los paquetes de datos $F_i$ transferidos del primer módulo de gestión G1 al módulo de verificación.

En esta variante, si la etapa 530 de verificación de un conjunto de paquetes de datos $F_i$, incluso del conjunto del archivo digital F, da un resultado negativo, el conjunto de paquetes $F_i$ en cuestión es sustituido por datos de sustitución, durante una etapa 537 de sustitución, antes de transmitirse (540) al segundo módulo de gestión G2 de un dispositivo de transferencia segura.

Los datos de sustitución presentan una forma indicadora del resultado negativo de la verificación y puedan reconocerse como tales por el segundo sistema informatizado, con el fin de que este último pueda detectar que el archivo digital F' leído en el segundo módulo de gestión G2 no ha sido validado durante el proceso de verificación.

Por ejemplo, los datos de sustitución pueden tomar la forma de caracteres "_".

De este modo, en esta variante, el archivo digital F se transmite sistemáticamente, después de la verificación, al segundo módulo de gestión G2, contrariamente al modo de realización ilustrado anteriormente en la figura 4A en el que la transferencia por paquetes del archivo digital F se interrumpe a partir de que la verificación efectuada sobre un conjunto de paquetes $F_i$, o sobre el archivo digital en su totalidad, presente un resultado negativo.

Se deriva de esta variante que el archivo digital F' está siempre disponible, después de la verificación al menos parcial de este archivo digital, para lectura por el segundo sistema informatizado PC2.

Como para la variante ilustrada en la figura 3B, esta variante del procedimiento según un segundo modo de realización es ventajosa cuando el segundo sistema informatizado, hacia el que se desea transferir el archivo digital, dispone de un cierto grado de autonomía y de capacidades de análisis de los archivos recibidos y es capaz de gestionar por sí mismo los archivos digitales potencialmente nocivos, detectándoles gracias a los datos de sustitución.

Se hace referencia ahora a la **figura 5A** en la que se ilustra esquemáticamente el dispositivo de transferencia segura DISP' según otro modo de realización de la presente invención.

En otro modo de realización, se busca ofrecer un doble nivel de verificación durante la transferencia segura en un archivo digital en este dispositivo DISP'.

En este sentido, el dispositivo de transferencia segura DISP' comprende un primer módulo de gestión de archivos G1 y un segundo módulo de gestión de archivos G2 similares a los del dispositivo de transferencia segura DISP descrito en la figura 1.

Como el dispositivo de transferencia segura DISP descrito en la figura 1, el dispositivo de transferencia segura DISP' comprende un módulo de verificación V, que se distingue sin embargo en que incluye un primer submódulo de verificación V1 y un segundo submódulo de verificación V2.

El primer submódulo de verificación V1 se dispone para recibir al menos un paquete de datos obtenido en el primer módulo de gestión de archivos G1 y para efectuar una primera verificación individual que trata sobre cada uno de los paquetes de datos $F_i$ transferidos desde el primer módulo de gestión de archivos G1, a la manera en que se describe en el sujeto de los procedimientos de transferencia segura 200 y 300 ilustrados en las figuras 3A y 3B.

El segundo submódulo de verificación V2 es adecuado para recibir al menos un paquete de datos verificados individualmente por el primer submódulo de verificación, por medio de una interfaz física B3 de tipo bus de memoria y se dispone para efectuar una segunda verificación que trata sobre al menos uno de los paquetes de datos recibidos del primer submódulo de verificación.

Es posible así ofrecer un doble nivel de verificación que permita reforzar la seguridad de la transferencia de datos.

En un primer modo de realización, la verificación efectuada en el segundo submódulo de verificación V2 puede ser del mismo nivel que el efectuado en el primer submódulo de verificación V1, es decir que puede ser de tipo individual y efectuarse paquete por paquete, utilizando sin embargo criterios de verificación diferentes a los empleados durante la primera verificación.

En otro modo de realización ventajoso, la verificación efectuada en el segundo submódulo de verificación V2 se realiza a un nivel diferente, más amplio, que el efectuado en el primer submódulo de verificación V1, es decir que trata no ya sobre un único paquete de datos, sino sobre un conjunto de paquetes de datos, lo que permite detectar una variedad mayor de defectos potenciales en este archivo digital F.

En este otro modo de realización ventajoso, el segundo submódulo de verificación V2 es entonces adecuado para recibir todos los paquetes de datos verificados por el primer submódulo de verificación y se dispone para efectuar una segunda verificación (de segundo nivel) que trata sobre varios paquetes entre los paquetes de datos $F_i$ transferidos recibidos desde el primer submódulo de verificación V1, a la manera en que se describe en el sujeto de los procedimientos de transferencia segura 400 y 500 ilustrados en las figuras 4A y 4B y que se han designado aquí por verificación intermedia. Es posible entonces aplicar dos niveles diferentes de verificación a los datos a transferir con el fin de asegurar mejor la transferencia.

En otro modo de realización particularmente ventajoso en el que el segundo submódulo de verificación V2 es adecuado para recibir todos los paquetes de datos verificados por el primer submódulo de verificación, el segundo submódulo de verificación V2 se dispone para efectuar una segunda verificación (de segundo nivel) que trata sobre el conjunto de los paquetes de datos $F_i$ recibidos del primer submódulo de verificación V1, siempre a la manera en que se describe en el sujeto de los procedimientos de transferencia segura 400 y 500 ilustrados en las figuras 4A y 4B y que se han designado aquí por verificación global. Es posible así combinar una verificación individual por paquetes con una verificación global que trata sobre el conjunto del archivo a transmitir con el fin de asegurar mejor la transferencia de este archivo.

En un modo de realización ventajoso, el segundo submódulo de verificación V2 dispone de medios de almacenamiento temporal (por ejemplo de tipo RAM) que permiten el almacenamiento de los paquetes $F_i$ verificados y recibidos del primer submódulo de verificación V1, así como su reensamblaje para reformar el archivo digital F en el segundo submódulo de verificación V2, lo que permite transferir el archivo digital F en sí al segundo módulo de gestión de archivos G2.

Este modo de realización es ventajoso en la medida en la que permite efectuar una verificación "global" sobre el archivo digital F en sí (como por ejemplo la verificación de una firma sobre el conjunto del archivo digital F) mientras se efectúa una transferencia del archivo digital por paquetes entre el primer módulo de gestión G1 y el segundo submódulo de verificación V2, con el fin de tener en cuenta por ejemplo limitaciones de capacidad de las interfaces físicas B1 y B3 situadas entre estos dos elementos.

La **figura 5B** ilustra un procedimiento 600 de transferencia segura según un tercer modo de realización de la invención, que es aplicable en particular al dispositivo de transferencia segura DISP' descrito en la figura 5A.

En este tercer modo de realización, las ventajas de estos procedimientos según un primero y el segundo modo de realización tal como se describen anteriormente en las figuras 3A, 3B, 4A y 4B se combinan.

El procedimiento 600 comprende así una primera etapa 610 de escritura del archivo digital F en un primer módulo de gestión de archivos G1 de un dispositivo de transferencia segura DISP' tal como se describe en la figura 5A, de modo similar a la etapa 110 descrita anteriormente.

A continuación del depósito de este archivo digital F en este primer módulo de gestión de archivos G1, el procedimiento 600 comprende una etapa 615 de descomposición de este archivo digital F en un conjunto de n paquetes de datos $\{F_i\}_{1\leq i\leq n}$

Un primer paquete $F_1$, se transfiere a continuación (etapa 620) hacia el primer submódulo de verificación V1 interno al dispositivo de transferencia segura DISP', con el fin de que este proceda a una primera verificación individual, de primer nivel, sobre este paquete F, durante la etapa 630 de verificación.

Como en el procedimiento 200 ilustrado en la figura 3A, esta primera verificación individual puede consistir en verificar que todos los caracteres del paquete $F_1$ pertenezcan a un alfabeto determinado.

Si el resultado de la primera verificación es negativo (etapa 631), son posibles entonces dos opciones, de manera similar a las opciones descritas respectivamente en las figuras 3A y 3B:

- o bien el paquete $F_1$ no se transfiere más adelante en el dispositivo de transferencia segura DISP' (etapa 632), lo que impide la transferencia del archivo digital F en este dispositivo y el procedimiento 600 de transferencia se interrumpe;
- o bien el paquete $F_1$ es reemplazado por un paquete de sustitución $F_1$' como se ha descrito anteriormente, durante una etapa 633 de sustitución, antes de transmitirse (etapa 634) al segundo submódulo de verificación V2 del dispositivo de transferencia segura DISP'.

Si por el contrario el resultado de la primera verificación es positivo (etapa 631), entonces el paquete $F_1$ se transfiere (etapa 634) hacia el segundo submódulo de verificación V2 del dispositivo de transferencia segura DISP'.

Mientras que el resultado de la primera verificación individual por paquete sea positivo, las etapas 620 a 634 se repiten a continuación secuencialmente para cada paquete $F_i$; hasta el último paquete $F_n$, como se indica por el bucle de incremento (etapa 635 y 636) representado en la figura 5B.

Si uno de los paquetes $F_i$ da un resultado negativo en el transcurso de la etapa 630 de verificación, hay o bien una interrupción en esta fase (etapa 633) del procedimiento 600 y el archivo digital F' no pasa a estar accesible al segundo sistema informatizado puesto que no se ha transferido completamente al segundo submódulo de verificación V2, o bien una sustitución (etapa 632) del paquete de datos $F_i$ implicado por un paquete de sustitución.

Si el procedimiento 600 llega, después de n-1 iteraciones con unos resultados de verificación positivos durante la etapa 630, al último paquete $F_n$ y si este último paquete $F_n$ se verifica igualmente de manera positiva durante la etapa 630 que le concierne, el procedimiento 600 se prosigue por una segunda verificación de segundo nivel (etapa 637), se trata sobre algunos, incluso el conjunto, de los paquetes $F_i$ recibidos por el segundo submódulo de verificación V2, de manera similar a lo que se describe en las figuras 4A y 4B.

Como para la verificación de segundo nivel descrita en las figuras 4A y 4B, esta segunda verificación puede consistir en buscar un carácter específico de retorno de línea, verificar la pertenencia a un cierto tipo de archivos, incluso verificar la firma del archivo, etc.

Si el resultado de esta segunda verificación es positivo (etapa 638), es decir si el conjunto de paquetes verificados es validado durante la etapa de verificación 637, entonces el procedimiento 600 de transferencia segura se prosigue por la transferencia (etapa 640) del archivo digital F hacia el segundo módulo de gestión de archivos G2, ya sea en la forma del archivo digital F en sí (recompuesto, por ejemplo por concatenación, a partir de los n paquetes $F_i$ en el segundo submódulo de verificación), o bien en la forma de paquetes $F_i$ en cuyo caso el archivo digital F se recompone, por ejemplo por concatenación, en el segundo módulo de gestión de archivos G2.

En estos dos casos de figuras, el archivo digital F se recupera íntegramente en el segundo submódulo de gestión de archivos G2 en el que está disponible para lectura (etapa 650) para el segundo sistema informatizado.

Por el contrario, si el resultado de esta segunda verificación es negativo (etapa 638), es decir si el conjunto de paquetes verificados no es validado durante la etapa de verificación 637, son posibles entonces dos opciones, de manera similar a las opciones descritas respectivamente en las figuras 4A y 4B:

- o bien el procedimiento 600 de transferencia segura se interrumpe en esta fase (etapa 632) y el archivo digital F no pasa a estar accesible al segundo sistema informatizado puesto que ninguno de sus paquetes de datos $F_i$ se transfiere al segundo módulo de gestión de archivos G2;

- o bien el conjunto de paquetes verificados es reemplazado por datos de sustitución (etapa 639), como se ha descrito anteriormente en el sujeto de la etapa 537 de la figura 4B, antes de transmitirse (etapa 640) al segundo módulo de gestión de archivos G2 del dispositivo de transferencia segura DISP'.

Por supuesto, la invención no está limitada a los ejemplos de realización descritos más arriba y representados, a partir de los que se podrán prever otros modos y otras formas de realización, sin, por ello, salirse del marco de la invención.

En particular, se han descrito anteriormente unos modos de realización ilustrativos que describen o bien una verificación de primer nivel, individual, sobre paquetes solamente, o bien una verificación de segundo nivel, más amplia, sobre conjuntos de paquetes o sobre el conjunto del archivo digital, o bien la combinación de estos dos tipos de verificaciones.

La invención no se limita sin embargo a estos únicos modos de realización ilustrativos y cubre igualmente cualquier combinación de diferentes niveles de verificación.

Se puede así imaginar perfectamente un dispositivo que disponga de tres submódulos de verificación con el fin de efectuar la verificación respectivamente en tres niveles distintos:

- un primer nivel en el que los paquetes de datos $F_i$ se verifican secuencialmente e individualmente, similarmente a lo que se describe en las figuras 3A y 3B;
- un segundo nivel intermedio en el que unos conjuntos de paquetes de datos $F_i$ que corresponden a líneas del archivo digital F se reensamblan con el fin de efectuar una verificación por línea, según el principio descrito en las figuras 4A y 4B;
- un tercer nivel global, finalmente, en el que el conjunto del archivo digital F se recompone a partir de los paquetes de datos $F_i$ y se verifica de manera global, por ejemplo por medio de la verificación de una firma aplicada al archivo digital.

**REIVINDICACIONES**

1. Procedimiento de transferencia segura de un archivo digital (F) que procede de un primer sistema informatizado hacia al menos un segundo sistema informatizado a través de un dispositivo de transferencia segura, que comprende:

- la escritura (110) del archivo digital en un primer módulo de gestión de archivos (G1) del dispositivo de transferencia segura (DISP), siendo adecuado dicho primer módulo de gestión de archivos para almacenar dicho archivo digital recibido del primer sistema informatizado;
- la transferencia (120) del archivo digital hacia un módulo de verificación (V) interno del dispositivo de transferencia segura;
- la verificación (130) de al menos una parte del archivo digital transferido en el módulo de verificación;
- la transferencia (140) del archivo digital al menos parcialmente verificado hacia un segundo módulo de gestión de archivos (G2) del dispositivo de transferencia segura en función del resultado de dicha verificación;

comprendiendo además una etapa de conformación (215) del archivo digital descrito en el primer módulo de gestión de archivos que comprende la división de dicho archivo digital en una pluralidad de paquetes de datos ($F_i$) de tamaño inferior a un tamaño máximo de paquetes de datos que permite la transferencia hacia el módulo de verificación, tratando la verificación sobre al menos uno de dichos paquetes de datos;
en el que el módulo de verificación comprende un primer submódulo de verificación (V1), comprendiendo la etapa de transferencia transferir (620) al menos uno de dichos paquetes de datos hacia el primer submódulo de verificación y comprendiendo la etapa de verificación una primera verificación individual (630) que trata sobre cada uno de dichos paquetes transferidos en el primer submódulo de verificación;
en el que el módulo de verificación comprende además un segundo submódulo de verificación (V2), **caracterizado por que** la etapa de verificación comprende además la transferencia (634) de al menos uno de los paquetes de datos verificados individualmente en el primer submódulo de verificación hacia el segundo submódulo de verificación y una segunda verificación (637) que trata sobre al menos uno de los paquetes de datos transferidos en el segundo submódulo de verificación.

2. Procedimiento de transferencia segura según la reivindicación 1, en el que todos los paquetes de datos verificados individualmente se transfieren hacia el segundo submódulo de verificación, **caracterizado por que** la segunda verificación es una verificación intermedia que trata sobre una pluralidad de paquetes de datos entre los paquetes de datos transferidos en el segundo submódulo de verificación.

3. Procedimiento de transferencia segura según la reivindicación 1, en el que todos los paquetes de datos verificados individualmente se transfieren hacia el segundo submódulo de verificación, **caracterizado por que** la segunda verificación es una verificación global que trata sobre todos los paquetes de datos transferidos en el segundo submódulo de verificación.

4. Procedimiento de transferencia segura según una de las reivindicaciones 1 a 3, **caracterizado por que**, si el resultado de la verificación individual de uno de dichos paquetes recibidos por el primer submódulo de verificación y/o de la segunda verificación es negativo, la transferencia de los paquetes de datos se interrumpe (237, 632).

5. Procedimiento de transferencia segura según una de las reivindicaciones 1 a 3, **caracterizado por que**, si el resultado de la verificación individual de uno de dichos paquetes recibidos por el primer submódulo de verificación es negativo, el paquete de datos cuya verificación da un resultado negativo es reemplazado por un paquete de datos de sustitución (337, 639).

6. Dispositivo de transferencia segura de datos adecuado para conectarse a un primer sistema informatizado y a un segundo sistema informatizado, que comprende:

- un primer módulo de gestión de archivos (G1) adecuado para almacenar un archivo digital (F) recibido del primer sistema informatizado;
- un módulo de verificación (V) dispuesto para recibir el archivo digital almacenado en el primer módulo de gestión de archivos y para efectuar una verificación sobre al menos una parte del archivo digital recibido;
- un segundo módulo de gestión de archivos (G2) adecuado para recibir el archivo digital del módulo de verificación;

en el que el primer módulo de gestión de archivos se conecta al módulo de verificación por medio de una interfaz física (B1), disponiéndose el primer módulo de gestión de archivos para dividir el archivo digital en una pluralidad de paquetes de datos ($F_i$) de tamaño inferior a un tamaño máximo de datos que pueden transferirse sobre dicha interfaz física, disponiéndose el módulo de verificación para efectuar una verificación sobre al menos uno de dichos paquetes de datos ($F_i$);
el módulo de verificación incluye un primer submódulo de verificación (V1) dispuesto para recibir al menos uno de los paquetes de datos ($F_i$) obtenidos en el primer módulo de gestión de archivos y para efectuar una primera verificación individual que trata sobre cada uno de los paquetes de datos recibidos;

el módulo de verificación incluye además un segundo submódulo de verificación (V2) adecuado para recibir al menos un paquete de datos verificado individualmente en el primer submódulo de verificación y dispuesto para efectuar una segunda verificación que trata sobre al menos un paquete de datos recibido del primer submódulo de verificación;
el segundo submódulo de verificación se dispone para transmitir al menos un paquete de datos verificado hacia el segundo módulo de gestión de archivos en función del resultado de la segunda verificación que trata sobre dicho al menos un paquete de datos y el segundo módulo de gestión de archivos se dispone para recomponer el archivo digital a partir de los paquetes de datos verificados recibidos del segundo submódulo de verificación.

7. Dispositivo de transferencia segura según la reivindicación 6, en el que el segundo submódulo de verificación es adecuado para recibir todos los paquetes de datos verificados individualmente en el primer submódulo de verificación, **caracterizado por que** la segunda verificación es una verificación intermedia que trata sobre una pluralidad de paquetes entre los paquetes de datos recibidos del primer submódulo de verificación.

8. Dispositivo de transferencia segura según la reivindicación 6, en el que el segundo submódulo de verificación es adecuado para recibir todos los paquetes de datos verificados individualmente en el primer submódulo de verificación, **caracterizado por que** la segunda verificación es una verificación global que trata sobre todos los paquetes de datos recibidos del primer submódulo de verificación.

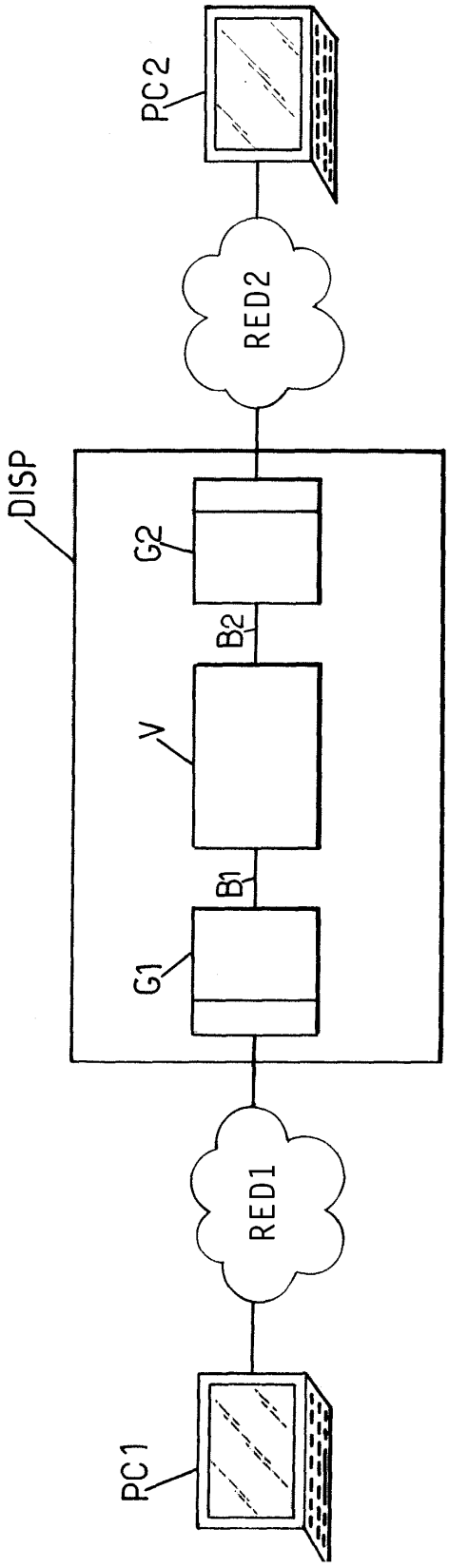



FIG.1.

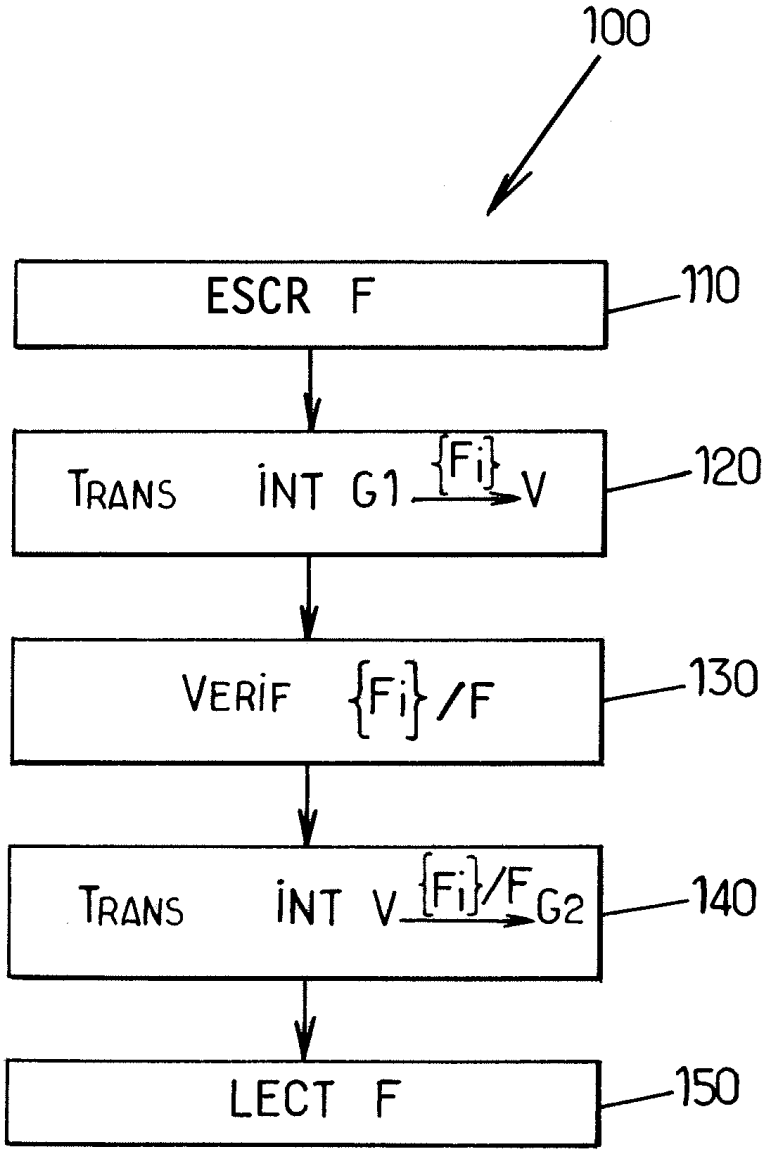

100
ESCR F
110
TRANS INT G1 {Fi} V
120
VERIF {Fi}/F
130
TRANS INT V {Fi}/F G2
140
LECT F
150

FIG. 2.

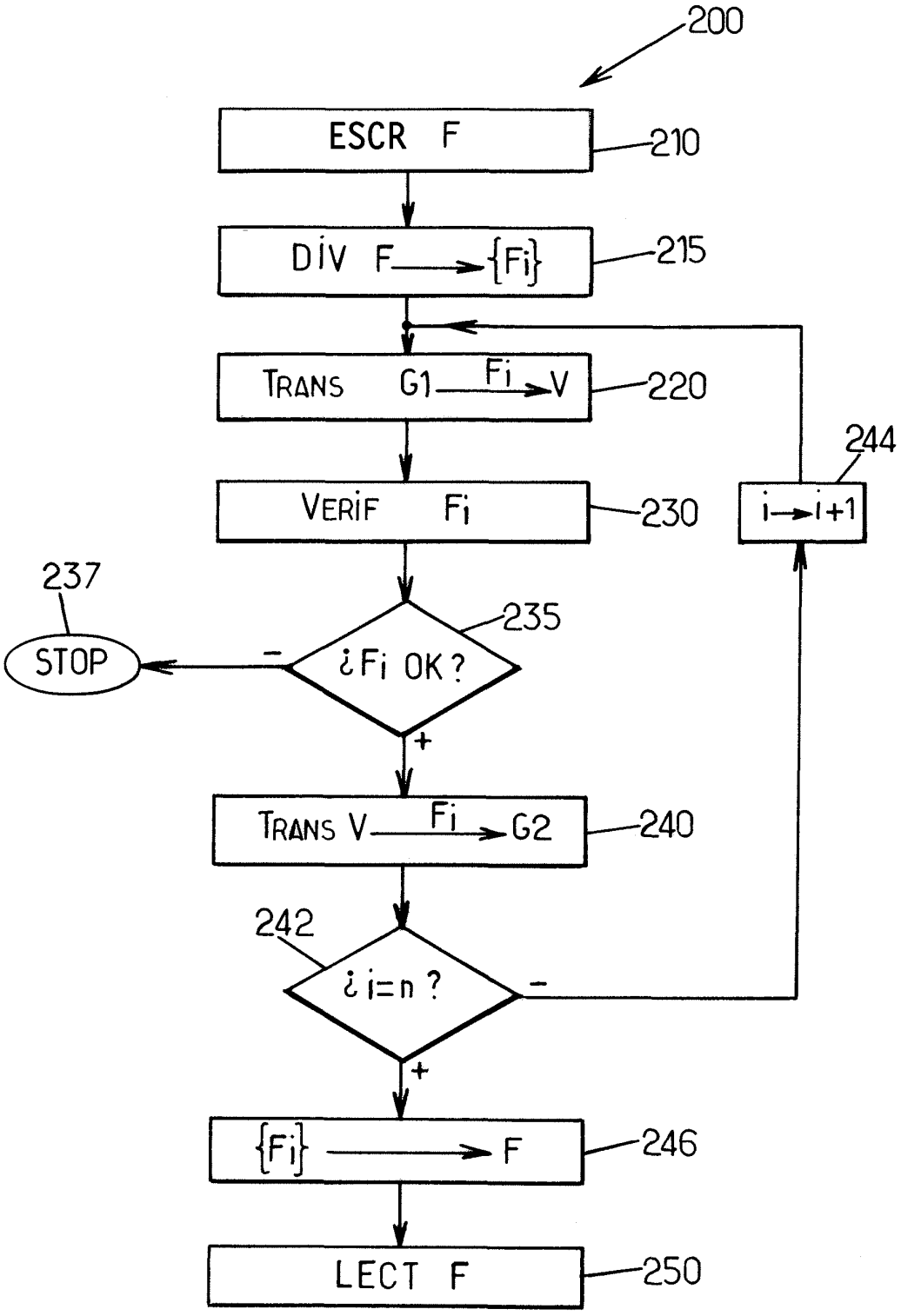

200
ESCR F
210
DIV F → {Fi}
215
TRANS G1 Fi → V
220
VERIF Fi
230
244
i → i+1
237
STOP
235
¿Fi OK?
-
+
TRANS V Fi → G2
240
242
¿i=n ?
-
+
{Fi} → F
246
LECT F
250

FIG.3A.

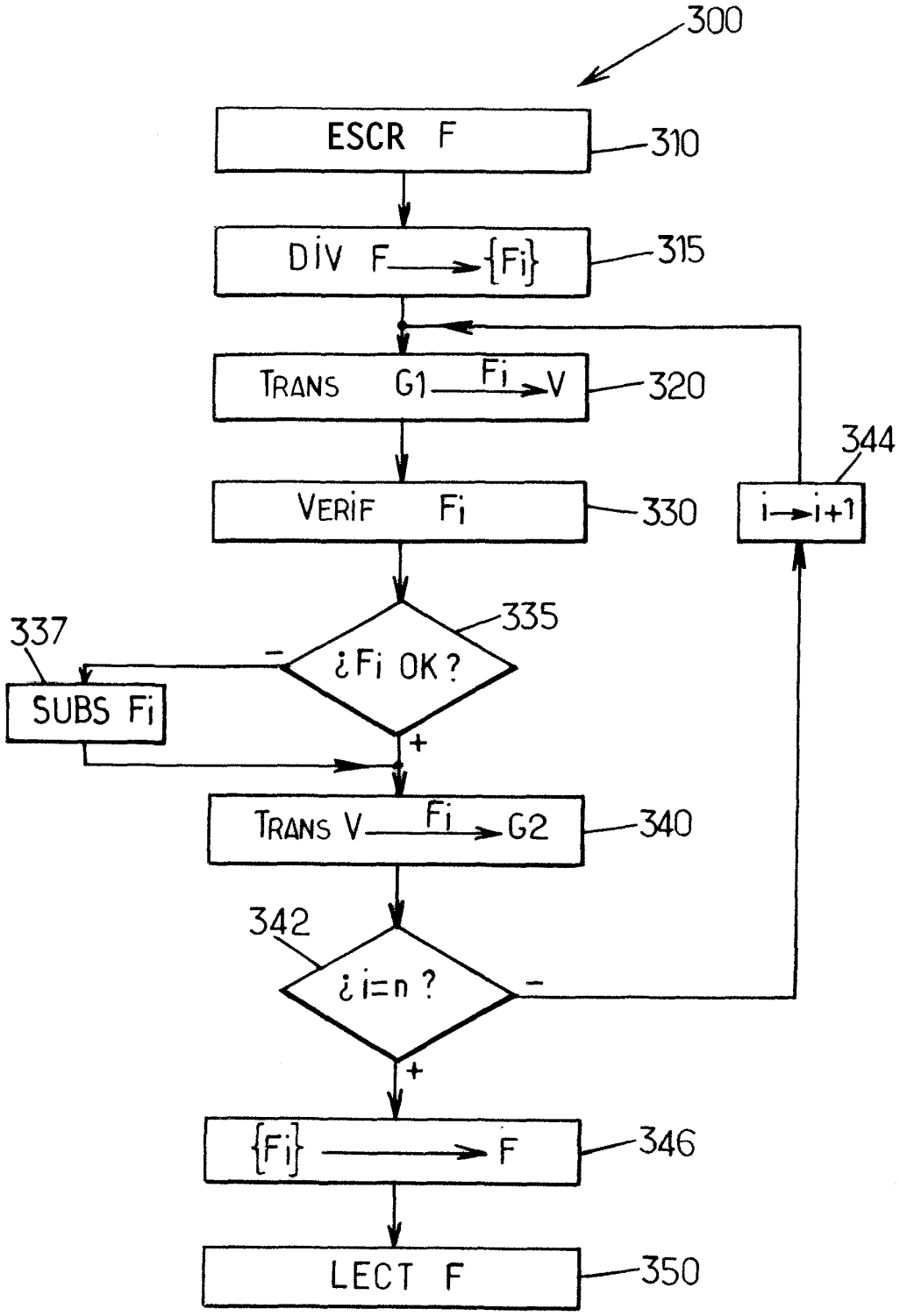

300
ESCR F
310
DIV F → {Fi}
315
TRANS G1 Fi → V
320
344
VERIF Fi
330
i → i+1
335
337
¿Fi OK?
SUBS Fi
TRANS V Fi → G2
340
342
¿i=n ?
{Fi} → F
346
LECT F
350

FIG.3B.

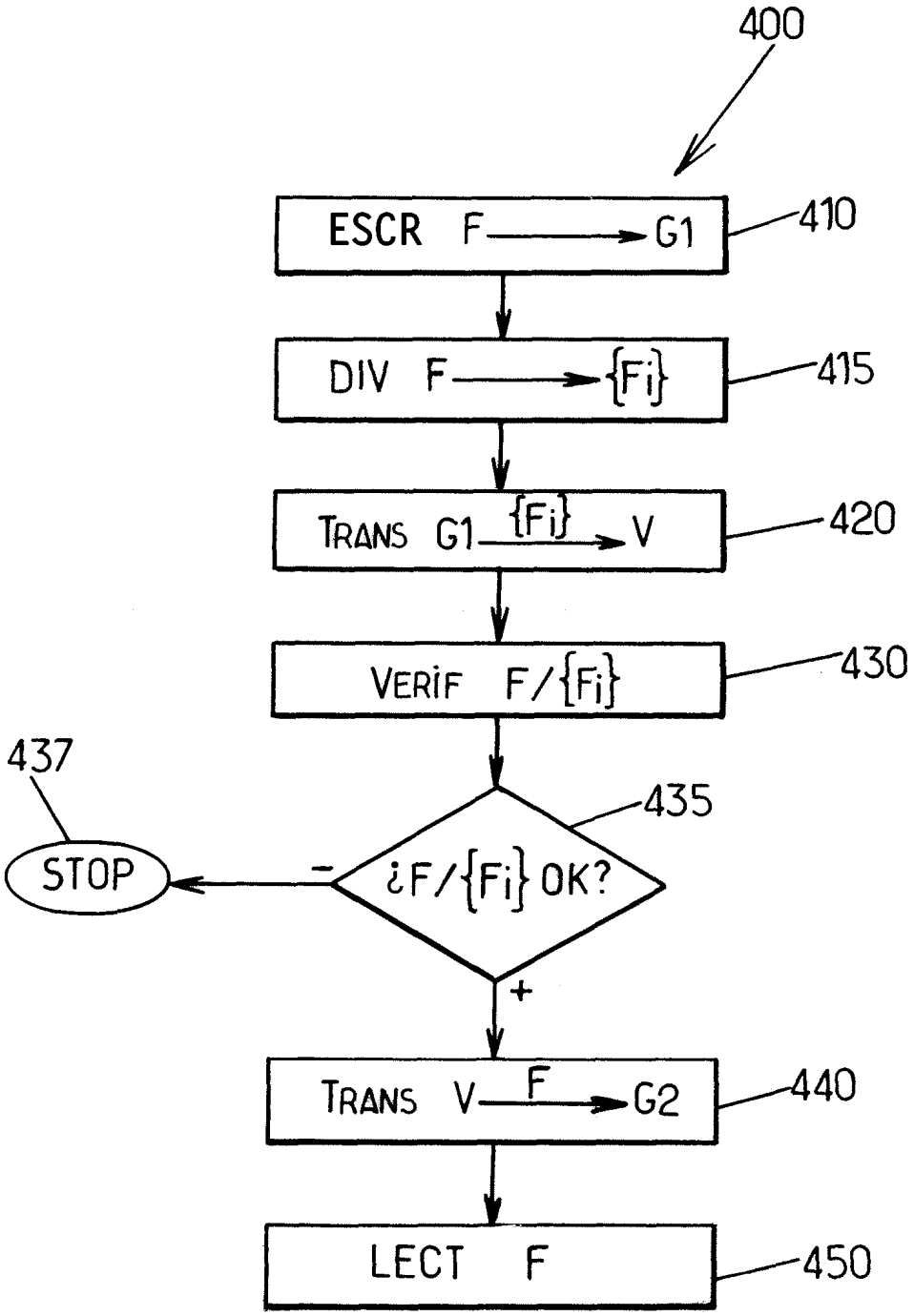

400
ESCR F → G1
410
DIV F → {Fi}
415
TRANS G1 {Fi} → V
420
VERIF F/{Fi}
430
437
435
STOP
¿F/{Fi} OK?
-
+
TRANS V F → G2
440
LECT F
450

FIG.4A.

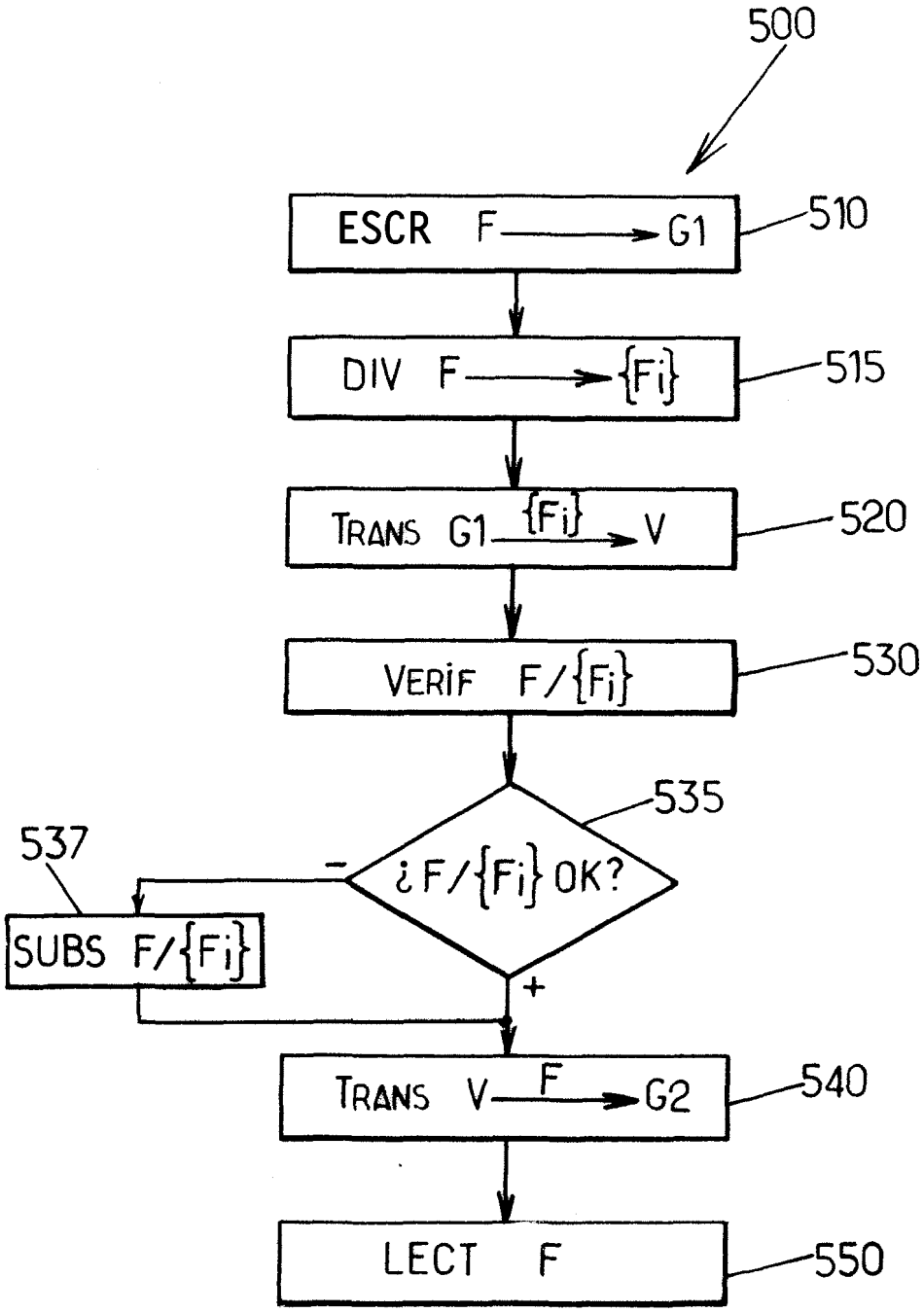

500
ESCR F → G1
510
DIV F → {Fi}
515
TRANS G1 {Fi} → V
520
VERIF F/{Fi}
530
535
¿F/{Fi} OK?
537
SUBS F/{Fi}
TRANS V F → G2
540
LECT F
550

FIG.4B.

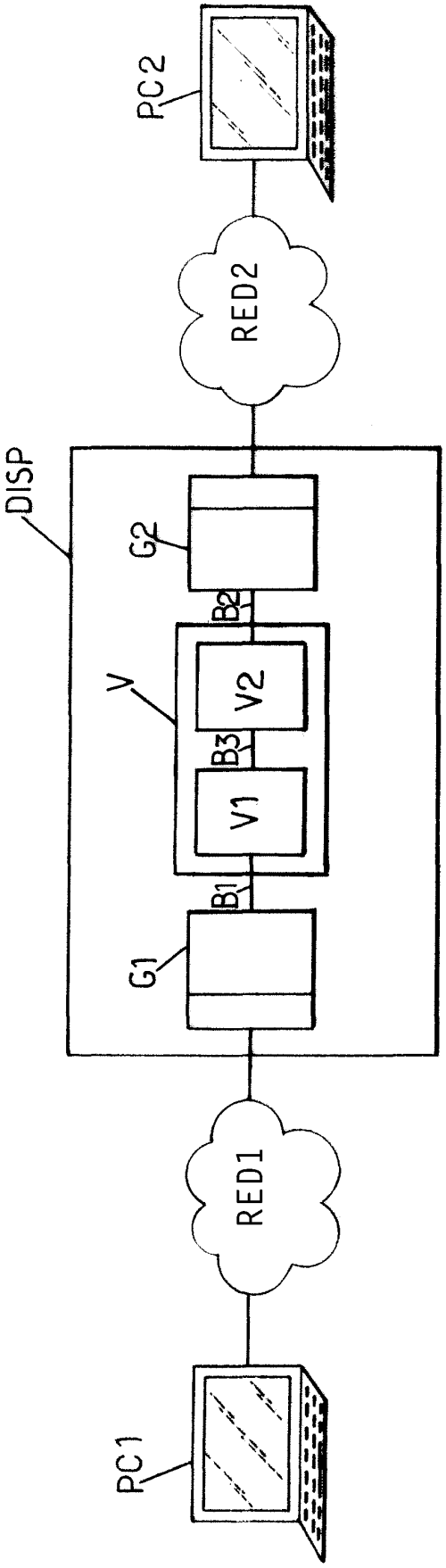
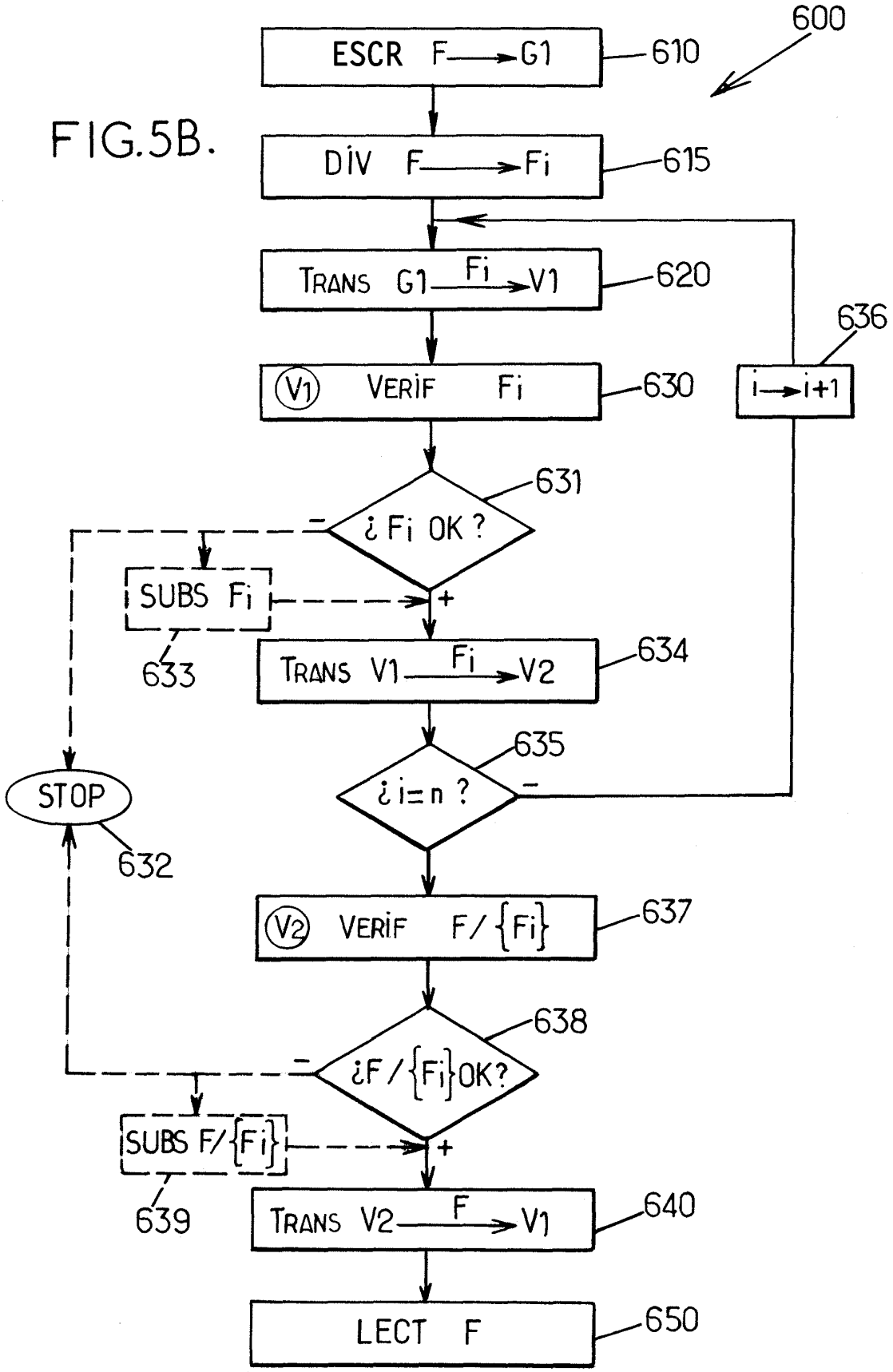



FIG.5A.

FIG.5B.


600
ESCR F→G1
610
DIV F→Fi
615
TRANS G1 Fi→V1
620
636
(V1) VERIF Fi
630
i→i+1
631
¿ Fi OK ?
SUBS Fi
633
TRANS V1 Fi→V2
634
635
¿ i=n ?
STOP
632
(V2) VERIF F/{Fi}
637
638
¿F/{Fi}OK?
SUBS F/{Fi}
639
TRANS V2 F→V1
640
LECT F
650