(19) OFICINA ESPAÑOLA DE PATENTES Y MARCAS

ESPAÑA

(11) Número de publicación: **2 337 370**

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

(12) TRADUCCIÓN DE PATENTE EUROPEA T3

(96) Número de solicitud europea: **05253771 .9**
(96) Fecha de presentación : **17.06.2005**
(97) Número de publicación de la solicitud: **1734719**
(97) Fecha de publicación de la solicitud: **20.12.2006**

(54) Título: **Codificación de mensajes para utilizar en un sistema de comunicación basado en el estado de clasificación de seguridad.**

(45) Fecha de publicación de la mención BOPI:
23.04.2010

(45) Fecha de la publicación del folleto de la patente:
23.04.2010

(73) Titular/es: **Research In Motion Limited**
295 Phillip Street
Waterloo, Ontario N2L 3W8, CA

(72) Inventor/es: **Brown, Michael K.;**
Little, Herbert A.;
Brown, Michael S.;
McCallum, Michael E.;
Totzke, Scott W. y
Adams, Neil P.

(74) Agente: **Elzaburu Márquez, Alberto**

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

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

DESCRIPCIÓN

Codificación de mensajes para utilizar en un sistema de comunicación basado en el estado de clasificación de seguridad.

Antecedentes

1. **Campo de la tecnología**

Esta solicitud se refiere en general a sistemas de comunicaciones capaces de codificar mensajes para fines de seguridad.

2. **Técnica relacionada**

El documento US 2003/0182435 A1 describe un sistema y método para extractar informaciones sensibles a la seguridad desde un objeto de datos y separar la información extractada del resto del documento.

El documento EP-A-1494121 describe un método y aparato para cambiar un modo de comunicación para un dispositivo basándose en su entorno.

Gobiernos, y algunas corporaciones, usan típicamente un sistema de clasificación de seguridad para determinar el nivel de sensibilidad de la información contenida en documentos y correos electrónicos. Dicho sistema de clasificación de seguridad varía entre países diferentes y diferentes organizaciones.

Una vez que se establece el nivel de clasificación de información, es importante asegurarse de que siempre se apliquen uniformemente las políticas de seguridad apropiadas. Cuando se aplican clasificaciones al correo electrónico, lo que se necesita es un método para hacer cumplir una codificación de mensajes apropiada basada en el estado de clasificación establecido (por ejemplo, nivel de clasificación, intensidad de cifrado, etc.).

Existe una solución anterior para añadir clasificación a mensajes Outlook (marca registrada propiedad de Microsoft Corporation). Se llama “Classify” y se encuentra en la Red Mundial Global en “markwilson.ca/products.html”. El producto es un pug-in para Outlook (marca registrada) que permite a uno añadir clasificación a un mensaje. Sin embargo, el nivel de clasificación no está necesariamente vinculado a codificación de mensajes. Por consiguiente, no hay ninguna manera de hacer cumplir, por ejemplo, que todos los mensajes “secretos” y anteriores tengan que ser cifrados.

Sumario

Para resolver este problema, permitimos que el Administrador de Tecnología de Información (IT) (a través de Política IT) establezca una correspondencia deseada entre estados de clasificación disponibles y los correspondientes niveles de codificación de mensajes aplicables. Esto podría ser una correspondencia explícita (tal como “Secreto” = “Cifrado”) o podría ser una serie de mínimos (tal como “Confidencial” >=“Firmado”).

Esta información, por ejemplo, podría ser “impulsada” a un dispositivo remoto de comunicación inalámbrica a través de dicha política IT. Una vez residente en el dispositivo, cuando el usuario desee enviar un mensaje, la lógica de aplicación del dispositivo miraría el nivel de clasificación actual establecido por el usuario y comparar la codificación actual de mensajes con aquélla en que debe basarse en política IT. Si no está especificada, naturalmente, sólo puede enviarse como está. Si está especificada, y la codificación actualmente especificada para su uso no es al menos de la intensidad mínima requerida, la codificación sería subida automáticamente al nivel apropiado (es decir, desde Plaintext a Firmado y Cifrado). Preferiblemente, esto sería perfecto para el usuario.

Esta lógica de codificación hecha cumplir puede hacerse también más granular que sólo especificando la codificación de mensajes codificada. Por ejemplo, como variación adicional, el Administrador de IT podría también (o en lugar de) especificar un nivel de “intensidad” para indicar algoritmos que deberían usarse para el cifrado. Por ejemplo, una clasificación de “Secreto” puede corresponder a una intensidad “fuerte” que podría significar que los algoritmos públicos clave usados tienen que ser >=2048 bits y el algoritmo simétrico tiene que ser AES-192 o superior. Pero clasificación “Muy Secreto” puede corresponder a “Extra Fuerte” que significaría que los algoritmos públicos clave usados tienen que ser >=4096 bits y el algoritmo simétrico tiene que ser AES-256 o superior.

Estas realizaciones pueden ser conseguidas en equipo físico, equipo lógico o una combinación de equipo físico y equipo lógico y proporcionan un método para mejorar la posibilidad de codificar mensajes basándose en el estado de clasificación (por ejemplo, en un dispositivo de comunicación inalámbrica). Las realizaciones ilustrativas ser conseguidas al menos en parte mediante un código de programa informático ejecutable que puede ser incorporado en medios físicos de memoria digital.

Breve descripción de los dibujos

Los objetos y ventajas de la solución descrita en esta memoria se entenderán y se apreciarán mejor en unión de la siguiente descripción detallada de realizaciones ilustrativas tomadas junto con los dibujos que se acompañan, en los que:

La figura 1 es una vista esquemática extensa de sistema global de un sistema de comunicación de correo electrónico inalámbrico ilustrativo que incorpora un dispositivo móvil de comunicación inalámbrica que tiene capacidad mejorada para codificar mensajes basándose en el estado de clasificación;

La figura 2 es un diagrama esquemático abreviado de equipo físico incluido dentro de un dispositivo móvil ilustrativo de comunicación inalámbrica;

La figura 3 es un organigrama esquemático abreviado ilustrativo de equipo lógico informático (es decir, lógica de programas) que puede ser utilizado en el dispositivo de la figura 2 para hacer cumplir una Política IT de codificación de cifrado según el estado de clasificación (por ejemplo, nivel de clasificación o intensidad de cifrado);

La figura 4 es una tabla que representa una Política IT ilustrativa para su uso en la lógica de programas de la figura 3; y

La figura 5 es un organigrama esquemático abreviado ilustrativo de equipo lógico informático (es decir, lógica de programas) que puede ser utilizado en el dispositivo de la figura 2 para asegurar al menos un nivel mínimo de codificación.

Descripción detallada de realizaciones ilustrativas

La figura 1 es una visión general de un sistema de comunicación ilustrativo en el que puede usarse un dispositivo de comunicación inalámbrica 100. Una persona versada en la materia apreciará que puede haber cientos de topologías diferentes de sistemas. Puede haber también muchos remitentes y destinatarios de mensajes. El sistema ilustrativo sencillo mostrado en la figura 1 es para fines ilustrativos solamente, y muestra tal vez el entorno de correo electrónico por Internet actualmente más dominante.

La figura 1 muestra un remitente de correos electrónicos 10, la Internet 12, un sistema de servidores de mensajes 14, una puerta inalámbrica 16, una infraestructura inalámbrica 18, una red inalámbrica 20 y un dispositivo de comunicaciones móvil 100.

Un remitente de correos electrónicos 10 puede estar conectado, por ejemplo, a un ISP (Proveedor de Servicios de Internet), en el que un usuario del sistema tiene una cuenta, ubicada dentro de una compañía, posiblemente conectada a una red de área local (LAN), y conectado a la Internet 12, o conectado a la Internet 12 a través de un ASP grande (proveedor de servicios de aplicaciones) tal como America Online™ (AOL). Los versados en la materia apreciarán que los sistemas mostrados en la figura 1 pueden conectarse en lugar de ello a una red de área amplia (WAN) distinta de la Internet, aunque las transferencias de correos electrónicos son realizadas corrientemente a través de disposiciones conectadas a Internet como se muestra en la figura 1.

El servidor de mensajes 14 puede implementarse, por ejemplo, en un ordenador de red dentro de un cortafuegos de una corporación, un ordenador dentro de un sistema ISP o ASP o similar, y actúa de interfaz principal para intercambio de correos electrónicos a través de la Internet 12. Si bien otros sistemas de mensajería pudieran no requerir un sistema de servidores de mensajes 14, un dispositivo móvil 100 configurado para recibir y posiblemente enviar correo electrónico estará normalmente asociado con una cuenta en un servidor de mensajes. Tal vez los dos servidores de mensajes más corrientes sean Microsoft Exchange™ y Lotus Domino™. Estos productos se usan a menudo en unión de encaminadores de correo a través de Internet que dirigen y entregan correo. Estos componentes intermedios no se muestran en la figura 1, ya que no desempeñan directamente un papel en la invención descrita en lo que sigue. Los servidores de mensajes tal como el servidor 14 se extienden típicamente más allá de sólo enviar y recibir correo electrónico; incluyen también motores dinámicos de almacenamiento de bases de datos para datos como calendarios, listas de cosas pendientes de hacer, listas de tareas, correo electrónico y documentos.

La puerta Inalámbrica 16 y la infraestructura 18 proporcionan un enlace entre la Internet 12 y la red inalámbrica 20. La infraestructura inalámbrica 18 determina la red más probable para localizar un usuario dado y sigue a los usuarios cuando vagabundean entre países o redes. Un mensaje es entregado entonces al dispositivo móvil 100 por transmisión inalámbrica, típicamente a una radiofrecuencia (RF), desde una estación de base en la red inalámbrica 20 al dispositivo móvil 100. La red particular 20 puede ser virtualmente cualquier red inalámbrica a través de la cual puedan ser intercambiados mensajes con un dispositivo de comunicaciones de móvil.

Como se muestra en la figura 1, un remitente de correo electrónico 10, situado en algún lugar de la Internet 12, envía un mensaje de correo electrónico compuesto 22. Este mensaje 22 usa típicamente Protocolo Simple de Transferencia de Correo (SMTP), cabeceras RFC 822 y partes de cuerpo de Extensión Multipropósito de Correo de Internet (MIME) para definir el formato del mensaje de correo. Estas técnicas son todas ellas bien conocidas por los expertos en la materia. El mensaje 22 llega al servidor de mensajes 14 y es almacenado normalmente en una memoria

de mensajes. Los sistemas de mensajería más conocidos soportan un esquema de acceso de mensaje llamado "pull", en el que el dispositivo móvil 100 tiene que pedir que los mensajes almacenados sean pasados por el servidor de mensajes al dispositivo móvil 100. Algunos sistemas proporcionan encaminamiento automático de tales mensajes que son dirigidos usando una dirección específica de correo electrónico con el dispositivo móvil 100. En una realización preferida, los mensajes dirigidos a una cuenta de servidor de mensajes asociada con un sistema de anfitrión tal como un ordenador personal u ordenador de oficina que pertenezca al usuario de un dispositivo móvil 100 son redirigidos desde el servidor de mensajes 14 al dispositivo móvil 100 cuando son recibidos. Los mensajes serán típicamente cifrados desde el remitente al destinatario utilizando una clave que sea única para un dispositivo dado. Ejemplos de dos métodos corrientemente usados son Estándar de Cifrado de Datos (Triple - DES) y Estándar de Cifrado Avanzado (AES).

Independientemente del mecanismo específico que controle el envío de mensajes al dispositivo móvil 100, el mensaje 22, o posiblemente una versión traducida o reformateada del mismo, es enviado a la puerta inalámbrica 16. La infraestructura inalámbrica 18 incluye una serie de conexiones a la red inalámbrica 20. Estas conexiones podrían ser Red Digital de Servicios Integrados (ISDN), Transmisión de Tramas o conexiones T1 que usan el protocolo TCP/IP usado a través de Internet. Tal como se usa en esta memoria, el término "red inalámbrica" está previsto que incluya tres tipos diferentes de redes, siendo esas (1) redes inalámbricas centradas en datos, (2) redes inalámbricas centradas en voz y (3) redes de modo dual que pueden soportar ambas comunicaciones de datos y voz a través de las mismas estaciones de base físicas. Las redes de modo dual combinadas incluyen, pero no se limitan a ellos, (1) redes de Acceso Múltiple por División de Código (CDMA), (2) el Grupo Especial Móvil o el Sistema Global para Comunicaciones Móviles (GSM) y las redes de Servicios Generales de Paquetes por Radio (GPRS), y (3) redes de tercera generación futura (3G) como Tasas de Datos Mejoradas para la Evolución Global (EDGE) y Sistemas Universales de Telecomunicaciones Móviles (UMTS). Algunos ejemplos anteriores de redes centradas en datos incluyen la Red de Radio Mobitex™ y la Red de Radio DataTAC™. Ejemplos de redes anteriores centradas en datos incluyen redes de Sistemas de Comunicaciones Personales (PCS) como GSM, y sistemas TDMA.

Como se representa en la figura 2, el dispositivo de comunicaciones móviles 100 incluye una antena de RF adecuada 102 para comunicación inalámbrica a y desde la red inalámbrica 20. Están previstos circuitos convencionales de RF, desmodulación/modulación y descodificación/codificación 104. Como los versados en la materia apreciarán, tales circuitos pueden entrañar posiblemente muchos procesadores de señales digitales (DSPs), microprocesadores, filtros, circuitos analógicos y digitales y similares. Sin embargo, como dichos circuitos son bien conocidos en la técnica, no se describirán con más detalle.

El dispositivo de comunicaciones móviles 100 también incluirá típicamente una CPU de control principal 106 que funciona bajo el control de un programa almacenado en una memoria de programas 108 (y que tiene acceso a una memoria de datos 110). La CPU 106 comunica también con un teclado convencional 112, una pantalla 114 (por ejemplo, una LCD) y un transductor de audio o altavoz 116. Una parte de la memoria de datos 110a se encuentra disponible para almacenar datos de Política IT usados para controlar operaciones de dispositivos asociados. Un código ejecutable de programa informático adecuado está almacenado en partes de la memoria de programas 108a para constituir la lógica de programa para hacer cumplir la Política IT, en cuanto a la codificación de acuerdo con la capacidad de estado de clasificación de mensajes se describe a continuación.

En la figura 3 se representa una lógica de cumplimiento de codificación ilustrativa. En este caso, la rutina "Nivel de Codificación Establecido" 300 puede ser introducida de cualquier manera deseada. Por ejemplo, puede introducirse a mano cuando un usuario establezca manualmente un nivel de clasificación o parámetro de intensidad de cifrado. Alternativamente, esta lógica puede ser introducida forzadamente como parte de una secuencia de transmisión de mensajes y antes de la misma de manera que es recorrida necesariamente para cada mensaje generado y/o transmitido desde el dispositivo 100. La propia lógica así como también una Política IT asociada (por ejemplo, véase la figura 4) pueden ser descargadas de una estación de base de empresas (otra vez posiblemente "impulsada" forzadamente en cada dispositivo de usuario de empresa 100).

Se realizan pruebas adecuadas en puntos de decisión 302, 204, 306, 308, 310, 312, 314 y 316 para detectar automáticamente qué estado de estados plurales de clasificación posible ha sido asociado con el mensaje disponible a mano. Como se apreciará, un código que represente un estado de clasificación particular (es decir, nivel de clasificación o intensidad de cifrado) puede ser conseguido como un campo adjunto al cuerpo o cabecera de un mensaje dado. Alternativamente, puede mantenerse una tabla separada o base de datos de estados de clasificación en asociación con otros datos peculiares de clasificación de mensajes (por ejemplo, números de mensajes de serie secuencial o similar). Como se apreciará, el número de puntos de decisión dependerá del número de estados de clasificación diferentes que se permiten de acuerdo con una Política IT dada.

De acuerdo con la Política IT indicada en la figura 4, si el mensaje es asociado con un nivel de clasificación no clasificado o sin ninguna intensidad de cifrado, entonces la rutina será hecha salir en 318 sin ningún requerimiento de codificación de cifrado especial. Sin embargo, de acuerdo con la Política IT de la figura 4, si un nivel de clasificación de "confidencial" es detectado en 304, entonces el mensaje simplemente es firmado en 320 antes de que la salida de la subrutina sea tomada en 318. Si se detecta el estado de clasificación de intensidad de cifrado "clasificado" o "regular", entonces el mensaje es firmado y cifrado con una clave de cifrado de 1024 bits antes de que la subrutina sea hecha salir en 318. De manera similar, si se detecta un nivel de clasificación de "secreto" o una intensidad de cifrado de "fuerte", entonces el mensaje es firmado y cifrado usando una clave más larga (por ejemplo, de 2048 bits) en 324. Por último, si

se detecta un nivel de clasificación de “muy secreto” o una intensidad de cifrado de “extra fuerte”, entonces el mensaje es firmado y cifrado con una clave de cifrado todavía más segura y más larga de 4096 bits en 326.

Si solamente se desea asegurar al menos un nivel de codificación mínimo (es decir, permitir niveles de codificación más altos que los mínimos si por lo demás son establecidos por el usuario o el sistema), entonces una rutina de nivel de codificación ilustrativa “Comprobar y Establecer” 500 está representada en la figura 5 (por ejemplo, que puede usarse como alternativa a la rutina de la figura 3). En este caso, tras la entrada en 500, se realiza una prueba en 502 para un estado de clasificación particular (por ejemplo, tal vez un nivel de clasificación o un nivel de intensidad de codificación). Si ese estado particular es detectado en 502, entonces se realiza otra prueba en 504 para ver si el nivel de codificación ya asociado con el mensaje disponible a mano está al menos al nivel mínimo de codificación correspondiente. Si es así, entonces el mensaje puede ser codificado en 506 usando cualquier nivel de codificación que ya haya sido asignado a ese mensaje. Sin embargo, si el nivel mínimo de codificación (por ejemplo, de acuerdo con la Política IT impuesta) no ha sido todavía satisfecho, entonces el nivel mínimo de codificación es usado para codificar el mensaje en 308 antes de que se tome la salida en 510. Como los versados en la materia apreciarán, pueden utilizarse tantos subgrupos similares de códigos como se desee para cada estado posible de clasificación.

Como los versados en la materia apreciarán, puede haber muchas variaciones y modificaciones de las realizaciones ilustrativas descritas en lo que antecede que todavía retengan algunas o todas las nuevas características y ventajas de estas realizaciones. Por consiguiente, se prevé que todas esas modificaciones y variaciones están incluidas dentro del alcance de las reivindicaciones adjuntas.

REIVINDICACIONES

1. Un método para aplicar automáticamente codificación de mensajes clasificados, comprendiendo dicho método:

para un mensaje a transmitir, asociar un estado de estados de clasificación plurales posibles con el mensaje, en que dicho estado de clasificación asociado con dicho mensaje es establecido manualmente;

antes de transmitir el mensaje, detectar el estado de clasificación asociado con el mensaje; y

codificar automáticamente el mensaje para transmisión usando un nivel de codificación de cifrado que corresponde al estado de clasificación detectado.

2. El método según la reivindicación 1, en el que la correspondencia entre estados de clasificación y niveles de codificación es establecida y hecha cumplir automáticamente en un usuario por una Política IT, residente en un dispositivo usado para generar y/o transmitir el mensaje.

3. El método según la reivindicación 1, en el que los estados de clasificación comprenden descriptores de intensidad de cifrado.

4. El método según la reivindicación 1, en el que los niveles de clasificación comprenden descriptores de nivel de seguridad.

5. El método según la reivindicación 1, en el que el nivel de codificación utilizado es al menos un nivel mínimo de codificación de cifrado para el estado de clasificación detectado o de un nivel más alto si es designado de otro modo.

6. Aparato para aplicar automáticamente codificación de mensajes clasificados, comprendiendo dicho aparato:

para un mensaje a transmitir, medios (10) para asociar un estado de estados de clasificación plurales posibles con el mensaje, siendo establecido manualmente dicho estado de clasificación asociado con dicho mensaje;

medios (10) para detectar, antes de transmitir el mensaje, el estado de clasificación asociado con el mensaje; y medios (10) para codificar automáticamente el mensaje para transmisión usando un nivel de codificación de cifrado que corresponde al estado de clasificación detectado.

7. Aparato según la reivindicación 6, en el que la correspondencia entre estados de clasificación y niveles de codificación es establecida y hecha cumplir automáticamente en un usuario por una Política IT, residente en un dispositivo usado para generar y/o transmitir el mensaje.

8. Aparato según la reivindicación 6, en el que los estados de clasificación comprenden descriptores de intensidad de cifrado.

9. Aparato según la reivindicación 6, en el que los niveles de clasificación comprenden descriptores de nivel de seguridad.

10. Aparato según la reivindicación 6, en el que el nivel de codificación utilizado es al menos un nivel mínimo de codificación de cifrado para el estado de clasificación detectado o de un nivel más alto si es designado de otro modo.

11. Un medio de memoria digital que tiene almacenado en él un programa informático que, cuando es ejecutado, produce automáticamente codificación de mensajes clasificados:

para un mensaje a transmitir, asociando un estado de estados de clasificación plurales posibles con el mensaje, en que dicho estado de clasificación con dicho mensaje es ajustado manualmente;

antes de transmitir un mensaje, detectando el estado de clasificación asociado con el mensaje; y

codificando automáticamente el mensaje para transmisión usando un nivel de codificación de cifrado que corresponde al estado de clasificación detectado.

12. El medio de memoria digital según la reivindicación 11, en el que la correspondencia entre estados de clasificación y niveles de codificación es establecida y hecha cumplir automáticamente en un usuario por una Política IT, residente en un dispositivo usado para generar y/o transmitir el mensaje.

13. El medio de memoria digital según la reivindicación 11, en el que los estados de clasificación comprenden descriptores de intensidad de cifrado.

14. El medio de memoria digital según la reivindicación 11, en el que los niveles de clasificación comprenden descriptores de nivel de seguridad.

15. El medio de memoria digital según la reivindicación 11, en el que el nivel de codificación utilizado es al menos un nivel mínimo de codificación de cifrado para el estado de clasificación detectado o de un nivel más alto si es designado de otro modo.

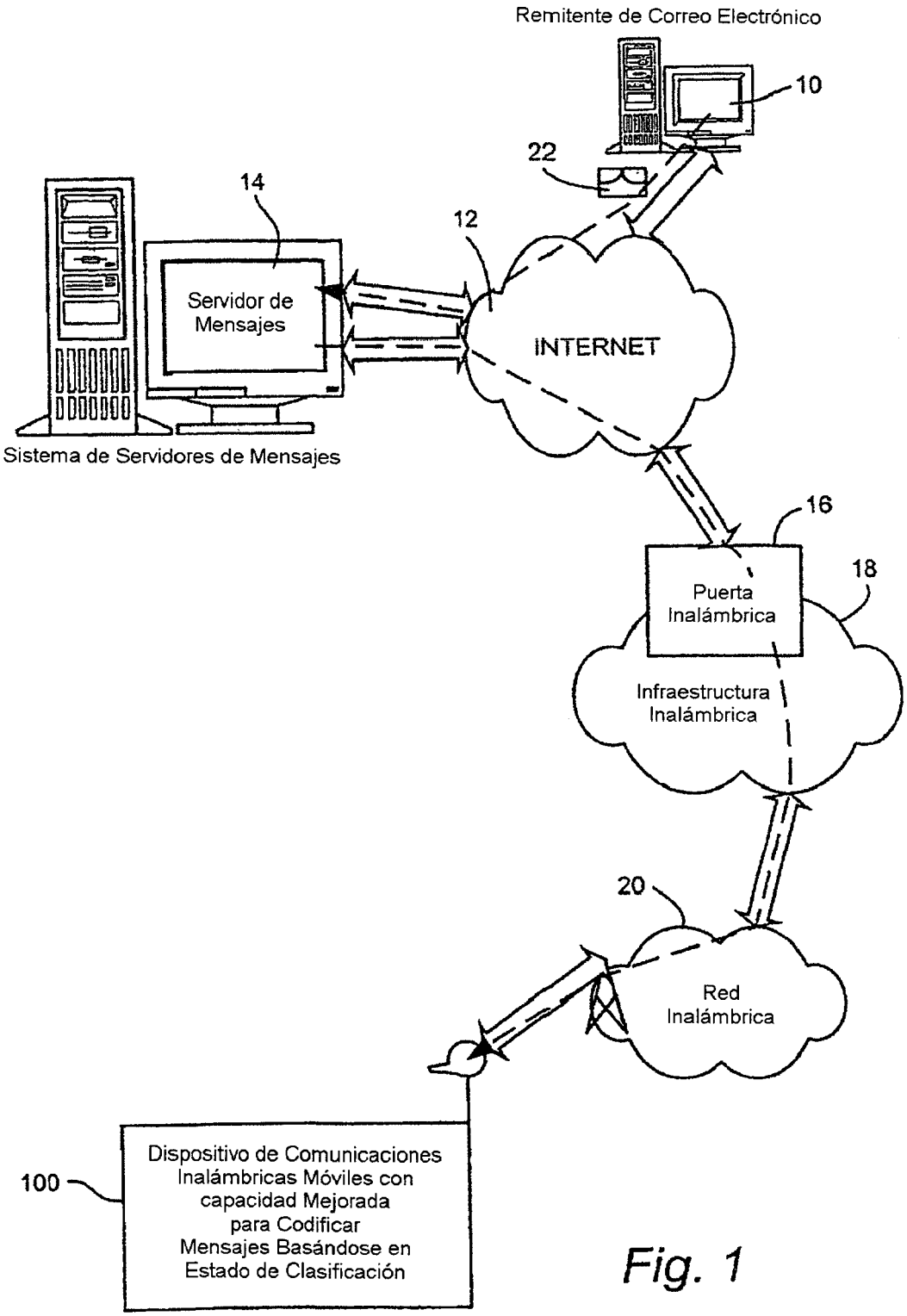
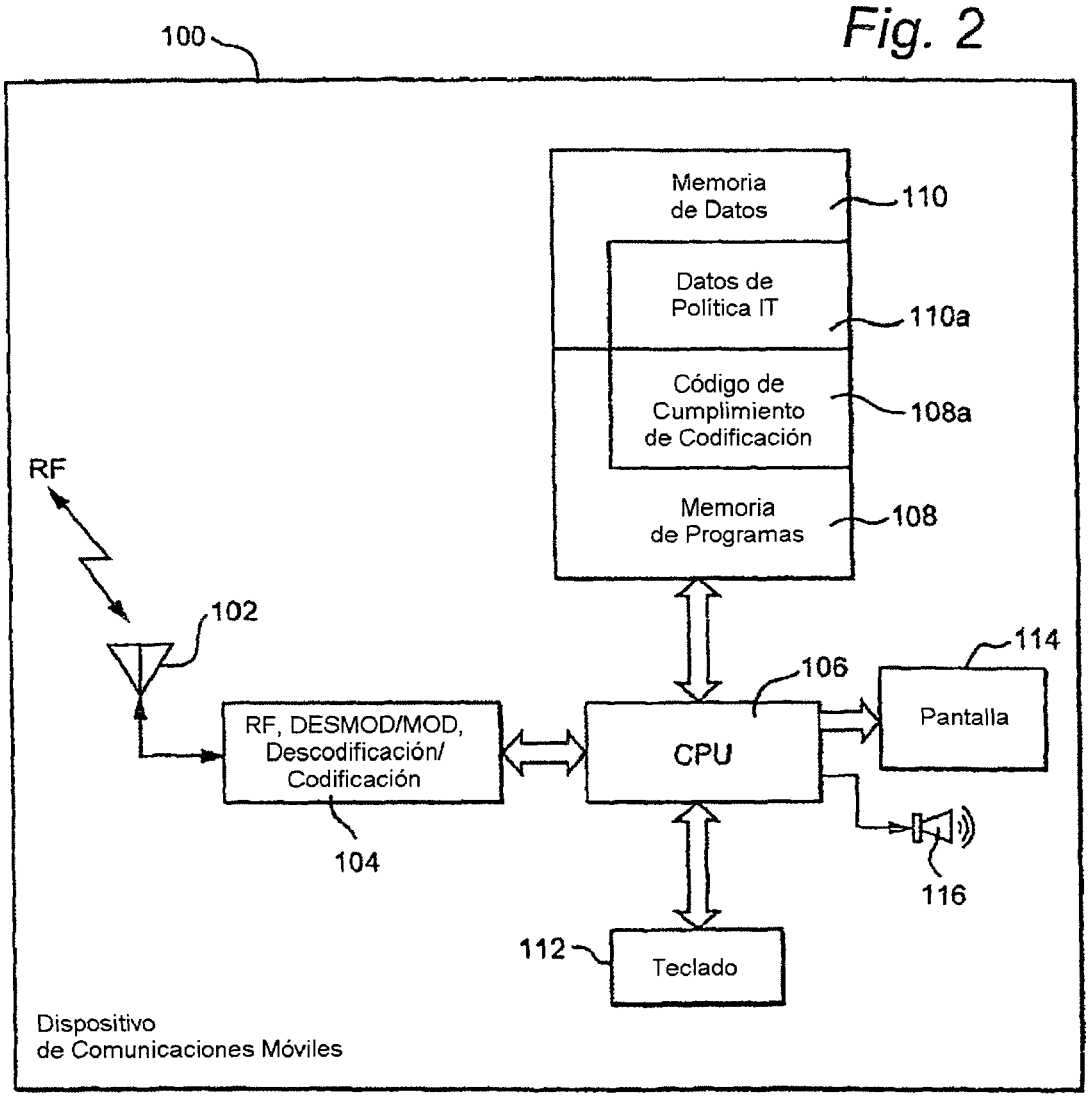

Remitente de Correo Electrónico
10
22
14
12
Servidor de Mensajes
INTERNET
Sistema de Servidores de Mensajes
16
18
Puerta Inalámbrica
Infraestructura Inalámbrica
20
Red Inalámbrica
100
Dispositivo de Comunicaciones Inalámbricas Móviles con capacidad Mejorada para Codificar Mensajes Basándose en Estado de Clasificación

Fig. 1

Fig. 2


100
Memoria de Datos
110
Datos de Política IT
110a
Código de Cumplimiento de Codificación
108a
Memoria de Programas
108
RF
102
RF, DESMOD/MOD, Descodificación/ Codificación
104
CPU
106
Pantalla
114
116
112
Teclado
Dispositivo de Comunicaciones Móviles

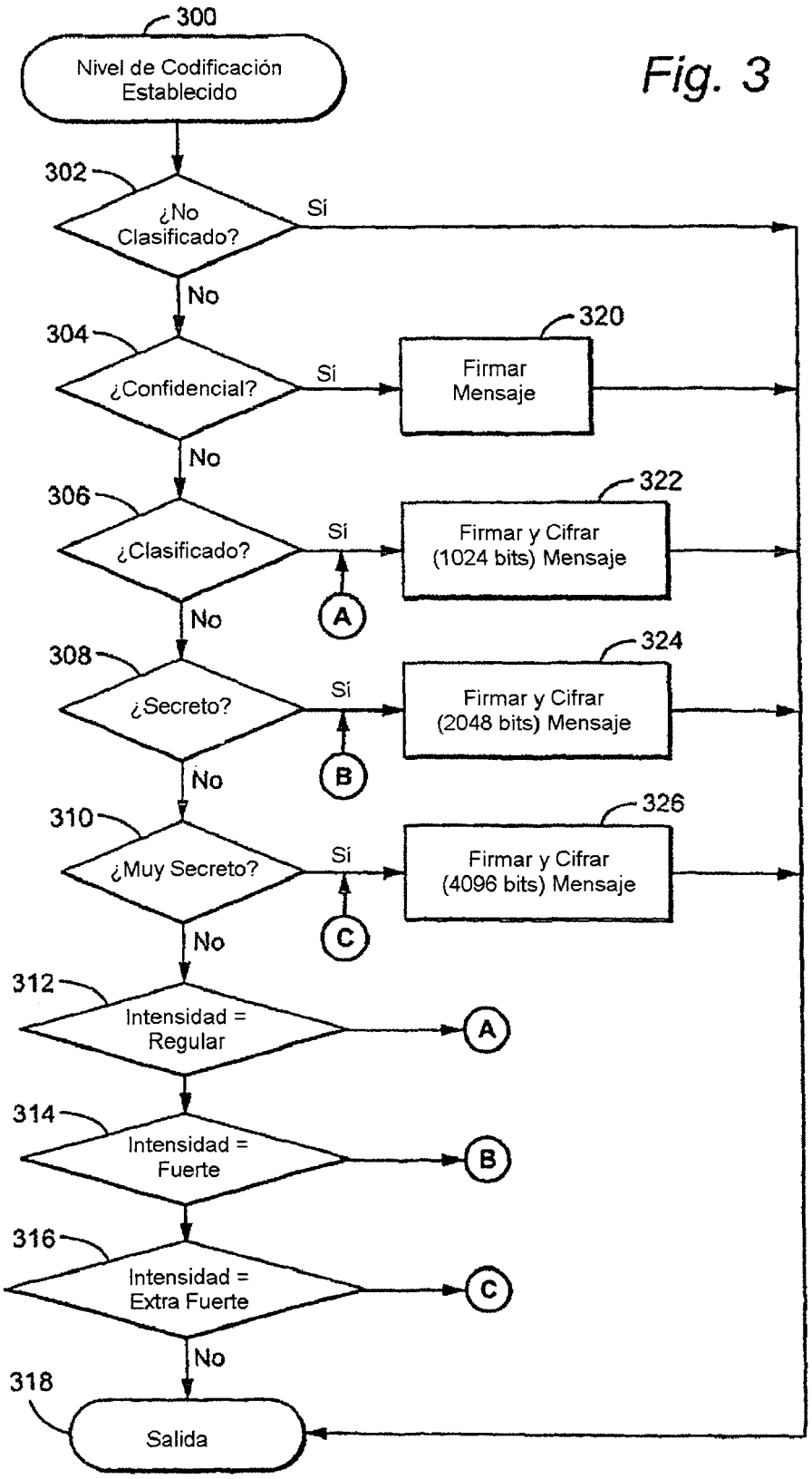

300
Nivel de Codificación Establecido
302
¿No Clasificado?
Sí
No
304
¿Confidencial?
Sí
320
Firmar Mensaje
No
306
¿Clasificado?
Sí
322
Firmar y Cifrar (1024 bits) Mensaje
A
No
308
¿Secreto?
Sí
324
Firmar y Cifrar (2048 bits) Mensaje
B
No
310
¿Muy Secreto?
Sí
326
Firmar y Cifrar (4096 bits) Mensaje
C
No
312
Intensidad = Regular
A
314
Intensidad = Fuerte
B
316
Intensidad = Extra Fuerte
C
No
318
Salida

Fig. 3

Fig. 4

Nivel de Clasificación	Intensidad de Cifrado	Codificación Requerida
No Clasificado	Ninguna	Ninguna
Confidencial	Ninguna	Sólo firmado
Clasificado	Regular (1024 bits)	Firmado y Cifrado
Secreto	Fuerte (2048 bits)	Firmado y Cifrado
Muy Secreto	Extra Fuerte (4096 bits)	Firmado y Cifrado

Fig. 5

