(19) OFICINA ESPAÑOLA DE PATENTES Y MARCAS

ESPAÑA

(11) Número de publicación: **2 546 817**

(51) Int. CI.:

H04L 9/32 (2006.01)

(12) TRADUCCIÓN DE PATENTE EUROPEA T3

(96) Fecha de presentación y número de la solicitud europea: **23.04.2008 E 08736508 (6)**

(97) Fecha y número de publicación de la concesión europea: **10.06.2015 EP 2147519**

(54) Título: **Procedimiento y dispositivo para transmitir, con total seguridad, informaciones emitidas por diferentes expedidores**

(30) Prioridad:

07.05.2007 DE 102007021808

(45) Fecha de publicación y mención en BOPI de la traducción de la patente:
28.09.2015

(73) Titular/es:

NOVOSEC AG (100.0%)
BERLINER STRASSE 44
60311 FRANKFURT AM MAIN, DE

(72) Inventor/es:

STOHN, MAIK;
RITTER, HARALD y
WEISS, JÜRGEN

(74) Agente/Representante:

MORGADES MANONELLES, Juan Antonio

DESCRIPCIÓN

Procedimiento y dispositivo para transmitir, con total seguridad, informaciones emitidas por diferentes expedidores

La presente invención se refiere a un procedimiento para la transmisión segura de informaciones (mensajes) de diferentes dispositivos expedidores mediante la acción de uno o varios mediadores a un dispositivo del receptor del mensaje (en lo sucesivo denominado también como "dispositivo") con una unidad de salida conectada al dispositivo o que forma parte del mismo (visualizador, altavoces, impresora, etc.) y una unidad de entrada conectada al dispositivo o que forma parte del mismo (teclado, pantalla táctil etc.) así como la transmisión de retorno segura de un mensaje de respuesta.

CAMPO DE LA INVENCIÓN

Una transmisión de mensajes se define como segura cuando se garantiza la confidencialidad del mensaje (es decir, una persona no autorizada no puede leer el mensaje), la autenticidad de los interlocutores de la comunicación (es decir, los interlocutores de la comunicación son realmente los que se han especificado como tales) y la integridad del mensaje (es decir, el mensaje no se ha modificado).

Los procedimientos conocidos para la transmisión confidencial de mensajes de diferentes expedidores a diferentes receptores se realizan habitualmente con la ayuda de los denominados procedimientos de cifrado simétricos o con la ayuda de los denominados procedimientos Public-Key.
En los procedimientos de cifrado simétricos, cada expedidor intercambia un código individual con cada receptor al que pretende enviar mensajes. Mediante dicho código los mensajes se pueden codificar mediante un procedimiento matemático y también volverse a descodificar.
En los procedimientos Public-Key se asigna a cada receptor de un mensaje un par de claves, una secreta que únicamente la conoce el receptor, y una pública que conoce el expedidor correspondiente. Mediante la clave pública, empleando un procedimiento matemático, se cifra el mensaje de tal forma que exclusivamente el poseedor de la clave secreta pueda volver a descifrar el mensaje empleando un procedimiento matemático. Los puntos por los que se envía el mensaje cifrado no lo pueden descifrar y, por lo tanto, tampoco lo pueden modificar.

Los procedimientos conocidos para la protección de la integridad de los mensajes emplean las denominadas firmas digitales, que frecuentemente se denominan asimismo como firmas electrónicas. Dichas firmas digitales se realizan asimismo habitualmente con la ayuda del procedimiento Public-Key. En el mismo se asigna al firmante un par de claves que comprende una clave secreta y una pública. Con la ayuda de la clave secreta, en un procedimiento matemático se crea una firma que se puede verificar con la ayuda de la clave pública. La clave secreta está controlada exclusivamente por el firmante, mientras que la clave pública puede darse a conocer a cualquiera.

Los procedimientos según el estado de la técnica para la autentificación de interlocutores de la comunicación se realizan asimismo frecuentemente con la ayuda del denominado procedimiento Public-Key. Para la autentificación del expedidor, o el mismo firma digitalmente el mensaje o el expedidor responde correctamente a una pregunta del receptor (Procedimiento Challenge-Response). En los procedimientos conocidos, la autenticidad del receptor se garantiza habitualmente mediante el procedimiento Challenge-Response o mediante el cifrado del mensaje con la clave pública del receptor.

La patente US nº 6 137 884 representa un cifrado de informaciones en un intercambio de datos entre dos personas que intercambian los datos mediante la acción de una oficina postal digital.

Para la distribución de la clave pública se emplean o los denominados certificados digitales, o cada receptor debe transmitir por anticipado a cada expedidor su clave pública. Esto debe hacerse por vías seguras para garantizar la integridad de la clave.

La entrega y la administración de los certificados digitales origina unos costes altos y su verificación requiere unos gastos adicionales para cálculo y comunicación. El intercambio de claves antes de la comunicación propiamente dicha es, particularmente cuando hay una pluralidad de potenciales expedidores o en receptores con una capacidad reducida de la memoria de almacenamiento, de difícil manejo y, por lo tanto, únicamente es posible en un círculo de usuarios muy pequeño. Ello es válido tanto en lo que respecta al número de expedidores potenciales como asimismo al número de receptores potenciales.

Para garantizar la autenticidad del expedidor, en los procedimientos conocidos es necesario el intercambio de más claves o la administración de certificados adicionales.

En los procedimientos conocidos, para evitar mensajes no pretendidos se comprueban los datos del expedidor en el lado del servidor o los contenidos de los mensajes se filtran por las palabras clave. Sin embargo, de este modo no se garantiza ni la confidencialidad del mensaje ni la protección de datos.

Sumario de la invención:

El objetivo de la presente invención es subsanar los puntos débiles de los procedimientos conocidos hasta ahora, enviando todos los mensajes al receptor correspondiente mediante la acción de uno o varios mediadores.
Dicho objetivo se alcanza mediante un dispositivo y un procedimiento con las características de las reivindicaciones independientes.

El mediador puede comprobar la autenticidad del expedidor, aunque no puede leer el mensaje cifrado por el expedidor para receptor respectivo. El receptor únicamente debe comprobar la autenticidad del mediador y precisa para ello únicamente una clave adicional. De este modo, el receptor precisa, independientemente del número de interlocutores de comunicación, únicamente un número fijo de claves. En la presente invención se puede prescindir asimismo de los certificados sin ninguna restricción en la seguridad. La presente invención emplea para el cifrado, la autentificación, la producción de firmas electrónicas y los cronomarcadores, los procedimientos criptográficos conocidos en el ámbito especializado.

En el contexto de la presente invención se entiende por un mensaje cualquier tipo de información que pueda reproducirse en forma electrónica, por ejemplo números, letras, combinaciones de números, combinaciones de letras, gráficos, tablas, etc.

En el contexto de la presente invención se entiende por una función de autentificación A y por la función de comprobación Ü asociada cualquier tipo de procedimiento con el que se pueda demostrar la autenticidad de un mensaje o de un interlocutor de comunicación - mediante la función de autentificación A - o comprobar la exactitud de la autentificación - mediante la función de comprobación Ü-.

En el contexto de la presente invención se entiende por una función de cifrado V y la función de descifrado E asociada cualquier tipo de procedimiento con el que - mediante la acción de la función de cifrado V - se asegura que ninguna persona no autorizada pueda leer el mensaje, mientras que una persona autorizada - tras el descifrado mediante la función de descifrado E - lo pueda leer.

En el contexto de la presente invención se entiende por una función de confirmación B y la función de comprobación P asociada cualquier tipo de procedimiento con el que se puede confirmar una característica de un mensaje - mediante la función de confirmación B - y comprobar la autenticidad de dicha confirmación - mediante la función de comprobación P -.

En el contexto de la presente invención se entiende por una función de cronomarcador Z cualquier tipo de procedimiento con el que se confirma el momento en el que llegó un mensaje. En el contexto de la presente invención se entiende por una función de verificación del cronomarcador asociada cualquier tipo de procedimiento con el que se puede comprobar el cronomarcador creado con la función Z.

A continuación se describirá con mayor detalle el procedimiento básico para la transmisión segura de mensajes, haciéndose referencia a la figura 1 de la descripción del proceso 1.

Para enviar de forma segura un mensaje N a un dispositivo D, el expedidor A cifra el mensaje empleando la función de cifrado V_D, se autentifica frente al mediador empleando la función de autentificación A_A y envía el mensaje cifrado al mediador. El mediador puede autentificar el mensaje con la ayuda de la función de autentificación A_M y reenviarlo al dispositivo D designado por el expedidor, aunque él mismo no puede descifrar el mensaje. La autentificación del mensaje y su reenvío al dispositivo por parte del mediador tiene lugar únicamente ha sido completada con éxito la comprobación de la autentificación mediante la función de comprobación $Ü_A$. El dispositivo D comprueba a autentificación del mediador con la ayuda de la función de comprobación $Ü_M$, realiza el descifrado si se ha completado con éxito la comprobación del mensaje y lo entrega mediante la acción de los medios de salida conectados (visualizador, impresora, altavoz, etc.). El dispositivo D provoca (dado el caso tras la autorización por parte del usuario) una respuesta, que se legitima con la ayuda de una función de confirmación B_D y se envía de vuelta al expedidor directamente o mediante la acción del mediador. El expedidor A puede comprobar el origen y la integridad de la respuesta con la ayuda de la función de comprobación P_D (véase la descripción de proceso 1 y el diagrama de flujo en la figura 1).

En otra manifestación ventajosa adicional del procedimiento, que se representa en el diagrama de flujo 2 y en la figura 2 asociada, el dispositivo D puede legitimar una respuesta, dado el caso tras la autorización por parte del usuario, con la ayuda de una función de confirmación B_D y enviarla de vuelta al mediador. Éste puede confirmar la entrada de una respuesta del dispositivo D con la ayuda de una función de confirmación B_M y reenviar la respuesta recibida del dispositivo D junto con la confirmación, al expedidor A del mensaje N original. El expedidor A puede comprobar la exactitud de las confirmaciones con la ayuda de las funciones de comprobación P_M y P_D (véase la descripción del proceso 2).

Otra manifestación ventajosa del procedimiento se representa en el diagrama de flujo 3 con la figura 3. En la misma, el dispositivo D, dado el caso tras la autorización por parte del usuario, puede legitimar una respuesta con la ayuda

de una función de confirmación B_D y enviarla de vuelta al mediador. Éste puede comprobar el origen y la integridad de la respuesta con la ayuda de la función de comprobación P_D, y con la ayuda de una función de confirmación B_M confirmar la comprobación realizada y reenviarla al expedidor A del mensaje N original. El expedidor A puede comprobar la exactitud de la confirmación con la ayuda de una función de comprobación P_M. En dicha manifestación, el expedidor A únicamente puede comprobar la confirmación mediante la acción del mediador y con ello ya puede estar seguro de que la respuesta procede del dispositivo D. El expedidor A no precisa ninguna clave adicional del dispositivo D para la comprobación de la confirmación por el dispositivo D.

La descripción del proceso 4 con la figura 4 representa otra manifestación ventajosa del procedimiento análoga a la descripción del proceso1 con la diferencia de que el dispositivo D cifra la respuesta con la ayuda de una función de cifrado V_M, de tal forma que únicamente el mediador pueda volver a descifrar la respuesta con la ayuda de la función de descifrado E_M asociada.

La descripción del proceso 5 con la figura 5 representa otra manifestación ventajosa del procedimiento análoga a la descripción del proceso 2 con la diferencia de que el dispositivo D cifra la respuesta con la ayuda de una función de cifrado V_M, de tal forma que únicamente el mediador pueda volver a descifrar la respuesta con la ayuda de la función de descifrado E_M asociada.

La descripción del proceso 6 con la figura 6 representa otra manifestación ventajosa del procedimiento análoga a la descripción del proceso 3 con la diferencia de que el dispositivo D cifra la respuesta con la ayuda de una función de cifrado V_M, de tal forma que únicamente el mediador pueda volver a descifrar la respuesta con la ayuda de la función de descifrado E_M asociada.

En otra manifestación ventajosa del procedimiento, según la descripción de proceso 7, los mensajes cifrados enviados al dispositivo se dotan de un ID del mensaje dependiente del expedidor A y del dispositivo D, que impide que un mensaje N sea aceptado más de una vez por el dispositivo D. Esta es una contramedida contra los denominados ataques de regrabación.

En otra manifestación ventajosa del procedimiento, según la descripción de proceso 8, los mensajes cifrados enviados al dispositivo se dotan de un ID del mensaje dependiente únicamente del dispositivo D, que impide que un mensaje N sea aceptado más de una vez por el dispositivo D. En esta manifestación, el ID del mensaje lo debe administrar el mediador.

En otra manifestación ventajosa del procedimiento, según la descripción de proceso 9 pueden elegirse las claves del mediador individualmente por dispositivo D o por expedidor A. Ello tiene como consecuencia que se dificultan los diferentes ataques que se amparan en el empleo demasiado frecuente de claves criptográficas. Asimismo, se vuelve a mejorar la confidencialidad.

En otra manifestación ventajosa del procedimiento, según la descripción de proceso 10, el mediador puede proporcionar adicionalmente un servicio de cronomarcador, con lo que se puede documentar de forma demostrable el momento en el que se ha realizado la transmisión del mensaje. Asimismo, de este modo se descarta la existencia de dos mensajes completamente idénticos.

En otra manifestación ventajosa del procedimiento se puede recurrir a un servicio de cronomarcador externo para marcar el mensaje con la hora actual.

En otra manifestación ventajosa del procedimiento se pueden variar los algoritmos criptográficos empleados por el mediador individualmente por expedidor A o individualmente por dispositivo D.

En otra manifestación ventajosa del procedimiento se pueden variar los algoritmos criptográficos a emplear por el expedidor A individualmente por dispositivo D.

En otra manifestación ventajosa del procedimiento, el mediador no obtiene de la respuesta ninguna información sobre la información contenida en la respuesta. Ello puede alcanzarse por ejemplo cifrando el expedidor A junto con el mensaje las posibles respuestas y valores (aleatorios) asociados; el dispositivo D envía a continuación, en lugar de la respuesta el valor (aleatorio) asociado.

En otra manifestación ventajosa del procedimiento, el mediador puede interpretar la respuesta del dispositivo D, sin sacar conclusiones sobre el mensaje N propiamente dicho enviado por el expedidor A. Este proceso es análogo a una de las descripciones de proceso 1 a 10 con la diferencia de que el mediador puede interpretar la respuesta y con ello puede crear p. ej. evaluaciones estadísticas por expedidor o valoraciones de dispositivos.

En otra manifestación ventajosa del procedimiento se pueden intercambiar, si es preciso, los algoritmos criptográficos y/o las claves criptográficas empleadas, utilizando la transmisión de mensajes segura según la presente invención.

En otra manifestación ventajosa del procedimiento, el expedidor A del mensaje N no debe autentificarse frente al mediador. El mediador traslada al dispositivo D el mensaje cifrado por el expedidor A únicamente si el usuario del dispositivo ha autorizado explícitamente mensajes no autentificados.

En otra manifestación ventajosa del procedimiento, la respuesta no se envía al expedidor del mensaje original, sino a un tercero.

En otra manifestación ventajosa del procedimiento no se envía ninguna respuesta.

En otra manifestación ventajosa del procedimiento, el mediador puede adoptar al mismo tiempo el papel del expedidor.

En otra manifestación ventajosa del procedimiento, las claves del dispositivo D que se precisan en el expedidor se guardan en el mediador y el expedidor las pide en el mismo.

Se prefiere que el dispositivo D sea un aparato portátil pequeño que trabaje de forma alámbrica, inalámbrica mediante red inalámbrica o mediante una conexión óptica y que presente únicamente una funcionalidad muy limitada. Esta comprende la respuesta afirmativa, la respuesta negativa y la visualización de informaciones en un visualizador. En el visualizador se pueden representar p. ej. los detalles de la transacción tales como la suma, el número de cuenta y el receptor, de tal forma que el usuario pueda asimismo confirmar la transacción realmente sin que haya riesgo de que se produzca un ataque de Man-in-the-Middle (hombre interpuesto).

El sistema operativo se endurece y no autoriza la ejecución de códigos externos. Las actualizaciones del Software no son posibles o lo son únicamente con unos requisitos de seguridad muy altos.

Una aplicación preferida es su empleo para la autorización segura de transacciones.

DESCRIPCIÓN DE LAS FIGURAS

A continuación se realizará una descripción resumida de las figuras que sirve para comprender mejor la presente invención.

La fig. 1 representa una 1ª descripción de proceso;
La fig. 2 representa una 2ª descripción de proceso;
La fig. 3 representa una 3ª descripción de proceso;
La fig. 4 representa una 4ª descripción de proceso;
La fig. 5 representa una 5ª descripción de proceso;
La fig. 6 representa una 6ª descripción de proceso;
La fig. 7 representa una administración de claves en las entidades individuales;
La fig. 8 representa los algoritmos implementados en las entidades individuales;

EJEMPLOS DE FORMAS DE REALIZACIÓN:

A continuación se entra en detalle en los ejemplos de formas de realización que ya se han mencionado anteriormente.

Por principio, para cada expedidor en el sistema se asigna un ID de expedidor (AID) inequívoco, que lo conoce el mediador. A cada dispositivo se le asigna un ID de dispositivo (DID) inequívoco, que lo conoce el mediador

NOMENCLATURAS

K_{XY} es la clave para la función X (=V,E,A,P,B,Ü,Z,T) y se asigna a la entidad Y (=A,M,D) (es decir, en caso de pares de claves asimétricos, la clave secreta está exclusivamente en posesión de la entidad Y)
$K_{X,Y,U}$ es la clave para la función X (=V,E,A,P,B,Ü,Z,T) y está asignada a la entidad Y (=A,M,D), siendo la clave distinta individualmente para cada entidad U (=A,D), || significa la concatenación de secuencias de caracteres, <. . . .> significa una lista de valores, $X_Y(a,b,C;K_{X,Y})$ significa la función X asignada a la entidad Y; los valores de entrada (en el ejemplo a, b y c) están en el paréntesis antes del punto y coma, la clave empleada (en el ejemplo $K_{X,Y}$) después del punto y coma. ZPn: tantos parámetros adicionales como se quiera según la manifestación del procedimiento; n es el número correlativo y sirve para distinguir, ya que los parámetros adicionales pueden variar de una función a otra.

La descripción de proceso de la figura 1 representa el proceso básico.

1. El expedidor A calcula $C=V_D(N,ZP1;K_{V,D})$ y $E=A_A(C,ZP5;K_{A,,A})$. El expedidor A envía <DID,E,C,ZP2> a la central [ZP2 comprende los valores de ZP5 requeridos para la comprobación de la autentificación y, dado el caso, más información]

2. El mediador comprueba la autentificación del expedidor A mediante $Ü_A(E,C,ZP5,K_{U,A})$. El mediador calcula $B=A_M(C,ZP3;K_{A,M})$ y envía <B,C,ZP4> al dispositivo [ZP4 comprende los valores de ZP3 requeridos para la autentificación y, dado el caso, más información].
3. El dispositivo D comprueba la autentificación del mediador mediante $Ü_M(B,C,ZP4,K_{U,M})$.
4. El dispositivo D descifra el mensaje mediante $E_D(C,K_{E,D})$.
5. El dispositivo D entrega el mensaje N (y, dado el caso, más información) al expedidor A mediante los medios de salida conectados.
6. El dispositivo D calcula (dado el caso, tras la autorización por parte del usuario) $F=B_D(Respuesta,ZP6;K_{B,D})$ y envía <F,ZP7> al mediador.
7. El mediador traslada <F,ZP7> inmediatamente al expedidor A
8. El expedidor A comprueba la confirmación mediante $P_D(F,ZP7;K_{P,D})$ e interpreta la respuesta.

Las claves que se precisan para ello son para

Dispositivo:
- Clave propia: $K_{E,D}$, $K_{B,D}$
- Clave del mediador: $K_{U,M}$
- Conocida por el expedidor: $K_{V,D}$, $K_{B,D}$

Expedidor:
- Clave propia: $K_{A,A}$ (puede ser también userID/password)
- Clave del dispositivo: $K_{V,D}$, $K_{P,D}$

Mediador:
- Clave propia: $K_{A,M}$
- Clave del expedidor: $K_{U,M}$ (puede ser también userID/password)
- Conocida por el dispositivo: $K_{U,M}$

La descripción de proceso 2, tal como se puede observarse en la figura 2, comprende el proceso básico con confirmación adicional por parte del mediador

1. El expedidor A calcula $C=V_D(N,ZP1;K_{V,D})$ y $E=A_A(C,ZP5;K_{A,A})$. El expedidor A envía <DID,E,C,ZP2> a la central [ZP2 comprende los valores de ZP5 requeridos para la comprobación de autentificación y, dado el caso, más información].
2. El mediador comprueba la autentificación del expedidor A mediante $Ü_A(E.C.ZP5;K_{Ü,A})$. El mediador calcula $B=A_M(C,ZP3;K_{A,M})$ y envía <B,C,ZP4> al dispositivo [ZP4 comprende los valores de ZP3 requeridos para la comprobación de la autentificación y, dado el caso, más información]
3. El dispositivo D comprueba la autentificación del mediador mediante $Ü_M(B.C.ZP4;K_{Ü,M})$
4. El dispositivo D descifra el mensaje mediante $E_D(C,K_{E,D})$
5. El dispositivo D entrega el mensaje N (y, dado el caso, información al expedidor A) mediante los medios de salida conectados
6. El dispositivo D calcula (dado el caso, tras autorización por parte del usuario) $F=B_D)(Respuesta,ZP6;K_{B,D})$ y envía <F,ZP7> al mediador
7. El mediador comprueba la confirmación por el dispositivo D mediante $P_D(F,ZP7;K_{P,D})$; una vez realizada la comprobación con éxito, el mediador confirma el origen y la integridad de la respuesta del dispositivo D mediante $G=B_M$ (respuesta, ZP8;$K_{B,M}$) y envía <DID,G,ZP9> al expedidor A
8. El expedidor A comprueba la confirmación del mediador mediante $P_M(G,ZP9;K_{P,M})$; una vez realizada la comprobación con éxito, el expedidor A interpreta la respuesta.

Las claves que se precisan para ello son:

Dispositivo:
- Clave propia: $K_{E,D}$, $K_{D,D}$
- Clave del mediador: $K_{Ü,M}$
- Conocida por el expedidor: $K_{V,D,}$ $K_{P,D}$

Expedidor:
- Clave propia: $K_{A,A}$, (también puede ser userID/password)
- Clave del mediador: $K_{P,M}$
- Clave del dispositivo: $K_{V,D,}$ $K_{P,D}$

Mediador:
- Clave propia: $K_{A,M}$, $K_{B,M}$
- Clave del expedidor: $K_{Ü,A}$ (también puede ser userID/password)
- Conocida por el expedidor: $K_{P,M}$
- Conocida por el dispositivo $K_{Ü,M}$

La descripción de proceso 3, tal como puede observarse en la figura 3, comprende la comprobación de la confirmación por parte del mediador

1. El expedidor A calcula $C=V_D(N,ZP1;K_{V,D})$ y $E=A_A(C,ZP5;K_{A,,A})$. El expedidor A envía <DID,E,C,ZP2> a la central [ZP2 comprende los valores de ZP5 requeridos para la comprobación de la autentificación y, dado el caso, más información]
2. El mediador comprueba la autentificación del expedidor A mediante $Ü_A(E.C.ZP5;K_{Ü,A})$. El mediador calcula $B=A_M(C,ZP3;K_{A,M})$ y envía <B,C,ZP4> al dispositivo [ZP4 comprende los valores de ZP3 requeridos para la comprobación de la autentificación y, dado el caso, más información
3. El dispositivo D comprueba la autentificación del mediador mediante $Ü_M(B.C.ZP4;K_{Ü,M})$
4. El dispositivo D descifra el mensaje mediante $E_D(C,K_{E,D})$
5. El dispositivo D entrega el mensaje N (y, dado el caso, información al expedidor A) mediante los medios de salida conectados
6. El dispositivo D calcula (dado el caso, tras autorización por parte del usuario) $F=B_D)(Respuesta,ZP6;K_{B,D})$ y envía <F,ZP7> al mediador
7. El mediador comprueba la confirmación por el dispositivo D mediante $P_D(F,ZP7;K_{P,D})$; una vez realizada la comprobación con éxito, el mediador confirma el origen y la integridad de la respuesta del dispositivo D mediante $G=B_M$ (respuesta, ZP8;$K_{B,M}$) y envía <DID,G,ZP9> al expedidor A
8. El expedidor A comprueba la confirmación del mediador mediante $P_M(G,ZP9;K_{P,M})$; una vez realizada la comprobación con éxito, el expedidor A interpreta la respuesta

Las claves que se precisan para ello son:

Dispositivo:
- Clave propia: $K_{E,D}$, $K_{D,D}$
- Clave del mediador: $K_{Ü,M}$
- Conocida por el mediador: $K_{P,D}$
- Conocida por el expedidor: $K_{V,D}$

Expedidor:
- Clave propia: $K_{A,A}$, (también puede ser userID/password)
- Clave del mediador: $K_{P,M}$
- Clave del dispositivo: $K_{V,D}$

Mediador:
- Clave propia: $K_{A,M}$, $K_{B,M}$
- Clave del dispositivo: $K_{P,D}$
- Clave del expedidor: $K_{Ü,A}$ (también puede ser userID/password)
- Conocida por el expedidor: $K_{P,M}$
- Conocida por el dispositivo $K_{Ü,M}$

Descripción de proceso 4 Proceso análogo al proceso 1, aunque con un cifrado de la respuesta para el mediador.

1. El expedidor A calcula $C=V_D(N,ZP1;K_{V,D})$ y $E=A_A(C,ZP5;K^{A,A})$ El expedidor A envía <DID,E,C,ZP2> a la central [ZP2 comprende los valores de ZP5 requeridos para la comprobación de la autentificación y, dado el caso, más información].
2. El mediador comprueba la autentificación del expedidor A mediante $Ü_A(E,C.ZP5;K_{Ü,A})$. El mediador calcula $B=A_M(C.ZP3;K_{A,M})$ y envía <B,C,ZP4> al dispositivo. [ZP4 comprende los valores de ZP3 requeridos para la comprobación de la autentificación y, dado el caso, más información]
3. El dispositivo D comprueba la autentificación del mediador mediante $Ü_M(B.C.ZP4;K_{Ü,M})$
4. El dispositivo D descifra el mensaje mediante $E_D(C,K_{E,D})$.
5. El dispositivo D entrega el mensaje N (y dado el caso, información al expedidor A) mediante los medios de salida conectados
6. El dispositivo D calcula (dado el caso, tras la autorización por parte del usuario) $F=B_D(Respuesta, ZP6;K_{B,D})$ así como $H=V_M(F,ZP10;K_{V,M})$ y envía <H,ZP11> al mediador
7. El mediador calcula <F,ZP10>= $E_M(M;K_{E,M})$ y envía <F, ZP12> al expedidor A
8. El expedidor A comprueba la confirmación mediante $P_D(F,ZP12;K_{P\ D})$ e interpreta la respuesta

Las claves que se precisan para ello son:

Dispositivo:
- Clave propia: $K_{E,D,}$ $K_{B,D}$
- Clave del mediador: $K_{Ü,M}$, $K_{V,M}$
- Conocida por el expedidor: $K_{V,D}$, $K_{P,D}$

Expedidor
- Clave propia $K_{A,A}$ (también puede ser userID/password)
- Clave del dispositivo: $K_{V,D}$, $K_{P,D}$

Mediador
- Clave propia $K_{A,M}$, $K_{E,M}$
- Clave del expedidor: $K_{Ü,A}$ (también puede ser userID/password)
- Conocida por el dispositivo: $K_{Ü,M.}$ $K_{V,M}$

La descripción de proceso 5, según la figura 5, es análoga al proceso 2, aunque con un cifrado de la respuesta para el mediador.

1. El expedidor A calcula $C=V_D(N,ZP1;K_{V,D})$ y $E=A_A(C,ZP5;K_{A,A})$. El expedidor A envía <DID,E,C,ZP2> a la central [ZP2 comprende los valores de ZP5 requeridos para la comprobación de la autentificación y, dado el caso, más información]
2. El mediador comprueba la autentificación del expedidor A mediante $Ü_A(D,C,ZP5;K_{Ü,A})$. El mediador calcula $B=A_M(C,ZP3;K_{A,M})$ y envía <B,C,ZP4> al dispositivo [ZP4 comprende los valores de ZP3 requeridos para la comprobación de la autentificación y, dado el caso, más información]
3. El dispositivo D comprueba la autentificación del mediador mediante $Ü_M(B.C.ZP4;K_{Ü,M})$
4. El dispositivo D descifra el mensaje mediante $E_D(C,K_{E,D})$.
5. El dispositivo D entrega el mensaje N (y dado el caso, información al expedidor A) mediante los medios de salida conectados
6. El dispositivo D calcula (dado el caso, tras la autorización por parte del usuario) $F=B_D(\text{Respuesta, ZP6};K_{B,D})$ así como $H=V_M(F,ZP10;K_{V,M})$ y envía <H,ZP11> al mediador
7. El mediador calcula $<F,ZP10>= E_M(M;K_{E,M})$, confirma la entrada de la respuesta del dispositivo D mediante $G=B_M(F,ZP8;K_{B,M})$ y envía <DID,G,ZP9> al expedidor A
8. El expedidor A comprueba la confirmación del mediador mediante $P_M(G,ZP9;K_{P,M})$. Una vez realizada la comprobación con éxito, el expedidor A comprueba la confirmación por el dispositivo D mediante $P_D(F,ZP7;K_{P\ D})$ e interpreta la respuesta

Claves que se precisan:

Dispositivo:
- Clave propia: $K_{E,D,}$ $K_{B,D}$
- Clave del mediador: $K_{Ü,M}$, $K_{V,M}$
- Conocida por el expedidor: $K_{V,D}$, $K_{P,D}$

Expedidor
- Clave propia $K_{A,A}$ (también puede ser userID/password)
- Clave del mediador: $K_{P,M}$
- Clave del dispositivo: $K_{V,D}$, $K_{P,D}$

Mediador
- Clave propia $K_{A,M}$, $K_{B,M}$ $K_{E,M}$
- Clave del expedidor: $K_{Ü,A}$ (también puede ser userID/password)
- Conocida por el expedidor: $K_{P,M}$
- Conocida por el dispositivo: $K_{Ü,M.}$ $K_{V,M}$

La descripción de proceso 6, según la figura 6, es análoga al proceso 3, cifrado de la respuesta para el mediador

1. El expedidor A calcula $C=V_D(N,ZP1;K_{V,D})$ y $E=A_A(C,ZP5;K_{A,A})$. El expedidor A envía <DID,E,C,ZP2> a la central [ZP2 comprende los valores de ZP5 requeridos para la comprobación de la autentificación y, dado el caso, más información]
2. El mediador comprueba la autentificación del expedidor A mediante $Ü_A(E,C,ZP5;K_{Ü,A})$. El mediador calcula $B=A_M(C,ZP3;K_{A,M})$ y envía <B,C,ZP4> al dispositivo [ZP4 comprende los valores de ZP3 requeridos para la comprobación de la autentificación y, dado el caso, más información]
3. El dispositivo D comprueba la autentificación del mediador mediante $Ü_M(B.C.ZP4;K_{Ü,M})$
4. El dispositivo D descifra el mensaje mediante $E_D(C,K_{E,D})$.
5. El dispositivo D entrega el mensaje N (y dado el caso, información al expedidor A) mediante los medios de salida conectados
6. El dispositivo D calcula (dado el caso, tras la autorización por parte del usuario) $F=B_D(\text{Respuesta, ZP6};K_{B,D})$ así como $H=V_M(F,ZP10;K_{V,M})$ y envía <H,ZP11> al mediador
7. El mediador calcula $<F,ZP10>= E_M(M;K_{E,M})$, comprueba la confirmación por el dispositivo D mediante $P_D(F,ZP7;K_{P,D})$; cuando se ha realizado con éxito la comprobación, el mediador confirma el origen y la integridad de la respuesta del dispositivo D mediante $G=B_M(\text{Respuesta ZP8};K_{P,M})$ y envía <DID,G,ZP9> al expedidor A
8. El expedidor A comprueba la confirmación del mediador mediante $P_M(G,ZP9;K_{P,M})$. Una vez realizada la comprobación con éxito, el expedidor A interpreta la respuesta.

Claves que se precisan:

Dispositivo:
- Clave propia: $K_{E,D,}$ $K_{B,D}$
- Clave del mediador: $K_{Ü,M}$, $K_{V,M}$
- Conocida por el mediador $K_{P,D}$
- Conocida por el expedidor: $K_{V,D}$

Expedidor
- Clave propia $K_{A,A}$ (también puede ser userID/password)

	Clave del mediador: $K_{P,M}$ Clave del dispositivo: $K_{V,D}$
Mediador	
	Clave propia $K_{A,M}$, $K_{B,M}$ $K_{E,M}$ Clave del dispositivo: $K_{P,D}$ Clave del expedidor: $K_{Ü,A}$ (también puede ser userID/password) Conocida por el expedidor: $K_{P,M}$ Conocida por el dispositivo: $K_{Ü,M.}$ $K_{V,M}$

En la descripción de proceso 7 se emplea asimismo un ID de mensaje proporcionado por el expedidor.

El proceso es idéntico a uno de los procesos 1-6 descritos anteriormente. El expedidor A transmite asimismo un ID de mensajes NID_A que depende del dispositivo y del expedidor, que cifra como (parte de) ZP1 junto con el mensaje N propiamente dicho. El dispositivo descifra el mensaje N y lo entrega mediante los medios de salida conectados, si el NID_A es válido (p. ej. superior al NID_A último transmitido por el expendedor A, aunque como máximo superior en 3). En esta manifestación, el dispositivo debe memorizar por cada expendedor A el último NID_A recibido.

Claves que se precisan:

Análogamente al proceso básico

La descripción de proceso 8 emplea un ID de mensaje administrado centralizadamente.

El proceso es idéntico a uno de los procesos 1 a 6 descritos anteriormente. El mediador administra por cada dispositivo un ID de mensaje que él (tras la autentificación del expedidor A) antes del paso 1 transmite al expedidor si se le pide. Para ello resulta ventajosa una transmisión cifrada, para impedir que se intercepte el NID actualmente válido por parte de un tercero no autorizado. El expendedor A cifra el NID como (parte de) ZP1 junto con el mensaje N propiamente dicho. El dispositivo descifra el mensaje N y lo entrega mediante los medios de salida conectados, únicamente si el NID transmitido es válido (p. ej. superior al NID último transmitido por el expendedor A, aunque como máximo superior en 3). En esta manifestación, el dispositivo debe memorizar únicamente el NID del último mensaje entregado.

Claves que se precisan:

Análogamente al proceso básico

En la descripción de proceso 9 se emplean claves del mediador específicas del dispositivo o del expedidor.

El proceso es idéntico a uno de los procesos 1 a 8 descritos anteriormente. Sin embargo, según el expedidor o según el dispositivo se emplea una clave distinta del mediador. En una variante del procedimiento, el mediador puede transmitir el NID (asimismo) como (parte de) ZP3 al dispositivo. La condición para ello es el empleo de unos pares de claves ($K_{A,M,D,}$ $K_{Ü,M,D}$) distintos por cada dispositivo y el empleo de un procedimiento de cifrado para la autentificación del mediador (es decir, con $A_M(C,ZP3;K_{A,M,D})$ ZP3 no se puede determinar si no se conoce $K_{U,M,D}$)

Claves que se precisan

Análogamente al proceso básico, aunque con unas claves específicas del dispositivo $K_{A,M,D}$, $K_{Ü,M\ D,}$ $K_{V,M,D,}$ $K_{E,M,D}$ en lugar de las claves independientes del dispositivo $K_{A,M}$, $K_{Ü,M,}$ $K_{V,M,}$ $K_{E,M}$ y las claves específicas del expedidor $K_{B,M,A}$, $K_{P,M,A}$ en lugar de las claves independientes del expedidor $K_{B,M}$, $K_{P,M}$

En la descripción de proceso 10 se emplea asimismo un servicio de cronomarcador.

El proceso es idéntico a uno de los procesos 1 a 9 descritos anteriormente, aunque el mediador puede confirmar de forma demostrable para terceros, mediante la función $J=Z_M(I.ZP11;K_{Z,M})$, el momento de recepción o de envío, para una información I cualquiera que deba recibir o enviar. Todo aquel que posea acceso a la clave asociada $K_{T,M}$, con la ayuda de la función $T_m(I,J,ZP11, K_{T,M})$ puede comprobar la autenticidad del cronomarcador.

Claves que se precisan:

Análogamente al proceso básico, aunque asimismo la clave $K_{T,M}$ del mediador al comprobar el cronomarcador (dispositivo, expedidor o tercero) y la llave propia $K_{Z,M}$ en el mediador.

Las formas de realización descritas sirven para una mejor comprensión y no pretenden restringir la presente invención.

REIVINDICACIONES

1. Procedimiento para un intercambio seguro de mensajes digitales para una transacción entre uno o varios expedidor(es) y uno o varios receptor(es), en el que

a) el mensaje del expedidor se transmite mediante la acción de un tercero, a saber, un mediador, no siendo la comunicación legible para el mediador debido a que el mensaje se transmite en forma cifrada y

b) en el que el expedidor se autentifica ante el mediador y, por consiguiente, el mensaje procede con seguridad del expedidor y

c) en el que el mediador se autentifica ante el receptor y, por consiguiente, se puede evitar la recepción de mensajes no pretendidos, y en el que el sistema operativo del receptor se endurece y no permite la ejecución de códigos ajenos y

d) el receptor visualiza el mensaje descifrado y

e) tras la aprobación por el usuario del receptor proporciona una respuesta con confirmación y la transmite al expedidor, directamente o mediante la acción de un mediador, verificando el expedidor el origen y la integridad del mensaje de respuesta mediante una función de test y la transacción puede confirmarse realmente.

2. Procedimiento según la reivindicación anterior, en el que el receptor proporciona una respuesta con confirmación y la transmite al expedidor mediante la acción de un mediador, verificando el mismo el origen y la integridad del mensaje de respuesta mediante una función de test en la que el mediador confirma preferentemente al expedidor el origen y la integridad de la respuesta, y el expedidor verifica la confirmación del mediador mediante una función de test.

3. Procedimiento según cualquiera de las reivindicaciones anteriores, en el que el expedidor asigna unos valores aleatorios a una o varias respuestas posibles y los cifra y los incorpora, junto con las posibles respuestas, al mensaje transmitido al receptor, pudiendo el mismo responder al mensaje mediante la emisión de un valor aleatorio correspondiente al expedidor evitando que el mediador o cualquier otro tercero pueda obtener cualquier información relativa a la respuesta real.

4. Procedimiento según cualquiera de las reivindicaciones anteriores en el que el mediador puede interpretar o descodificar el mensaje o aspectos parciales del mensaje y puede, por consiguiente, generar unos datos estadísticos concernientes a los expedidores o receptores correspondientes.

5. Procedimiento según cualquiera de las reivindicaciones anteriores en el que los mensajes transmitidos por el expedidor se proporcionan con un identificador de mensaje ID inequívoco, administrado por el expedidor o por el mediador y pueden depender de la identidad del expedidor o del receptor, en el que el receptor únicamente acepta el mensaje basado en dicho identificador ID, cuando lo considera válido el receptor, y en el que los mensajes transmitidos por el expedidor se proporcionan preferentemente con un ID que comprende una información temporal, de tal forma que quede descartada la presencia de dos mensajes idénticos.

6. Procedimiento según cualquiera de las reivindicaciones anteriores, en el que las funciones realizadas por el receptor se implementan en un dispositivo portátil, en el que los mensajes pueden transferirse mediante una conexión por cable, mediante unas señales de radio o mediante unas señales ópticas y presenta preferentemente una función muy limitada que comprende la confirmación, el rechazo y la visualización de una información en un visualizador.

7. Procedimiento según cualquiera de las reivindicaciones anteriores, en el que el receptor cifra una respuesta y la transmite al mediador, de tal forma que únicamente el mediador pueda descifrar de nuevo el mensaje de respuesta y transmitirlo al expedidor.

8. Sistema para un intercambio seguro de informaciones digitales para una transacción con un mediador y un receptor **caracterizado por** un mediador y un receptor para la realización del procedimiento de la reivindicación 1 entre uno o varios expedidor(es) y uno o varios receptor(es), en el que el mensaje del expedidor se transmite mediante la acción del mediador, no siendo legible el mensaje para el mediador debido a que está cifrado y en el que el mediador comprende unos medios de tal forma que el expedidor se autentifique ante el mediador y, por consiguiente, el mensaje procede con seguridad del expedidor y en el que se proporcionan unos medios para que el mediador se autentifique ante el receptor y, por consiguiente, se pueda evitar la recepción de mensajes no pretendidos y en el que el sistema operativo del receptor se endurece y no permite la ejecución de otros códigos y el receptor comprende unos medios para descifrar y visualizar el mensaje; y comprende unos medios para que el usuario pueda autorizar el receptor y para

generar una respuesta y proporcionarla con una confirmación y transmitirla directamente, o mediante la acción de un mediador, al expedidor, verificando éste el origen y la integridad del mensaje de respuesta mediante una función de test de tal forma que permita la confirmación de la transacción.

9. Sistema según la reivindicación anterior, en el que el receptor provee una confirmación al mensaje de respuesta y lo transmite directamente al expedidor mediante la acción del mediador, verificando el expedidor el origen y la integridad del mensaje de respuesta mediante una función de test y/o en el que el receptor provee una confirmación a la respuesta y la envía al expedidor mediante la acción del mediador, verificando el expedidor el origen y la integridad del mensaje de respuesta mediante un función de test y en el que preferentemente el mediador confirma al expedidor el origen y la integridad de la respuesta y en el que el expedidor verifica la confirmación del mediador mediante una función de test.

10. Sistema según cualquiera de las reivindicaciones del sistema anteriores, en el que el expedidor asigna unos valores aleatorios a uno o a varios mensajes de respuesta posibles y los transmite, junto con las respuestas posibles, incorporados al mensaje cifrado y transmitido al receptor, pudiendo responder el receptor al mensaje mediante la transmisión del valor aleatorio correspondiente al expedidor, evitando que el mediador o cualquier tercero pueda obtener cualquier información concerniente a la respuesta efectiva.

11. Sistema según cualquiera de las reivindicaciones del sistema anteriores, en el que el mediador puede interpretar y descodificar el mensaje o unos aspectos parciales del mismo y, por consiguiente, generar unos datos estadísticos correspondientes al expedidor o receptor.

12. Sistema según cualquiera de las reivindicaciones del sistema anteriores, en el que los mensajes transmitidos por el expedidor se dotan de un identificador inequívoco del mensaje ID, administrado por el mediador y que puede depender de la identidad del expedidor o del receptor, en el que el receptor únicamente acepta el mensaje basado en dicho identificador ID, cuando el receptor lo considera válido y en el que los mensajes transmitidos por el expedidor se dotan preferentemente de un ID que comprende una información temporal, de tal forma que se descarte la presencia de dos mensajes idénticos.

13. Sistema según cualquiera de las reivindicaciones del sistema anteriores, en el que el receptor cifra una respuesta y la transmite al mediador, de tal forma que el mediador pueda descifrar el mensaje de respuesta y hacerlo llegar al expedidor.

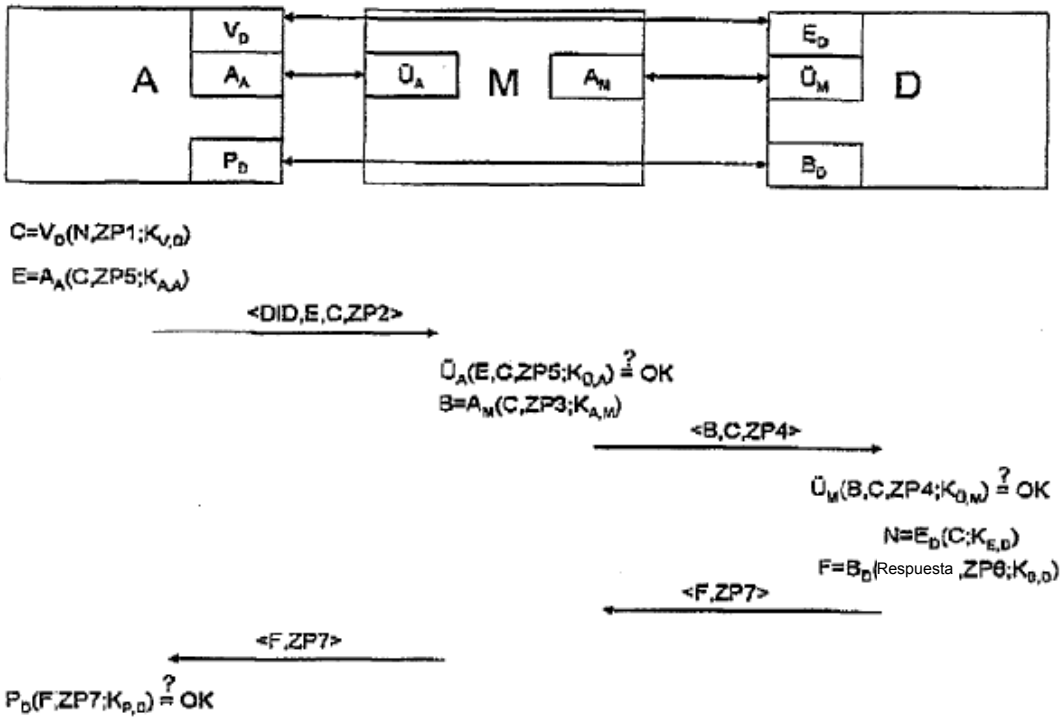
A
V_D
A_A
P_D
$Ü_A$
M
A_M
E_D
$Ü_M$
B_D
D
$C=V_D(N,ZP1;K_{V,D})$
$E=A_A(C,ZP5;K_{A,A})$
<DID,E,C,ZP2>
$Ü_A(E,C,ZP5;K_{Ü,A}) \stackrel{?}{=} OK$
$B=A_M(C,ZP3;K_{A,M})$
<B,C,ZP4>
$Ü_M(B,C,ZP4;K_{Ü,M}) \stackrel{?}{=} OK$
$N=E_D(C;K_{E,D})$
$F=B_D$(Respuesta ,ZP6;$K_{B,D}$)
<F,ZP7>
<F,ZP7>
$P_D(F,ZP7;K_{P,D}) \stackrel{?}{=} OK$

Fig. 1

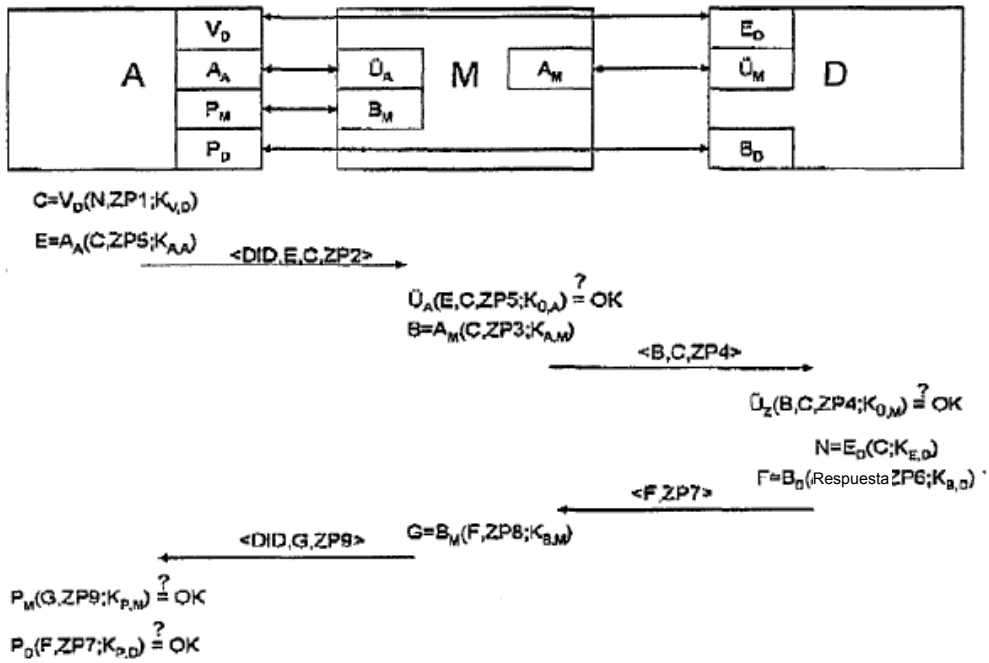
A
V_D
A_A
P_M
P_D
$Ü_A$
B_M
M
A_M
E_D
$Ü_M$
B_D
D
$C=V_D(N,ZP1;K_{V,D})$
$E=A_A(C,ZP5;K_{A,A})$
<DID,E,C,ZP2>
$Ü_A(E,C,ZP5;K_{Ü,A}) \stackrel{?}{=} OK$
$B=A_M(C,ZP3;K_{A,M})$
<B,C,ZP4>
$Ü_Z(B,C,ZP4;K_{Ü,M}) \stackrel{?}{=} OK$
$N=E_D(C;K_{E,D})$
$F=B_D$(Respuesta ZP6;$K_{B,D}$)
<F,ZP7>
$G=B_M(F,ZP8;K_{B,M})$
<DID,G,ZP9>
$P_M(G,ZP9;K_{P,M}) \stackrel{?}{=} OK$
$P_D(F,ZP7;K_{P,D}) \stackrel{?}{=} OK$

Fig. 2

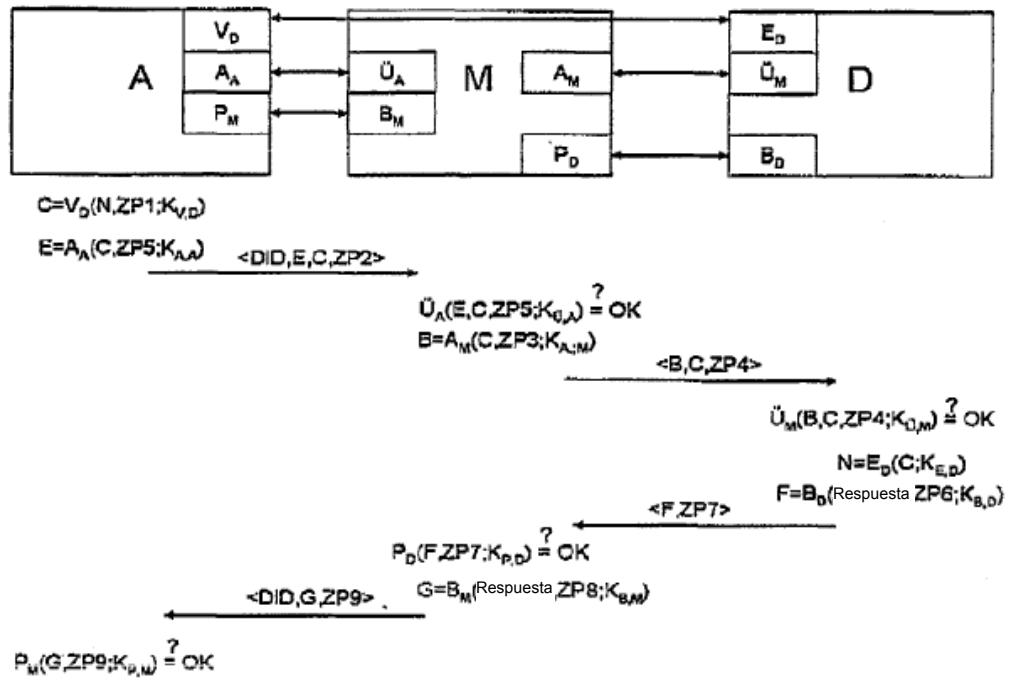
A
V_D
A_A
P_M
$Ü_A$
B_M
M
A_M
P_D
E_D
$Ü_M$
B_D
D
$C=V_D(N,ZP1;K_{V,D})$
$E=A_A(C,ZP5;K_{A,A})$
<DID,E,C,ZP2>
$Ü_A(E,C,ZP5;K_{Ü,A}) \stackrel{?}{=} OK$
$B=A_M(C,ZP3;K_{A,M})$
<B,C,ZP4>
$Ü_M(B,C,ZP4;K_{Ü,M}) \stackrel{?}{=} OK$
$N=E_D(C;K_{E,D})$
$F=B_D(\text{Respuesta ZP6};K_{B,D})$
<F,ZP7>
$P_D(F,ZP7;K_{P,D}) \stackrel{?}{=} OK$
$G=B_M(\text{Respuesta ZP8};K_{B,M})$
<DID,G,ZP9>
$P_M(G,ZP9;K_{P,M}) \stackrel{?}{=} OK$

Fig. 3

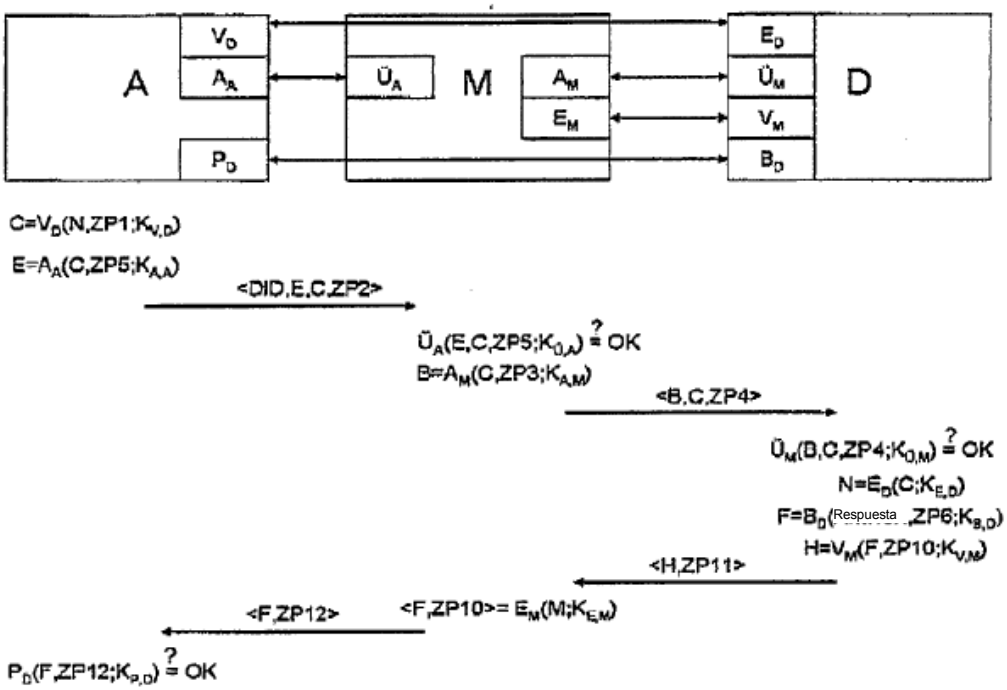
A
V_D
A_A
P_D
$Ü_A$
M
A_M
E_M
E_D
$Ü_M$
V_M
B_D
D
$C=V_D(N,ZP1;K_{V,D})$
$E=A_A(C,ZP5;K_{A,A})$
<DID,E,C,ZP2>
$Ü_A(E,C,ZP5;K_{Ü,A}) \stackrel{?}{=} OK$
$B=A_M(C,ZP3;K_{A,M})$
<B,C,ZP4>
$Ü_M(B,C,ZP4;K_{Ü,M}) \stackrel{?}{=} OK$
$N=E_D(C;K_{E,D})$
$F=B_D(Respuesta,ZP6;K_{B,D})$
$H=V_M(F,ZP10;K_{V,M})$
<H,ZP11>
<F,ZP12>
<F,ZP10>= $E_M(M;K_{E,M})$
$P_D(F,ZP12;K_{P,D}) \stackrel{?}{=} OK$

Fig. 4

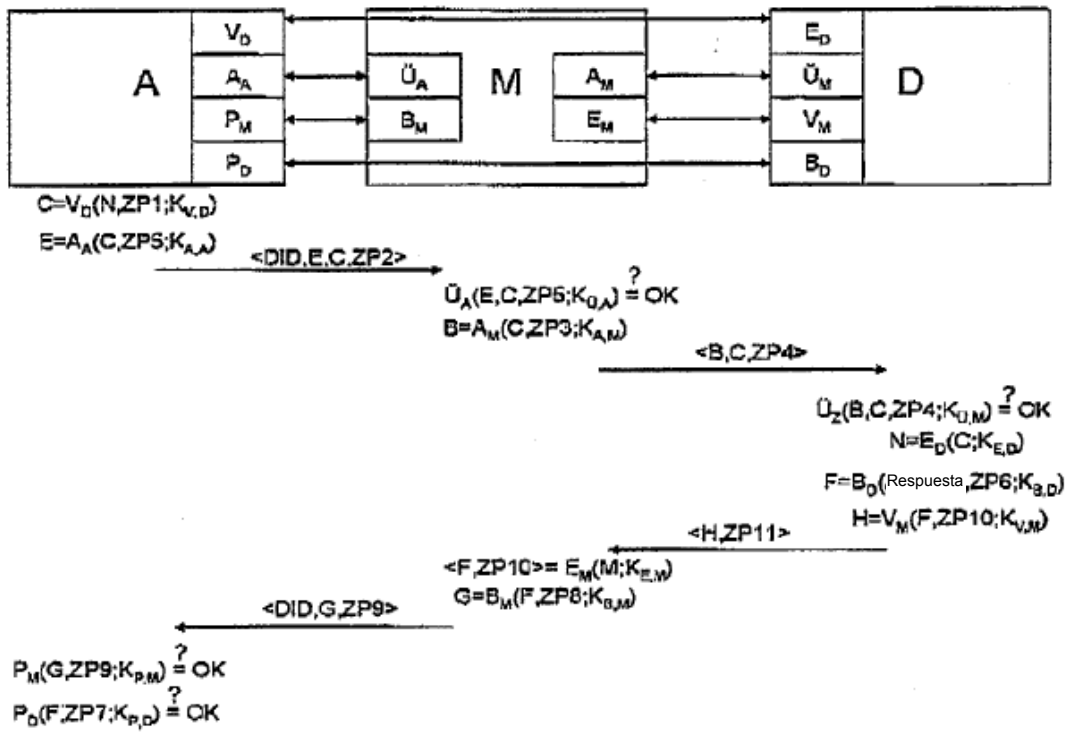
A
M
D
V_D
A_A
P_M
P_D
$Ü_A$
B_M
A_M
E_M
E_D
$Ü_M$
V_M
B_D
C=V_D(N,ZP1;$K_{V,D}$)
E=A_A(C,ZP5;$K_{A,A}$)
<DID,E,C,ZP2>
$Ü_A$(E,C,ZP5;$K_{Ü,A}$) ? OK
B=A_M(C,ZP3;$K_{A,M}$)
<B,C,ZP4>
$Ü_Z$(B,C,ZP4;$K_{Ü,M}$) ? OK
N=E_D(C;$K_{E,D}$)
F=B_D(Respuesta,ZP6;$K_{B,D}$)
H=V_M(F,ZP10;$K_{V,M}$)
<H,ZP11>
<F,ZP10>= E_M(M;$K_{E,M}$)
G=B_M(F,ZP8;$K_{B,M}$)
<DID,G,ZP9>
P_M(G,ZP9;$K_{P,M}$) ? OK
P_D(F,ZP7;$K_{P,D}$) ? OK

Fig. 5

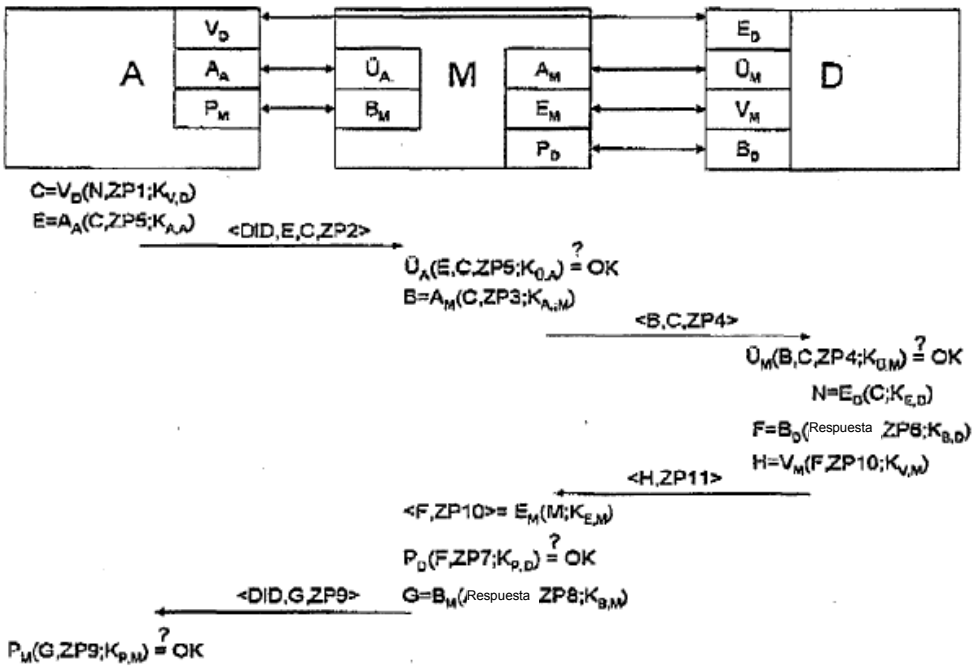
A
M
D
V_D
A_A
P_M
$Ü_A$
B_M
A_M
E_M
P_D
E_D
$Ü_M$
V_M
B_D
$C=V_D(N,ZP1;K_{V,D})$
$E=A_A(C,ZP5;K_{A,A})$
<DID,E,C,ZP2>
$Ü_A(E,C,ZP5;K_{Ü,A}) \stackrel{?}{=} OK$
$B=A_M(C,ZP3;K_{A,M})$
<B,C,ZP4>
$Ü_M(B,C,ZP4;K_{Ü,M}) \stackrel{?}{=} OK$
$N=E_D(C;K_{E,D})$
$F=B_D(\text{Respuesta},ZP6;K_{B,D})$
$H=V_M(F,ZP10;K_{V,M})$
<H,ZP11>
$<F,ZP10>=E_M(M;K_{E,M})$
$P_D(F,ZP7;K_{P,D}) \stackrel{?}{=} OK$
<DID,G,ZP9>
$G=B_M(\text{Respuesta},ZP8;K_{B,M})$
$P_M(G,ZP9;K_{P,M}) \stackrel{?}{=} OK$

Fig. 6

N.° de proceso	Clave en el expedidor			Clave en el mediador			Clave en el dispositivo	
	Propia	Mediador	Dispositivo	Propia	Expedidor	Dispositivo	Propia	Mediador
1	$K_{A,A}$	–	$K_{V,D}$, $K_{P,D}$	$K_{A,M}$	$K_{U,A}$	–	$K_{E,D}$, $K_{B,D}$	$K_{U,M}$
2	$K_{A,A}$	$K_{P,M}$	$K_{V,D}$, $K_{P,D}$	$K_{A,M}$, $K_{E,M}$	$K_{U,A}$	–	$K_{E,D}$, $K_{B,D}$	$K_{U,M}$
3	$K_{A,A}$	$K_{P,M}$	$K_{V,D}$	$K_{A,M}$, $K_{U,M}$	$K_{U,A}$	$K_{P,D}$	$K_{E,D}$, $K_{A,D}$	$K_{U,M}$
4	$K_{A,A}$	–	$K_{V,D}$, $K_{P,D}$	$K_{A,M}$, $K_{E,M}$	$K_{U,A}$	–	$K_{E,D}$, $K_{B,D}$	$K_{U,M}$, $K_{V,M}$
5	$K_{A,A}$	$K_{P,M}$	$K_{V,D}$, $K_{P,D}$	$K_{A,M}$, $K_{U,M}$, $K_{E,M}$	$K_{U,A}$	–	$K_{E,D}$, $K_{B,D}$	$K_{U,M}$, $K_{V,M}$
6	$K_{A,A}$	$K_{P,M}$	$K_{V,D}$	$K_{A,M}$, $K_{B,M}$, $K_{E,M}$	$K_{U,A}$	$K_{P,D}$	$K_{E,D}$, $K_{B,D}$	$K_{U,M}$, $K_{V,M}$
7[1]								
8[1]								
9[1]		$K_{P,M,A}$		$K_{A,M,D}$, $K_{B,M,A}$, $K_{E,M,D}$				$K_{U,M,D}$, $K_{V,M,D}$
10[1]		$(K_{T,M})$		$K_{Z,M}$				$(K_{T,M})$

Fig. 7

N.° de proceso	en el expedidor	en el mediador	en el dispositivo
1	A_A, V_D, P_D	A_M, $\ddot{U}_A$	E_D, B_D, $\ddot{U}_M$
2	A_A, P_M, V_D, P_D	A_M, B_M, $\ddot{U}_A$	E_D, B_D, $\ddot{U}_M$
3	A_A, P_M, V_D	A_M, B_M, $\ddot{U}_A$, P_D	E_D, B_D, $\ddot{U}_M$
4	A_A, V_D, P_D	A_M, $\ddot{U}_A$, E_M	$\hat{E}_D$, B_D, $\ddot{U}_M$, V_M
5	A_A, P_M, V_D, P_D	A_M, B_M, $\ddot{U}_A$, E_M	$\hat{E}_D$, B_D, $\ddot{U}_M$, V_M
6	A_A, P_M, V_D	A_M, B_M, $\ddot{U}_A$, P_D, E_M	$\hat{E}_D$, B_D, $\ddot{U}_M$, V_M
7[2]			
8[2]			
9[2]			
10[2]	(T_M)	Z_M	(T_M)

Fig. 8

REFERENCIAS CITADAS EN LA DESCRIPCIÓN

La presente lista de referencias citadas por el solicitante se presenta únicamente para la comodidad del lector. No forma parte del documento de patente europea. Aunque la recopilación de las referencias se ha realizado muy cuidadosamente, no se pueden descartar errores u omisiones y la Oficina Europea de Patentes declina toda responsabilidad en este sentido.

Documentos de patente citados en la descripción

- **US 6137884 A**