(19) OFICINA ESPAÑOLA DE PATENTES Y MARCAS

ESPAÑA

(11) Número de publicación: **2 380 026**

(51) Int. CI.:
G06F 21/20 (2006.01)

(12) TRADUCCIÓN DE PATENTE EUROPEA T3

(96) Número de solicitud europea: **05745495 .1**
(96) Fecha de presentación: **10.05.2005**
(97) Número de publicación de la solicitud: **1886204**
(97) Fecha de publicación de la solicitud: **13.02.2008**

(54) Título: **Procedimiento de transación y procedimiento de verificación**

(45) Fecha de publicación de la mención BOPI:
07.05.2012

(45) Fecha de la publicación del folleto de la patente:
07.05.2012

(73) Titular/es:
DTS LTD.
NATHAN HOUSE LAVITTS QUAY
CORK, IE

(72) Inventor/es:
WARD, Scott, MacDonald y
TEL, Teunis

(74) Agente/Representante:
Sugrañes Moliné, Pedro

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).

DESCRIPCIÓN

Procedimiento de transacción y procedimiento de verificación

La presente invención se refiere a un procedimiento de transacción y a un procedimiento de verificación para verificar una parte de transacción.

En la actualidad, numerosas transacciones están siendo manejadas por medios electrónicos en formato digital. Las redes digitales han evolucionado en el sentido de permitir que partes de clase diferente en todo el mundo se comuniquen entre sí e intercambien datos e información para realizar las transacciones deseadas.

En las transacciones, en particular en las transacciones que implican acceso a redes privadas, compromisos contractuales o financieros, acuerdos y/o pagos, cada parte que interviene en dicha transacción desea realizar la verificación de cualquier otra parte, o al menos, poder rastrear a cualquier otra parte, por si después de la terminación de la transacción surge algún problema. Para dichos fines de verificación, se sabe usar identificadores personales, como contraseñas, Números de Identificación Personales (PIN), y similares, que son sólo conocidos por un usuario específico. Sin embargo, al usar identificadores personales en redes públicas como Internet, existe la posibilidad de que el identificador personal sea conocido por otra persona, lo que permitiría a esa otra persona ejecutar transacciones o tener acceso a datos digitales presentándose a sí misma como si fuera otra. Si surgiera un problema después de la terminación de la transacción, no sería posible rastrear al interlocutor de la transacción real, ya que su identificador personal podría haber sido usado por un usuario malicioso de la red pública.

El documento GB 2 338 381 desvela un sistema para la autenticación de transacciones en una red pública, en el que un terminal envía digitalmente datos de transacción firmados a un proveedor de servicios en una red pública, junto con datos de solicitud de tarjeta generados por una tarjeta inteligente. Los datos de solicitud de tarjeta son enviados a un servidor de autorización que verifica que la tarjeta inteligente es válida y que los datos de solicitud de tarjeta deben haber sido generados por esa tarjeta inteligente en la transacción actual. También se envía información de identificación de usuario desde el terminal al proveedor de servicios y desde allí al servidor de autorización, en el que se verifica esta información con los detalles correctos del usuario para la tarjeta inteligente. Los resultados de estas verificaciones se indican en una respuesta de autorización firmada digitalmente desde el servidor de autorización al proveedor de servicios, que a continuación determina si se debe o no seguir con la transacción estableciendo criterios de aceptación para la transacción actual y determinando a partir de la respuesta de autorización si se cumplen estos criterios.

Para una transacción más segura, se ha propuesto en el documento EP 1 219 088 usar un servidor de transacciones de tercera parte de confianza que comprende perfiles de las partes de transacción. El servidor de transacciones verifica la identidad de las partes de transacción usando datos de autenticación que comprenden una tabla de datos aleatorios para verificar una firma digital. La firma digital es generada a partir de un testigo aleatorio usando un lector de testigos. La tabla de datos aleatorios corresponde a datos recogidos de dicho testigo aleatorio. Así, una firma digital que se origina en el testigo aleatorio y que es diferente para cada transacción ulterior es prácticamente imposible de suplantar y, por tanto, identifica de forma única la parte de transacción por el testigo aleatorio usado por la parte de transacción.

El documento WO 2004 111 752 desvela un procedimiento para realizar una transacción electrónica. El procedimiento proporciona un dispositivo electrónico con datos de autenticación y software de autenticación almacenados preferentemente en un lugar de almacenamiento seguro u otro lugar inaccesible para el usuario o el sistema operativo del dispositivo. Cuando se solicita una autenticación de firma digital desde una primera parte de transacción asociada con el dispositivo electrónico por una segunda parte de transacción, se activa el software de autenticación para generar dicha firma digital a partir de los datos de autenticación almacenados en la posición de almacenamiento segura usando datos específicos de transacción, para generar así una firma digital específica de la transacción. A continuación se proporciona la firma digital a la segunda parte de transacción.

La segunda parte de transacción puede estar almacenando los datos de autenticación junto con información de identificación de la primera parte de transacción, debido, por ejemplo, a que la segunda parte de transacción proporcionó originalmente los datos de autenticación a la primera parte de transacción. Usando los datos específicos de transacción, la segunda parte de transacción puede, como la primera parte de transacción, generar la firma digital específica de la transacción. Una comparación de la firma digital recibida y la generada permite a la segunda parte de transacción verificar la identidad de la primera parte de transacción.

Una consecuencia del procedimiento descrito anteriormente para proporcionar una firma digital específica de la transacción es el hecho de que la segunda parte de transacción guarda todos los datos para generar la firma digital específica de la transacción. Por tanto, la segunda parte de transacción está habilitada para generar una firma digital de la primera parte de transacción, permitiendo así el uso fraudulento. La primera parte de transacción puede usar esta consecuencia para sugerir que la segunda parte usó su capacidad para cometer fraude después de la

transacción, intentando así provocar incertidumbre sobre si la primera parte de transacción realizó la transacción. Además, cualquier otra parte puede obtener todos los datos ilegalmente de la segunda parte de transacción y realizar transacciones a la vez que se presenta a sí misma como la primera parte de transacción.

Un objeto de la presente invención es proporcionar un procedimiento de transacción y un procedimiento de autenticación en los que una parte de transacción pueda verificarse más allá de cualquier duda razonable.

Para alcanzar el anterior objeto, la presente invención proporciona un procedimiento para permitir la autenticación de una primera parte de transacción de una transacción electrónica con una segunda parte de transacción, comprendiendo el procedimiento la instalación de un dispositivo electrónico de dicha primera parte de transacción, comprendiendo el procedimiento:

- suministrar datos de autenticación en una primera sección de memoria de dicho dispositivo electrónico de manera que los datos de autenticación sean inaccesibles para un usuario de dicho dispositivo electrónico;

- la segunda parte de transacción suministrar datos de identificación públicos en una segunda sección de memoria de dicho dispositivo electrónico;

- generar un código de identificación secreto SIC en el dispositivo electrónico de la primera parte de transacción;

- almacenar el SIC en una tercera sección de memoria de dicho dispositivo electrónico de manera que el SIC sea inaccesible para un usuario de dicho dispositivo electrónico;

- la segunda parte de transacción suministrar el software de autenticación a dicho dispositivo electrónico, los datos de autenticación y el SIC siendo accesibles para dicho software de autenticación;

- generar un certificado de SIC encriptando el SIC en el dispositivo electrónico de la primera parte de transacción;

- generar una clave de encriptación de sesión a partir de los datos de autenticación usando datos específicos de la sesión en el dispositivo electrónico de la primera parte de transacción;

- suministrar el certificado de SIC y al menos uno entre la clave de encriptación de sesión y los datos específicos de la sesión a la segunda parte de transacción;

- la segunda parte de transacción almacenar los datos de identificación públicos, el certificado de SIC y dicho al menos uno entre la clave de encriptación de sesión y los datos específicos de la sesión junto con los datos de autenticación;

- encriptar el SIC usando la clave de encriptación de sesión para generar así un SIC encriptado en el dispositivo electrónico de la primera parte de transacción;

- suministrar al menos el certificado de SIC y el SIC encriptado a una tercera parte de confianza.

La presente invención proporciona además un procedimiento para realizar una transacción electrónica entre una primera parte de transacción y una segunda parte de transacción, estando ambas partes de transacción habilitadas de acuerdo con el procedimiento anterior para permitir autenticación de una de dichas partes de transacción, comprendiendo el procedimiento:

- activar el software de autenticación para generar una firma digital a partir de los datos de autenticación;

- encriptar la firma digital usando el SIC como clave de encriptación para generar así una firma digital encriptada;

- suministrar la firma digital y la firma digital encriptada a la segunda parte de transacción.

La presente invención proporciona además un procedimiento para verificar una primera parte de transacción habiendo realizado una transacción electrónica de acuerdo con el procedimiento de transacción anterior, comprendiendo el procedimiento:

- la segunda parte de transacción suministrar el certificado de SIC, la firma digital y la firma digital encriptada, recibidos durante la transacción electrónica, a la tercera parte de confianza; y

- la tercera parte de confianza buscar el SIC correspondiente al certificado de SIC y comparación de la firma digital y la firma digital encriptada usando dicho SIC.

La presente invención mejora el procedimiento desvelado en el documento WO 2004 111 752. En los procedimientos según la presente invención sólo la primera parte de transacción guarda todos los datos necesarios para generar la firma digital y la firma digital encriptada.

Para generar la firma digital encriptada, se usan la firma digital y el código de identificación secreto (SIC). Para generar la firma digital se usan los datos de autenticación y los datos específicos de transacción. Los datos de autenticación, el certificado de SIC y los datos específicos de transacción pueden ser conocidos para la segunda parte de transacción. La segunda parte de transacción está habilitada así para verificar la firma digital. Sin embargo, el código de identificación secreto (SIC) es conocido sólo para la primera parte de transacción y la tercera parte de confianza, evitando que la segunda parte de transacción genere la firma digital encriptada. La tercera parte de confianza no está habilitada para generar la firma digital, ya que no tiene los datos específicos de transacción o los datos de autenticación.

Si la primera parte de transacción debe someterse a verificación, posiblemente en una transacción o cuando surja una disputa después de una transacción, la segunda parte de transacción proporciona el certificado de SIC, la firma digital, que ya puede haber validado usando los datos de autenticación, y la firma digital encriptada, que recibió en la transacción, a la tercera parte de confianza. La tercera parte de confianza, que tiene el SIC, puede encriptar la firma digital y comparar el resultado con la firma digital encriptada o, análogamente, puede desencriptar la firma digital encriptada y comparar el resultado con la firma digital. En cualquier modo, la tercera parte de confianza puede determinar si la firma digital está encriptada usando el código de identificación segura SIC de la primera parte de transacción.

En una forma de realización, el SIC se divide en un SIC de encriptación y un SIC de desencriptación que forman una pareja como en una clave privada y pública según se conoce en la técnica. A continuación se usa el SIC de encriptación para encriptar la firma digital. Sólo la primera parte de transacción tiene el SIC de encriptación. El SIC de desencriptación correspondiente para desencriptar la firma digital encriptada se proporciona a la tercera parte de confianza como el SIC en la forma de realización descrita anteriormente de la presente invención. Así, en esta forma de realización, una parte de los datos necesarios para generar la firma digital específica de transacción encriptada sólo está disponible para la primera parte de transacción. No se habilita por tanto ninguna combinación de partes para generar falsamente la firma digital encriptada.

A continuación se explica la presente invención con referencia a varios diagramas, en los que

el DIAGRAMA 1A ilustra un procedimiento de instalación para permitir el procedimiento de autenticación según la presente invención;

el DIAGRAMA 1B ilustra los datos disponibles para cada parte después del procedimiento de instalación del DIAGRAMA 1A;

el DIAGRAMA 1C ilustra los datos disponibles para cada parte después de realizar una forma de realización del procedimiento de instalación según la presente invención;

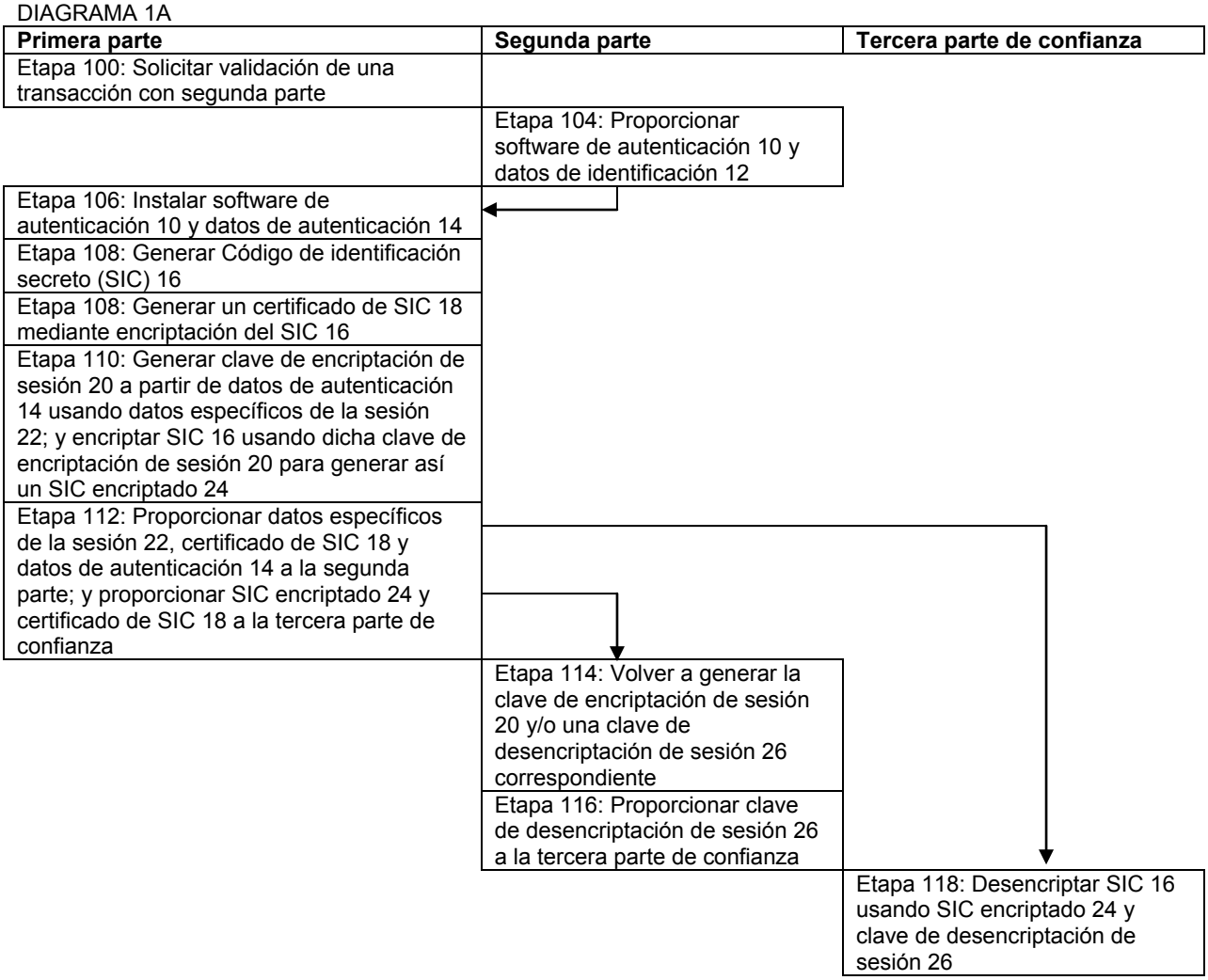
el DIAGRAMA 2 ilustra un procedimiento de transacción de acuerdo con la presente invención; y

el DIAGRAMA 3 ilustra un procedimiento de autenticación según la presente invención.

El DIAGRAMA 1A muestra un esquema de acciones realizadas por cada parte (cada columna representa las acciones de una parte). El orden de las filas representa el orden de las acciones.

En el procedimiento de instalación según la presente invención intervienen tres partes. Una primera parte de transacción y una segunda parte de transacción según se muestra en la columna izquierda y en la columna central, respectivamente, pretenden realizar una transacción electrónica. La segunda parte de transacción puede desear establecer la identidad de la primera parte de transacción, por ejemplo porque la primera parte de transacción hará un pago. Una tercera parte de confianza está tomando parte pasivamente en el procedimiento de instalación. Según se describe más adelante, la tercera parte de confianza sólo recibe ciertos datos y almacena dichos datos.

DIAGRAMA 1A



En una primera etapa 100 del procedimiento la primera parte de transacción entra en contacto con la segunda parte de transacción solicitando ser habilitada para realizar transacciones con la segunda parte de transacción. En respuesta, en la etapa 104, la segunda parte de transacción proporciona software de autenticación 10 y datos de identificación 12 a la primera parte de transacción. Los datos de identificación 12 comprenden una combinación especial de caracteres o similares para permitir identificar a la primera parte de transacción más adelante a partir de los datos de identificación 12 recibidos. Naturalmente, los datos de identificación 12 pueden ser usados también más adelante en el procedimiento para cualquier otra finalidad como, por ejemplo, encriptación de datos.

Después de la recepción del software de autenticación 10 y los datos de identificación 12, la primera parte de transacción instala el software de autenticación 10 en su dispositivo electrónico en la etapa 106. Durante la instalación del software de autenticación 10, se crea una sección de memoria segura o se accede a ella de manera que el usuario del dispositivo no pueda obtener o alterar los datos almacenados en dicha sección de memoria segura. Sólo el software de autenticación 10 puede acceder a la sección de memoria segura para obtener datos de la misma. Dicho procedimiento y dicho sistema se conocen por el documento WO 2004 111752.

En una sección de memoria segura del dispositivo electrónico se almacenan los datos de autenticación 14. Los datos de autenticación 14 pueden ser generados aleatoriamente por la primera parte de transacción o pueden deducirse a partir de los datos de identificación 12, por ejemplo. En otra forma de realización, la segunda parte puede proporcionar los datos de autenticación 14 junto con los datos de identificación 12. Si los datos de autenticación 14 no son proporcionados por la segunda parte de transacción o no pueden deducirse sin ambigüedades de los datos de identificación 12, la primera parte de transacción proporciona los datos de autenticación 14 a la segunda parte de transacción, por ejemplo en la etapa 112 que se explicará más adelante.

En la etapa 106, la primera parte de transacción genera un código de identificación secreto (SIC) 16, posiblemente iniciado por el software de autenticación 10. El SIC 16 es generado de manera que la segunda parte de transacción

no pueda obtener o deducir el SIC 16 de ninguno de los datos que la segunda parte de transacción ha proporcionado o proporciona y/o ha recibido o recibe de la primera parte de transacción.

A continuación en la etapa 108, la primera parte de transacción encripta el SIC 16 usando un algoritmo predeterminado, para generar así un certificado de SIC 18. El algoritmo se selecciona de manera que no sea posible deducir el SIC original 16 del certificado de SIC 18.

En la etapa 110, la primera parte de transacción genera una clave de encriptación de sesión 20. La clave de encriptación de sesión 20 se genera usando los datos de autenticación 14 y datos específicos de la sesión 22. Por ejemplo, los datos específicos de la sesión 22 pueden ser un número de sesión, una fecha de sesión, un número aleatorio o cualquier otro número. Es adecuada también cualquier combinación de números o caracteres. Una combinación de los datos de autenticación 14, la identificación de la primera parte de transacción y los datos específicos de la sesión 22 produce una clave de encriptación 20 específica de la sesión y específica de la primera parte de transacción. Por ejemplo, los datos de autenticación 14 forman una tabla de caracteres y los datos específicos de la sesión 22 se usan para seleccionar una serie de caracteres a partir de la tabla, para generar así una cadena de caracteres.

A continuación, la clave de encriptación de sesión se emplea para encriptar el SIC 16, para generar así un SIC encriptado 24.

Después de generar los datos de autenticación 14 mencionados anteriormente, el SIC 16, el certificado de SIC 18, la clave de encriptación de sesión 20 y el SIC encriptado 24, la primera parte de transacción proporciona los siguientes datos a la segunda parte y la tercera parte de confianza en la etapa 112. A la segunda parte de transacción se le proporcionan los datos específicos de la sesión 22, los datos de autenticación 14 (si es necesario, según se menciona anteriormente) y el certificado de SIC 18. A la tercera parte de confianza se le proporciona el certificado de SIC 18 y el SIC encriptado 24. La tercera parte de confianza puede recibir también los datos de identificación 12, aunque esto no es obligatorio.

En la etapa 114 la segunda parte de transacción usa los datos específicos de la sesión 22 y los datos de autenticación 14 para volver a generar la clave de encriptación de sesión 20 y/o una clave de desencriptación de sesión 26 correspondiente.

La clave de desencriptación de sesión 26 se proporciona a la tercera parte de confianza en la etapa 116.

La tercera parte de confianza ha recibido de la primera parte de transacción el certificado de SIC 18 y el SIC encriptado 24, y ha recibido de la segunda parte de transacción la clave de desencriptación de sesión 26. En la etapa 118 la tercera parte de confianza usa la clave de desencriptación de sesión para desencriptar el SIC encriptado para obtener el SIC 16. Así, la tercera parte de confianza puede obtener el SIC y el certificado de SIC.

En el DIAGRAMA 1B se ilustra qué datos están disponibles para cada parte después de la instalación según se describe anteriormente en relación con el DIAGRAMA 1A.

DIAGRAMA 1B

Primera parte	**Segunda parte**	**Tercera parte de confianza**
Datos de identificación 12	Datos de identificación 12	Datos de identificación 12
Datos de autenticación 14	Datos de autenticación 14	
Código de identificación secreto (SIC) 16		Código de identificación secreto (SIC) 16
Certificado de SIC 18	Certificado de SIC 18	Certificado de SIC 18

La primera parte de transacción, mostrada en la columna izquierda, tiene disponibles los datos de identificación 12, los datos de autenticación 14, el SIC 16 y el certificado de SIC 18. Según se describe más adelante, los datos de autenticación 14 y el SIC 16 son necesarios para generar una firma digital y para generar una firma digital encriptada para realizar una transacción electrónica.

La segunda parte de transacción tiene los datos de identificación 12, los datos de autenticación 14 y el certificado de SIC 18 disponibles. La segunda parte de transacción no tiene acceso al SIC 16 y, por tanto, la segunda parte de transacción no puede generar una firma digital encriptada válida.

La tercera parte de confianza puede tener acceso a los datos de identificación 12, que pueden ponerse a disposición pública, pero tiene al menos acceso al SIC 16 y al certificado de SIC 18. Dado que la tercera parte de confianza no tiene acceso a los datos de autorización 14, la tercera parte de confianza no puede generar una firma digital válida (encriptada).

El DIAGRAMA 1C ilustra un resultado de instalación de una forma de realización adicional del procedimiento de

instalación según la presente invención, en el que el SIC 16 se divide en un par de SIC de encriptación 16A y un SIC de desencriptación 16B. El SIC de desencriptación 16B es adecuado para desencriptar datos encriptados usando el SIC de encriptación 16A. Sin embargo, no es posible deducir el SIC de encriptación 16A del SIC de desencriptación 16B.

DIAGRAMA 1C

Primera parte	**Segunda parte**	**Tercera parte de confianza**
Datos de identificación 12	Datos de identificación 12	Datos de identificación 12
Datos de autenticación 14	Datos de autenticación 14	
Código de identificación secreto de encriptación (SIC de encriptación) 16A		
Código de identificación secreto de desencriptación (SIC de desencriptación) 16B		Código de identificación secreto (SIC de desencriptación) 16B
Certificado de SIC 18	Certificado de SIC 18	Certificado de SIC 18

Durante la instalación de acuerdo con el procedimiento ilustrado en el DIAGRAMA 1A, el SIC 16 se genera en la etapa 106. En la forma de realización adicional, el SIC 16 puede generarse como un par de encriptación-desencriptación de SIC de encriptación 16A y SIC de desencriptación 16B en la etapa 106. Posteriormente, se encripta sólo el SIC de desencriptación 16B para generar un SIC de desencriptación 24B encriptado de acuerdo con la etapa 110 del DIAGRAMA 1A. El SIC de desencriptación 24B encriptado se proporciona a la tercera parte de confianza de acuerdo con la etapa 112 del DIAGRAMA 1A. La tercera parte de confianza obtiene así el SIC de desencriptación 16B en lugar del SIC 16 como se muestra en el DIAGRAMA 1A.

En consecuencia, y como puede verse en el DIAGRAMA 1C, el SIC de encriptación 16A está disponible sólo en la primera parte de transacción. Por tanto, no se permite que ninguna parte o combinación de las partes segunda y tercera genere una firma digital encriptada válida.

El DIAGRAMA 2 ilustra un procedimiento de transacción según la presente invención.

DIAGRAMA 2

Primera parte	**Segunda parte**	**Tercera parte de confianza**
Etapa 200: Iniciar transacción con segunda parte		
	Etapa 202: Solicitar autenticación y proporcionar ID de transacción 28	
Etapa 204: Generar firma digital 30 a partir de datos de autenticación 14 usando el ID de transacción 28, y otros datos específicos de transacción y el certificado de SIC 18		
Etapa 206: Encriptar firma digital 30 usando SIC 16 para generar así una firma digital encriptada 32		
Etapa 208: Proporcionar datos de identificación 12 o certificado de SIC 18 junto con la firma digital 30 y la firma digital encriptada 32 a la segunda parte		
	Etapa 210: Verificar firma digital 30 volviendo a generar la firma digital 30 a partir de datos de autenticación 14 usando el ID de transacción 28, los otros datos específicos de transacción y el certificado de SIC 18	

Se supone que la primera parte de transacción inicia la transacción en la etapa 200. Sin embargo, la segunda parte de transacción puede iniciar asimismo la transacción. Después de inicializar la transacción, puede realizarse una serie de acciones por cualquiera de las partes de transacción. En algún momento de la transacción, por ejemplo cuando la segunda parte de transacción acepta la transacción solicitada, la segunda parte de transacción solicita a

la primera parte de transacción que proporcione una identificación y proporciona un número de identificación de transacción 28 a la primera parte de transacción (etapa 202).

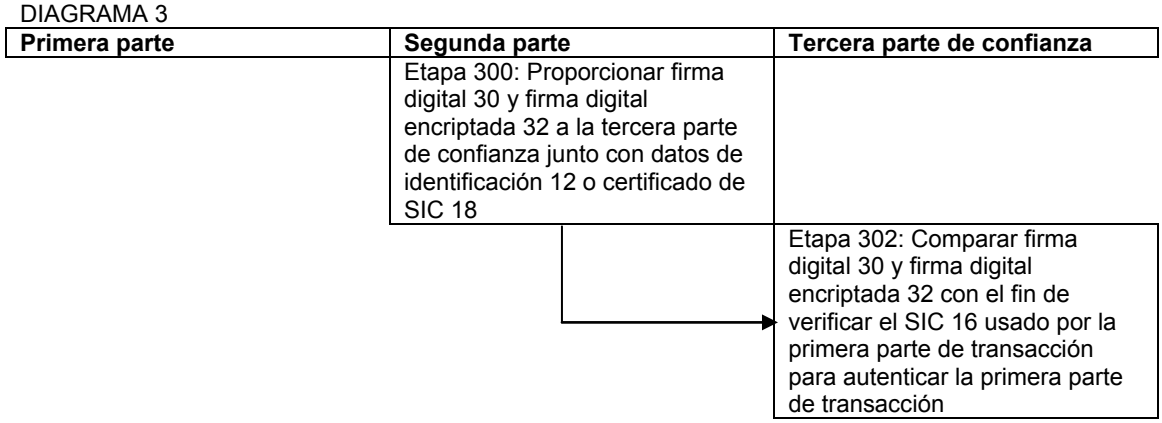
En respuesta, la primera parte de transacción inicia el software de autenticación según es proporcionado por el procedimiento de instalación mostrado en el DIAGRAMA 1A. El software de autenticación es iniciado para generar una firma digital 30 a partir de los datos de autenticación 14 según se indica en la etapa 204. Para generar una firma digital 30 a partir de los datos de autorización 14, se necesitan datos adicionales, por ejemplo el número de identificación de transacción 28, un PIN o una plantilla biométrica y el certificado de SIC 18, ligando así la firma digital 30 a la transacción y a la primera parte de transacción y/o a un usuario autorizado específico. Sin embargo, pueden usarse también otros datos.

En la etapa 206, la firma digital 30 generada es encriptada usando el SIC 16 o la encriptación del SIC 16A como clave de encriptación. La firma digital 30 y la firma digital encriptada 32 son suministradas a la segunda parte de transacción en la etapa 208. En la etapa 210, posteriormente, la segunda parte de transacción puede volver a generar la firma digital 30 cuando la segunda parte tiene todos los datos disponibles necesarios para hacerlo (ver DIAGRAMA 1B o DIAGRAMA 1C). Basándose en una comparación de la firma digital 30 recibida y la firma digital 30 generada nuevamente, la segunda parte de transacción puede autenticar la primera parte de transacción, el usuario autorizado y/o la integridad de los datos de transacción.

La segunda parte de transacción no puede volver a generar la firma digital encriptada 32, ya que la segunda parte de transacción no tiene el SIC 16 o el SIC de encriptación 16A disponibles. En cualquier caso, la segunda parte de transacción almacenará los datos relativos a la autenticación y la transacción, incluyendo entre otros la firma digital 30 recibida, la firma digital encriptada 32 recibida, el número de identificación de transacción 28, el certificado de SIC 18, los datos de autorización 14 y los datos de identificación 12 que se usarán en caso de una disputa. Posteriormente, la transacción puede completarse y puede terminarse una conexión con la primera parte de transacción.

El DIAGRAMA 3 ilustra un procedimiento de verificación según la presente invención. La verificación puede realizarse durante la transacción o puede realizarse sólo cuando surja una disputa después de la terminación de la transacción, por ejemplo si la primera parte de transacción proclama que no ha realizado la transacción.

DIAGRAMA 3



Para verificar la primera parte de transacción, la segunda parte de transacción reúne datos como la firma digital 30 recibida, la firma digital encriptada 32 recibida y los datos de identificación 12 y/o el certificado de SIC 18. Los datos se suministran a la tercera parte de confianza en una primera etapa 300.

Después de la recepción de los datos, en la etapa 302, la tercera parte de confianza verifica la primera parte de transacción usando los datos de identificación 12 o el certificado de SIC 18 y reúne los datos almacenados previamente después del procedimiento de instalación según se ilustra en el DIAGRAMA 1A. Como la tercera parte de confianza tiene la firma digital 30 y el SIC 16, la tercera parte de confianza puede volver a generar la firma digital encriptada 32 y compararla con la firma digital encriptada 32 recibida, comparando con ello en la práctica el SIC 16 almacenado en la tercera parte de confianza y el SIC 16 usado por la primera parte de transacción para encriptar la firma digital 30.

Análogamente, la tercera parte de confianza puede generar una clave de desencriptación correspondiente al SIC 16 como clave de encriptación y desencriptar la firma digital encriptada 32 recibida para obtener la firma digital 30. A continuación, puede compararse la firma digital 30 obtenida con la firma digital 30 recibida. Si el SIC 16 se divide en un SIC de encriptación 16A y un SIC de desencriptación 16B según se sugiere en relación con el DIAGRAMA 1C, la tercera parte de confianza puede realizar sólo, naturalmente, una desencriptación de la firma digital encriptada 32

recibida y verificar la firma digital 32 ahora desencriptada por comparación con la firma digital 30 obtenida.

A partir de lo anterior, un experto en la materia comprenderá fácilmente cómo conseguir que se pueda generar una firma digital y una firma digital encriptada específica de la sesión y específica de la parte de transacción de manera que sólo dicha primera parte de transacción esté habilitada para generar dicha firma digital y dicha firma digital encriptada. Por tanto, posteriormente o durante la transacción, la primera transacción puede identificarse más allá de cualquier duda razonable. El procedimiento se describe anteriormente a la luz de las descripciones del documento WO 2004 111752 y es adecuado especialmente para combinarse con los procedimientos y sistemas descritos en él. Sin embargo, el procedimiento según la presente invención puede usarse asimismo en combinación con otros procedimientos de transacción sin apartarse del ámbito de la invención según comprenderán los expertos en la materia.

REIVINDICACIONES

1. Procedimiento para permitir la verificación y la autenticación de una primera parte de transacción de una transacción electrónica con una segunda parte de transacción, comprendiendo el procedimiento la instalación de un dispositivo electrónico de dicha primera parte de transacción, comprendiendo el procedimiento:

- suministrar datos de autenticación en una primera sección de memoria de dicho dispositivo electrónico de manera que los datos de autenticación sean inaccesibles para un usuario de dicho dispositivo electrónico;

- la segunda parte de transacción suministrar datos de identificación públicos en una segunda sección de memoria de dicho dispositivo electrónico;

- generar un código de identificación secreto, SIC, en el dispositivo electrónico de la primera parte de transacción;

- almacenar el SIC en una tercera sección de memoria de dicho dispositivo electrónico de manera que el SIC sea inaccesible para un usuario de dicho dispositivo electrónico;

- la segunda parte de transacción suministrar el software de autenticación a dicho dispositivo electrónico, siendo los datos de autenticación y el SIC accesibles para dicho software de autenticación;

- generar un certificado de SIC encriptando el SIC en el dispositivo electrónico de la primera parte de transacción;

- generar una clave de encriptación de sesión a partir de los datos de autenticación usando datos específicos de la sesión en el dispositivo electrónico de la primera parte de transacción;

- suministrar el certificado de SIC y al menos uno entre la clave de encriptación de sesión y los datos específicos de la sesión a la segunda parte de transacción;

- la segunda parte de transacción almacenar los datos de identificación públicos, el certificado de SIC y dicho al menos uno entre la clave de encriptación de sesión y los datos específicos de la sesión junto con los datos de autenticación;

- encriptar el SIC usando la clave de encriptación de sesión para generar así un SIC encriptado en el dispositivo electrónico de la primera parte de transacción;

- suministrar al menos el certificado de SIC y el SIC encriptado a una tercera parte de confianza.

2. Procedimiento según la reivindicación 1, en el que el suministro de los datos de autenticación en una memoria de dicho dispositivo electrónico comprende generar los datos de autenticación y el almacenamiento de los datos de autenticación en una posición de memoria segura, inaccesible para el usuario, comprendiendo además el procedimiento suministrar los datos de autenticación a la segunda parte de transacción.

3. Procedimiento según la reivindicación 1 ó 2, en el que el procedimiento comprende además:

- la segunda parte de transacción volver a generar la clave de encriptación de sesión, si se proporcionaron los datos específicos de la sesión;

- generar una clave de desencriptación de sesión correspondiente a la clave de encriptación de sesión y suministrar la clave de desencriptación de sesión a la tercera parte de confianza;

- la tercera parte de confianza desencriptar el SIC encriptado, obteniendo así el SIC;

- la tercera parte de confianza almacenar el SIC junto con el certificado de SIC.

4. Procedimiento según cualquiera de las reivindicaciones precedentes, en el que el SIC comprende un SIC de encriptación y un SIC de desencriptación correspondiente, siendo encriptado el SIC de desencriptación usando la clave de encriptación de sesión y proporcionándose a la tercera parte de confianza junto con el certificado de SIC.

5. Procedimiento para realizar una transacción electrónica entre una primera parte de transacción y una segunda parte de transacción, estando las dos partes de transacción habilitadas de acuerdo con el procedimiento según cualquiera de las reivindicaciones precedentes, comprendiendo el procedimiento:

- activar el software de autenticación para generar una firma digital a partir de los datos de autenticación;

- encriptar la firma digital usando el SIC como una clave de encriptación para generar así una firma digital encriptada;

- suministrar la firma digital y la firma digital encriptada a la segunda parte de transacción.

6. Procedimiento para realizar una transacción electrónica entre una primera parte de transacción y una segunda parte de transacción, estando ambas partes de transacción habilitadas de acuerdo con el procedimiento según la reivindicación 4, comprendiendo el procedimiento:

- activar el software de autenticación para generar una firma digital a partir de los datos de autenticación;

- encriptar la firma digital usando el SIC de encriptación como una clave de encriptación para generar así una firma digital encriptada;

- suministrar la firma digital y la firma digital encriptada a la segunda parte de transacción.

7. Procedimiento para verificar una primera parte de transacción habiendo realizado una transacción electrónica de acuerdo con el procedimiento según la reivindicación 5, comprendiendo el procedimiento:

- la segunda parte de transacción suministrar el certificado de SIC, la firma digital y la firma digital encriptada, recibidos durante la transacción electrónica, a la tercera parte de confianza; y

- la tercera parte de confianza buscar el SIC correspondiente al certificado de SIC y comparar la firma digital y la firma digital encriptada usando dicho SIC.

8. Procedimiento para verificar una primera parte de transacción habiendo realizado una transacción electrónica de acuerdo con el procedimiento según la reivindicación 6, comprendiendo el procedimiento:

- la segunda parte de transacción suministrar el certificado de SIC, la firma digital y la firma digital encriptada, recibidos durante la transacción electrónica, a la tercera parte de confianza; y

- la tercera parte de confianza buscar el SIC de desencriptación correspondiente al certificado de SIC y comparar la firma digital y la firma digital encriptada usando dicho SIC de desencriptación.

9. Procedimiento según la reivindicación 7 u 8, comprendiendo el procedimiento:

- la segunda parte de transacción volver a generar la clave de encriptación de sesión, si se han suministrado los datos específicos de la sesión;

- generar una clave de desencriptación de sesión correspondiente a la clave de encriptación de sesión y suministrar la clave de desencriptación de sesión a la tercera parte de confianza;

- la tercera parte de confianza desencriptar el proporcionado de entre el SIC encriptado y el SIC de desencriptación encriptado, obteniendo con ello uno de entre el SIC y el SIC de desencriptación.