(19) OFICINA ESPAÑOLA DE PATENTES Y MARCAS

ESPAÑA

(11) Número de publicación: **2 445 326**

(51) Int. CI.:

G06Q 20/00 (2012.01)
G07F 19/00 (2006.01)
G07F 7/10 (2006.01)

(12) TRADUCCIÓN DE PATENTE EUROPEA T3

(96) Fecha de presentación y número de la solicitud europea: **14.05.2003 E 03755996 (0)**

(97) Fecha y número de publicación de la concesión europea: **04.09.2013 EP 1509888**

(54) Título: **Método para asegurar una transacción en línea**

(30) Prioridad:

31.05.2002 FR 0206760

(45) Fecha de publicación y mención en BOPI de la traducción de la patente:
03.03.2014

(73) Titular/es:

GEMALTO SA (100.0%)
6, RUE DE LA VERRERIE
92190 MEUDON, FR

(72) Inventor/es:

SAUVEBOIS, JEAN-PAUL

(74) Agente/Representante:

ISERN CUYAS, María Luisa

DESCRIPCIÓN

Método para asegurar una transacción en línea.

La presente invención se refiere a la seguridad de una transacción comercial en línea pagado por un cliente con una tarjeta inteligente.

Cuenta con una aplicación general en los intercambios de datos seguros y en particular en el comercio electrónico cuando el cliente usa una computadora personal la comunicación en línea a través de Internet con un sitio comercial.

El desarrollo del comercio electrónico requiere de un alto nivel de seguridad de los pagos electrónicos. Es especialmente necesario para proporcionar:

- un proceso de autenticación para garantizar la identidad de los dos actores;
- la integridad de la información transmitida en conexión con la transacción y el pago
- la confidencialidad de la información intercambiada
- el no-repudio para impedir cualquier desafío a la transacción o pago.

Soluciones se han diseñado para garantizar los pagos electrónicos, tales como sistema de C-SET propuesto por los grandes agentes de tarjetas como Visa, Mastercard, American Express, JCB combinando el protocolo SET y la tarjeta inteligente (véase por ejemplo el documento tarjeta de circuito integrado Especificación para EMV2000 Sistema de Pagos versión 4.0, anexo D de procesamiento de transacciones para el chip de Comercio Electrónico). Otras soluciones son descritas por ejemplo en los documentos EP 0427465, GB 2 261 538 o también en EP 1026 644.

En general, la seguridad de las transacciones utilizando una tarjeta inteligente basada en la verificación de la autenticidad del titular tarjeta a través de la firma electrónica está entrando en una contraseña, también llamado código de acceso o código PIN (PIN es el acrónimo de Número de Identificación Personal) y sólo lo conoce el cliente y la autoridad la autenticación.

La introducción del código PIN en el teclado de una estación de procesamiento, tales como un ordenador personal conectado a un chip lector de tarjetas es arriesgado.

De hecho, teclear el código expone el PIN a una captura visual. Además, el tratamiento del PIN por la computadora lo expone a un espionaje local o remoto, cuando los estafadores tienen acceso vía internet a la computadora.

Por ejemplo, los programas espías, residentes en el ordenador, graban las páginas web y la entrada de claves durante cada sesión. Esta información se reenvía discretamente como un archivo adjunto a los infractores electrónicos. El análisis de estos documentos, permite al hacker encontrar el PIN y otra información financiera del usuario, nombre, dirección, número de tarjeta, etc.

Agentes locales también pueden sustituir al titular para realizar una transacción sin su conocimiento y a su costa desde la computadora.

Otro fraude consiste en tomar el control remoto del ordenador por un hacker. Esto se ve en la pantalla y el teclado. El teleinfractor no sólo puede reemplazar al agente local, sino también superar las pruebas de reconocimiento de patrones. Puede actuar en una transacción de bienes y modificar los términos para dejar que el usuario legítimo firme en su lugar, etc.

Del mismo modo, el trayecto del PIN en el cable que conecta el ordenador a la unidad y su paso por el último también presenta riesgos de captura, permitiendo después que un estafador pueda hacer transacciones en lugar del usuario imprudente que dejó su tarjeta en el lector, o incluso interferir en una transacción legítima y modificar los términos tales como la cantidad o el beneficiario.

Son conocidos los lectores asegurados con teclado integrado que permiten la entrada segura del PIN en particular evitando que dicho PIN no transite por el terminal.

Sin embargo, estas unidades aseguradas presentan el inconveniente de que resultan caras.

La presente invención supera este inconveniente proporcionando una solución cuya aplicación se lleva a cabo en un entorno no seguro del tipo de ordenador personal, y cuya implementación es fácil y económica al tiempo que proporciona un grado de seguridad.

Es un método para asegurar una transacción realizada en línea por un cliente con una tarjeta inteligente, definido en los términos de la reivindicación 1.

De acuerdo con una definición general de la invención, el método comprende los siguientes pasos:

a) la carga en la tarjeta inteligente, de un archivo de imagen que tiene una pluralidad de elementos capaces de formar un teclado gráfico en la pantalla de la estación de procesamiento para la introducción de un código de acceso, cada elemento del teclado gráfico se identifica por las coordenadas correspondientes;

b) de la tarjeta inteligente, cargar el archivo de imagen en la estación de procesamiento para visualizar dicho teclado gráfico en dicha pantalla

c) hacer seleccionar al cliente al menos un elemento de dicho teclado gráfico para introducir dicho código de autenticación

d) transmitir a la tarjeta inteligente las coordenadas correspondientes del elemento del teclado gráfico seleccionado por el cliente

e) en la tarjeta inteligente, comparar las coordenadas del código de autenticación derivada de las coordenadas del elemento del teclado gráfico y los transmitidos desde el código de autenticación de la parte del cliente de la tarjeta inteligente;

f) en caso de una comparación positiva en el nivel de la tarjeta, cifrar un certificado que comprenda una palabra relacionada con el resultado de la comparación, un identificador, y un desafío vinculando el resultado de la transacción en curso, y enviar dicho certificado así cifrado a la autoridad de autenticación, y

g) la autoridad de autenticación, descifra el certificado enviado para verificar la autenticidad de la titular de la tarjeta, y caso de verificación positiva, permitir la transacción.

Por lo tanto, la autenticidad de la titular de la tarjeta inteligente se verifica mediante la introducción de la contraseña en un teclado gráfico generado a través de un proceso que se establece entre la autoridad y la autenticación de la tarjeta inteligente. Este método tiene la ventaja de la reutilización sin requerir la adición de otra pantalla y trabajar en un entorno inseguro (ordenador personal) que sin embargo asegura la confidencialidad de los titulares de tarjetas vis-a-vis de los ataques locales y remotos antes mencionados.

De acuerdo con otro aspecto de la invención, el método comprende además una prueba de proximidad para verificar la presencia física del cliente cerca de la estación de procesamiento durante la transacción en línea. De este modo, también asegura que el cliente envía la transacción que es una persona que está físicamente cerca de la pantalla y físicamente en posesión de la tarjeta de chip.

Esta prueba es otra medida eficaz contra el espionaje de una operación a distancia.

La prueba de la proximidad esencialmente implica en hacer entrar a los clientes información que le había facilitado la tarjeta directamente o través del lector de tarjetas.

Preferiblemente, el ensayo de proximidad comprende las siguientes etapas:

i) equipar al lector de tarjetas inteligentes de medios de difusión de información visual y/o sonora bajo el control de la de la tarjeta de chip;

ii) hacer controlar por la tarjeta inteligente la transmisión de un conjunto seleccionado de informaciones visuales y/o sonoras;

iii) en respuesta a la transmisión del conjunto de la información, hacer accionar al cliente selectivamente la interfaz hombre/máquina del puesto de tratamiento para transmitir a destino de la tarjeta inteligente un juego de información en respuesta al juego de información transmitido por la tarjeta;

iv) en la tarjeta, se recibe el conjunto de información generada por el cliente y se compara con el juego de información juego generado por la tarjeta inteligente, y

v) en el caso de una comparación positiva, autorizar la transacción.

En la práctica, esta prueba de proximidad puede ser implementada en cualquier momento de la transacción, es decir, antes, durante y/o después.

De acuerdo con otro aspecto de la invención, debe asegurarse de que el cliente paga la cantidad correcta al comerciante legítimo y que el cliente no puede rechazar ulteriormente la transacción propiamente dicha. También se debe evitar la sustitución de los elementos de la transacción por un hacker (pirata informático) a favor de otra transacción de dicho pirata.

Para esto, la invención también proporciona un procedimiento para el no rechazo de la transacción.

En la práctica, el procedimiento de no-repudio incluye los siguientes pasos:

I) a nivel de la autoridad de autenticación, almacenamiento en un fichero de imagen la información financiera relativa a la transacción;

II) la transmisión de dicho archivo de imagen asociado a la transacción con destino a la tarjeta inteligente a través del procesamiento posterior y el chip lector de tarjetas;

III) proviniendo de la tarjeta, cargarlo en dicha estación de procesamiento dicha imagen para mostrar en la pantalla;

IV) seleccionar por parte del cliente al menos una información financiera de dicho archivo de imagen así mostrado;

V) transmitir a la tarjeta inteligente las coordenadas correspondientes de dicha información financiera así seleccionada por el cliente;

VI) a nivel de la tarjeta inteligente, cifrar un mensaje que comprende al menos dicha información financiera de la transacción financiera así deducida; y enviar dicho mensaje así cifrado con destino a la autoridad de autenticación; y

VII) a nivel de la autoridad de autenticación, descifrar el mensaje así enviado, verificar la información financiera asociada y validar la transacción en caso de verificación positiva.

La presente invención también tiene por objeto un dispositivo para la puesta en práctica del procedimiento según la invención.

La presente invención también tiene por objeto un programa de ordenador adaptado para ser ejecutado en un ordenador para realizar las funcionalidades técnicas del procedimiento según la invención.

Otras características y ventajas de la invención serán evidentes a partir de la descripción detallada de una realización no limitante de la invención con referencia a los dibujos adjuntos en los que:

- la figura 1 es una vista esquemática de los dispositivos que participan para la realización de una transacción de acuerdo con la invención;

- la figura 2 ilustra las etapas del test de proximidad de acuerdo con la invención;

- la figura 3 ilustra las etapas de autenticación del titular de la tarjeta de chip según la invención; y

- la figura 4 ilustra los pasos de no-repudio de la transacción de acuerdo con la invención.

El ejemplo elegido para ilustrar la presente invención se refiere a una aplicación de una transacción electrónica realizada a través de Internet. Por supuesto, la invención no se limita a esta sola aplicación y se refiere más en general a todas las aplicaciones seguras utilizando una tarjeta inteligente.

Preferiblemente en la Figura 1, se prevé realizar con seguridad una transacción electrónica entre un usuario y un sitio del comerciante. El usuario está instalado delante de una estación en un puesto de procesamiento PT, que es por ejemplo su ordenador personal.

Este ordenador PT está conectado a la red de internet WE y permite acceder a un sitio web del vendedor (no mostrado) en relación con una autoridad de autenticación AA.

Después de haber decidido comprar un artículo en la página de la tienda, el titular pasa una orden de compra y comunica los datos de identificación requerida por el proveedor, particularmente las referencias de su tarjeta de pago.

Para ello, el titular teclea sus datos en el teclado de su ordenador PT y los transmite a través de Internet a la página de la tienda. La comunicación entre la autoridad de autenticación y el sitio comercial AA se realiza entonces según el protocolo en vigor en la página de la tienda.

Por ejemplo, el protocolo "3D secure" desarrollado por VISA se puede implementar.

Cuando la comunicación es segura, al igual que con el protocolo "3D Secure" la identidad y autenticidad del usuario deben ser garantizadas. Para ello, el usuario debe enviar certificados cifrados basados en métodos de cifrado conocidos, ya sean de tipo simétrico o clave secreta (DES) o asimétrica ó clave pública (RSA).

Para garantizar la identidad y autenticidad del usuario, los certificados cifrados implementan software y claves que sólo está en posesión del usuario.

La implantación de dichas informaciones secreta no se puede hacer en el ordenador PT pues todos los recursos son de fácil acceso incluso a través de los virus informáticos y otros programas espía.

Estos datos secretos se almacenan preferentemente y de modo perfectamente inviolable en el circuito electrónico de una tarjeta de chip CP, a saber, su tarjeta de pago tradicional o incluso una tarjeta de crédito dedicada a las compras por Internet.

Por ello, el usuario dispone de una tarjeta de pago CP de chip electrónico obtenida de una institución financiera adecuada. Esta tarjeta se inserta en un lector de tarjetas LC conectado al ordenador PT, que le permite acceder a recursos de software de la tarjeta CP.

El ordenador PT está equipado con un software apropiado, del tipo de emulación de terminal bancario, y con el fin de poder enviar al sitio web del vendedor un certificado de autenticidad o de integridad que luego será enviado por éste ultimo a una autoridad de autenticación AA (servidor del banco) para obtener la autorización del banco para aceptar la transacción. El acceso al software de la tarjeta de activación de la emisión de certificados cifrados requiere la presentación previa de un código secreto (o código de autenticación) memorizado por el usuario y que se llama código PIN.

El tarjeta inteligente CP es un objeto estándar tal como se define en las ISO 7810, 7816 y 14443.

La tarjeta de acuerdo con la invención es capaz de comunicarse con el mundo exterior, por ejemplo, ordenador PT, el uso del CP contacto de la tarjeta inteligente.

Estos incluyen el contacto VCC que proporciona la tensión de alimentación del chip, el contacto GND que proporciona conexión a tierra del chip y los contactos D+ y D- que proporcionan la transmisión bidireccional de datos.

Cuando la transmisión de datos está garantizada por los contactos de D+ y D-, el formato de estos datos y el protocolo utilizado son definidos por la norma USB.

El interfaz USB de la tarjeta realiza una decodificación de los datos transmitidos por los contactos G+ y G- y los reformatea de manera que dichos datos pueden ser generados y gestionados por la tarjeta inteligente CP y más precisamente por su unidad central.

La transmisión USB entre la tarjeta CP y el lector LC, así como entre el lector LC y el ordenador PT presenta la ventaja de ser rápida y sincronizada en modo semi-duplex, que elimina la necesidad de transmitir una señal de reloj a través del reloj de contacto.

El contacto de I/O (entrada/salida) es por lo tanto libre y se puede utilizar para transmitir el PIN.

En la práctica, el lector de tarjetas inteligentes LC de acuerdo con la invención está destinado a acomodar la tarjeta CP para ser conectado a través de un protocolo USB.

Se incluye una carcasa en la que se inserta la tarjeta de PC y un cable con un conector USB para conectar el lector al puerto USB correspondiente del ordenador PT.

La carcasa consta de un alojamiento para recibir, al menos parcialmente, la tarjeta inteligente CP.

El alojamiento que comporta el lector de tarjetas inteligentes LC comprende medios de la conexión con las zonas de contacto situadas en las tarjetas inteligente CP.

Estos medios de conexión comprenden cinco patas que forman un cabezal, cuatro patas correspondientes a las zonas USB de la tarjeta CP, es decir, D+, D-, VCC y GND y una pata correspondiente a la salida de entrada/salida.

Esta pata entrada/salida está conectada a un circuito interno VO apropiado al lector de tarjetas inteligentes LC.

Este circuito VO es, por ejemplo, el circuito de alimentación de un diodo electroluminiscente LED montado en el lector del cable LC de modo que sea visible por el usuario.

Alternativamente, este circuito VO puede ser un emisor de informaciones sonoras y/o visuales.

Gracias a este circuito VO y a la difusión de la información pertinente, la tarjeta inteligente CP va a ser quien comunique los datos visualmente al usuario y sin que el ordenador conectado al lector LC puede darse cuenta.

Como se discute en más detalle a continuación, el circuito VO participa en la prueba de proximidad definida anteriormente.

Por su parte, por ejemplo, el puesto de tratamiento PT incluye medios de selección SE capaces de seleccionar una parte del monitor CE, un ratón o incluso un lápiz táctil o similar.

Por su parte, de acuerdo con la invención, la autoridad de autenticación AA incluye medios generadores capaces de generar al menos un programa por si mismo, capaz de generar un archivo de imagen (por ejemplo, mapa de bits) en la pantalla EC.

En la práctica, el archivo de imagen incluye al menos una pluralidad de elementos capaces de formar un teclado gráfico en la pantalla CE para introducir un código de autentificación.

Cada elemento del archivo de imagen en mapa de bits se identifica por las coordenadas correspondientes, como por ejemplo en X e Y, en la pantalla EC. Los elementos del archivo de imagen pueden consistir en elementos del grupo que consiste en representaciones de conceptos, representaciones gráficas, representaciones alfanuméricas simples o complejas, pictogramas, imágenes, combinaciones de representaciones gráficas y alfanuméricas, representaciones gráficas modificadas siguiendo las contramedidas seleccionadas.

Es muy fácil para un usuario recordar una combinación de conceptos en lugar de una combinación arbitraria de letras y números que es muy difícil de recordar.

Por el contrario, descubrir a partir de representaciones gráficas del tipo imágenes, textos y dibujos elegidos por el usuario es extremadamente difícil para los hackers potenciales, para los cuales las herramientas informáticas existentes son de ayuda limitada.

De forma ventajosa, pero no limitativa, el procedimiento de autenticación que se describirá con más detalle a continuación, utiliza una de esas representaciones conceptuales.

Se va a describir a continuación el conjunto de pasos de autenticación a proceder de acuerdo con la invención con referencia a las figuras 2 a 4.

En primer lugar (Figura 2), se procede a comprobar la proximidad:

Paso 100: la autoridad de autenticación AA recibe una solicitud de autenticación de la página de la tienda (no mostrada) a través de un protocolo del tipo 3D Secure, por ejemplo.

Paso 101: la autoridad de autenticación AA envía un programa al puesto de tratamiento PT.

Este programa comprende una forma encriptada (es decir, encriptada usando una clave pública en el caso de una función criptográfica del tipo RSA) el número de destellos de luz difundida por el circuito VO, un reto-desafío y otras informaciones que se describirán con más detalle más adelante.

Paso 102: el puesto tratamiento PT muestra en la pantalla EC un mensaje destinado al usuario.

Este mensaje puede tener la siguiente leyenda "se le invita a realizar un examen de proximidad, inserte su tarjeta y responder a cada flash del lector de tarjetas haciendo clic en el círculo rojo, pulse Aceptar cuando esté listo para comenzar."

Paso 103: el usuario hace clic en Aceptar.

Paso 104: el puesto de tratamiento PT envía al lector de tarjeta LC un applet APDU que contiene un mensaje cifrado consistente en el número de destellos de luz y un reto-desafío de la autoridad de autenticación.

Paso 105: la tarjeta inteligente PC y el usuario intercambian a través del lector LC y del puesto de tratamiento PT, informaciones en forma de preguntas/respuestas. Por ejemplo, la tarjeta inteligente CP puede enviar una información visual y/o sonora que se muestra o se difunde en el circuito VO.

Por ejemplo, estas informaciones se corresponden con destellos visuales (en número y duración) proporcionados por la autoridad de autenticación.

Paso 106: el usuario hace clic en la pantalla EC del puesto de tratamiento PT. El número de intercambios se determina con antelación (número y duración de los destellos de luz).

Paso 107: el puesto de tratamiento PT se dirige a la tarjeta CP, en respuesta a las solicitudes visuales difundidas por el circuito VO. Esta réplica comprende por ejemplo, informaciones de teclado o ratón SE devueltas por el usuario en

respuesta a la serie aleatoria (en número y duración) de los impulsos de destellos luminosos.

Paso 108: las informaciones generadas por el cliente en la pantalla EC se comparan con el conjunto de informaciones esperada por la tarjeta inteligente CP (número y duración de los destellos luminosos).

En la práctica, la envolvente temporal de las señales luminosas del circuito VO y la reconstituida por el procesamiento de mensajes transmitidos por la estación de tratamiento PT están correlacionados por la tarjeta CP.

Si las dos envolventes se solapan, entonces la tarjeta determina que el usuario ha visto la tarjeta CP.

Paso 109a, en caso de una comparación positiva, la prueba se considera exitosa y los próximos pasos de la transacción pueden efectuarse. Paso 109, en caso de comparación negativa, la operación vuelve a la etapa inicial.

Es de esperar que después de una serie de comparaciones negativas, la tarjeta inteligente CP se bloquee.

Así, la prueba de proximidad permite verificar la presencia física del usuario.

Una variante en la realización de la prueba de la proximidad consiste en pedir al usuario que reaccione a cada "flash" no haciendo clic en un área de la pantalla sino presionando un pulsador que se puede conectar a la tarjeta inteligente.

La prueba de proximidad está garantizada por el campo visual del visor VO del conector CO y no puede ser simulada por un agente fraudulento remoto (espionaje y control remoto a través de la red) o que resida en el ordenador PT por estos casos, el estafador es prácticamente ciego.

La transacción segura pueden comenzar, terminar o incluso incorporar esta prueba de proximidad y prohibir por tanto el control remoto de la tarjeta CP por parte de un agente remoto fraudulenta y bloquear la tarjeta mediante la introducción de tres códigos PIN falsos.

A continuación, se proporciona un paso de autenticación del titular de la tarjeta inteligente CP.

Paso 200: la tarjeta CP envía un mensaje informando a la estación de tratamiento PT de que la prueba de proximidad es positivo.

Paso 201: Si la prueba de la proximidad es positiva, el ordenador muestra el siguiente mensaje: "prueba de proximidad exitosa. Ahora se le solicita la autenticación. Un teclado gráfico se mostrará en breve. Por favor, introduzca su contraseña, haciendo clic en la pantalla con la ayuda del ratón. Haga clic en Aceptar cuando esté listo para iniciar el procedimiento de autenticación".

Paso 202: el usuario hace clic en Aceptar.

Paso 203: el puesto de tratamiento PT envía a la tarjeta CP una petición para mostrar un teclado gráfico.

Paso 204: la tarjeta inteligente CP envía los elementos del teclado gráfico. Paso 205: la pantalla EC muestra el teclado gráfico generado por la tarjeta inteligente CP.

Por lo tanto, se pone a disposición del usuario un teclado gráfico para que pueda entrar en su código de autenticación.

Paso 206: el usuario introduce un código de autenticación de acuerdo con las instrucciones de la pantalla EC.

El usuario selecciona con la ayuda del ratón SE al menos un teclado gráfico para introducir su código de autenticación.

Paso 207: las coordenadas correspondientes al código de autenticación seleccionado por el usuario en el teclado gráfico se transfieren a la tarjeta inteligente CP.

Paso 208: en la tarjeta inteligente CP, las coordenadas del código de autenticación son comparadas con las registradas en la tarjeta inteligente CP.

Etapa 209a: En caso de una comparación positiva, la autoridad de autenticación AA recibe de la tarjeta inteligente CP una confirmación de la autenticación en forma de mensaje.

Tras enviar el mensaje, la tarjeta inteligente CP cripta (cifra) el contenido del mensaje con su clave pública.

Por su parte, el destinatario del mensaje cifrado, aquí la autoridad de autenticación AA desencripta (descifra) el

contenido con la ayuda de su clave privada.

Paso 209b: en caso de una comparación negativa, la operación vuelve a la etapa 207.

Es de esperar que después de una serie de comparaciones negativas, la tarjeta inteligente CP se bloquee.

Por ejemplo, cuando las coordenadas X e Y en el teclado gráfico corresponden a una imagen indexada "4".

Sólo la tarjeta CP sabe que la imagen indexada "4" puede corresponder a una representación numérica de la cifra 3, por ejemplo.

Sólo la tarjeta CP conoce la tabla de correspondencia que puede variar para cada transacción.

Cuando la tarjeta CP recibe las coordenadas del teclado gráfico y verifica que se corresponden bien con el código de autenticación, en el caso de una comparación positiva la tarjeta CP firma (cifra) el mensaje formando el resultado y envía a la atención de la autoridad de autenticación AA procesado del desafío por la función de autenticación y la envía al servidor.

Por su parte, el servidor verifica la firma (descifra), compara la respuesta al desafío y en caso de verificación positiva, autoriza la transacción ya que el titular es auténtico.

En caso de una comparación negativa, se puede mostrar el siguiente mensaje: "Autenticación denegada, le quedan dos intentos."

Si el usuario hace clic en "cancelar" se muestra un mensaje de confirmación con la siguiente redacción: "esta operación anulará su transacción, ¿está Ud. seguro de que desea cancelar o no", si el usuario selecciona la respuesta "sí", el usuario es redirigido a la página de la tienda correspondiente, si el usuario selecciona la respuesta "no", el usuario recibe la siguiente invitación por mensaje: "haga clic en Aceptar para intentar de nuevo la prueba de autenticación."

Además, la presente invención prevé un método de no-repudio de la transacción.

Esta opción permite generar un nuevo elemento visual que permite al usuario validar las informaciones financieras relativas a su compra. Las informaciones financieras relativas a su compra pueden ser el nombre del comerciante, la cantidad, la moneda, la orden de pedido.

Estas informaciones se muestran en forma gráfica para asegurarse de que no se pueden alterar de manera fraudulenta en lugar de la información que viaja por la red entre la tienda y la computadora con los riesgos antes mencionados.

El servicio de no-repudio de la transacción de acuerdo con la invención permite aquí detener el repudio a posteriori de ciertos elementos de la transacción (importe, moneda, fecha, etc.).

El mecanismo utiliza la autoridad de autenticación (AA) que efectúa aquí cálculos de certificados (o firma) en dichas informaciones asociadas a la transacción.

Por su parte, la tarjeta inteligente (CP) verifica los certificados correspondientes. El usuario debe conservar los elementos de la transacción y los certificados asociados para su utilización posterior en caso de litigio.

En la práctica, el mecanismo de no-repudio de acuerdo con la invención implementa una firma de la transacción (con la contraseña o el código PIN del cliente) a fin de autentificar dicho cliente y evitar un repudio de la compra así como un acuse de recibo firmado para protegerse contra el repudio de la recepción de la compra.

Por ejemplo (Figura 4), según el paso 300, la autoridad de autenticación almacena en un archivo de imagen las informaciones comerciales referentes a la transacción.

Podrá tratarse del importe de la transacción o de la moneda en que se realizó, la hora y/o la fecha en que se efectuó la referencia a la orden, etc.

Paso 301: la autoridad de autenticación AA envía información comercial a la tarjeta inteligente CP a través del puesto de tratamiento PT y el lector de tarjeta la tarjeta inteligente LC.

Paso 302: la tarjeta inteligente transmite los elementos gráficos que contienen la información comercial.

Paso 303: el puesto de tratamiento PT los muestra en la pantalla EC.

Paso 304: el usuario valida la información haciendo clic en el icono o en la representación gráfica correspondiente mostrada en la pantalla EC.

Paso 305: las coordenadas correspondientes son transferidas a la tarjeta inteligente CP.

Paso 306: en el seno de la tarjeta inteligente CP, las coordenadas transferidas por el puesto de tratamiento se comparan con las correspondientes a la información tal como se recibe en el paso 301.

Etapa 307a: en caso de comparación positiva, la autoridad de autenticación AA recibe una confirmación de la tarjeta inteligente CP mientras que en el paso 307b, en caso de comparación negativa la operación vuelve al paso 302.

Es de esperar que después de un número de comparaciones negativas, la transacción sea anulada.

También se puede prever que se muestre en la pantalla EC un elemento de anulación en el que el usuario pueda hacer clic para cancelar la transacción.

Así, el usuario tiene la posibilidad de confirmar la transacción.

Esto limita las impugnaciones en el momento de la entrega del producto solicitado.

REIVINDICACIONES

1. Procedimiento para asegurar una transacción realizada en línea por un cliente mediante una tarjeta de chip (CP), siendo capaz dicho cliente de utilizar un puesto de tratamiento (PT) adaptado para comunicarse en línea con una autoridad de autenticación (AA) y equipado con una interfaz hombre/máquina tal como una pantalla (CE), y un lector de tarjeta inteligente (LC), **caracterizado porque** comprende una prueba de proximidad adaptado para comunicar para verificar la presencia física del cliente cerca del puesto de tratamiento (PT) adaptado para comunicar en línea con la autoridad de autenticación (AA), una prueba de autenticación del titular de la tarjeta inteligente (CP) y una prueba de no-repudio de la transacción. La prueba de proximidad comprende la introducción de una información por el cliente coincidente con una información emitida por la tarjeta inteligente directamente o vía el lector de la tarjeta.

2. Procedimiento para asegurar una transacción de acuerdo con la reivindicación 1, caracterizado porque la prueba de autenticación comprende la introducción de un código secreto de identificación por el cliente y el control de dicho código por dicha tarjeta inteligente.

3. Procedimiento para asegurar una transacción de acuerdo con la reivindicación 1, caracterizado porque la prueba de autenticación comprende las siguientes etapas:

a) la carga en la tarjeta inteligente, de un archivo de imagen que tiene una pluralidad de elementos capaces de formar un teclado gráfico en la pantalla de la estación de procesamiento para la introducción de un código de acceso, cada elemento del teclado gráfico se identifica por las coordenadas correspondientes;

b) de la tarjeta inteligente, cargar el archivo de imagen en la estación de procesamiento para visualizar dicho teclado gráfico en dicha pantalla

c) hacer seleccionar al cliente al menos un elemento de dicho teclado gráfico para introducir dicho código de autenticación

d) transmitir a la tarjeta inteligente las coordenadas correspondientes del elemento del teclado gráfico seleccionado por el cliente

e) en la tarjeta inteligente, comparar las coordenadas del código de autenticación derivada de las coordenadas del elemento del teclado gráfico y los transmitidos desde el código de autenticación de la parte del cliente de la tarjeta inteligente;

f) en caso de una comparación positiva en el nivel de la tarjeta, cifrar un certificado que comprenda una palabra relacionada con el resultado de la comparación, un identificador, y un desafío vinculando el resultado de la transacción en curso, y enviar dicho certificado así cifrado a la autoridad de autenticación, y

g) la autoridad de autenticación, descifra el certificado enviado para verificar la autenticidad de la titular de la tarjeta, y caso de verificación positiva, permitir la transacción.

4. Procedimiento de acuerdo con la reivindicación 1, **caracterizado porque** la prueba de proximidad comprende las siguientes etapas:

i) equipar al lector de tarjetas inteligentes de medios de difusión de información visual y/o sonora bajo el control de la de la tarjeta de chip;

ii) hacer controlar por la tarjeta inteligente la transmisión de un conjunto seleccionado de informaciones visuales y/o sonoras;

iii) en respuesta a la transmisión del conjunto de la información, hacer accionar al cliente selectivamente la interfaz hombre/máquina del puesto de tratamiento para transmitir a destino de la tarjeta inteligente un juego de información en respuesta al juego de información transmitido por la tarjeta;

iv) en la tarjeta, se recibe el conjunto de información generada por el cliente y se compara con el juego de información juego generado por la tarjeta inteligente, y

v) en el caso de una comparación positiva, autorizar la transacción.

5. 4. Procedimiento de acuerdo con la reivindicación 1, **caracterizado porque** la prueba de no-repudio comprende las siguientes etapas:

l) a nivel de la autoridad de autenticación, almacenamiento en un fichero de imagen la información financiera relativa a la transacción;

II) la transmisión de dicho archivo de imagen asociado a la transacción con destino a la tarjeta inteligente a través del procesamiento posterior y el chip lector de tarjetas;

III) proviniendo de la tarjeta, cargarlo en dicha estación de procesamiento dicha imagen para mostrar en la pantalla;

IV) seleccionar por parte del cliente al menos una información financiera de dicho archivo de imagen así mostrado;

V) transmitir a la tarjeta inteligente las coordenadas correspondientes de dicha información financiera así seleccionada por el cliente;

VI) a nivel de la tarjeta inteligente, cifrar un mensaje que comprende al menos dicha información financiera de la transacción financiera así deducida; y enviar dicho mensaje así cifrado con destino a la autoridad de autenticación; y

VII) a nivel de la autoridad de autenticación, descifrar el mensaje así enviado, verificar la información financiera asociada y validar la transacción en caso de verificación positiva.

6. Sistema que comprende un puesto de tratamiento (PT) adaptado pata comunicar en línea con autoridad de autenticación (AA) y equipado con un interfaz hombre/máquina tal como una pantalla (EC), un lector de tarjetas inteligentes (CP), así como una tarjeta inteligente (CP), estando dicho sistema **caracterizado porque** está organizado para asegurar una transacción realizada en línea por un cliente poseedor de dicha tarjeta inteligente (CP) implementando un procedimiento según una de cualquiera de las reivindicaciones 1 a 4.

7. Programa de ordenador adaptado para su ejecución en un ordenador por etapas para realizar las etapas del procedimiento según una de las reivindicaciones 1 a 5.

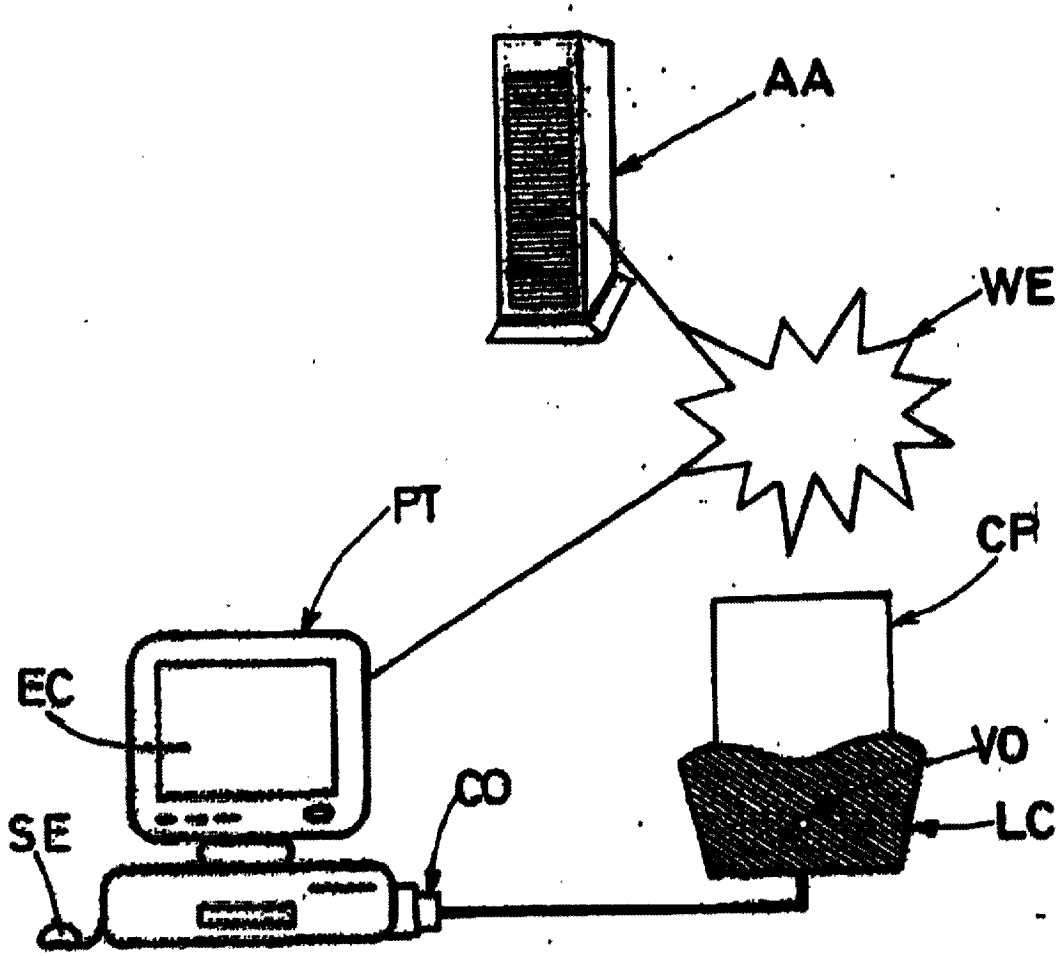

FIG.1

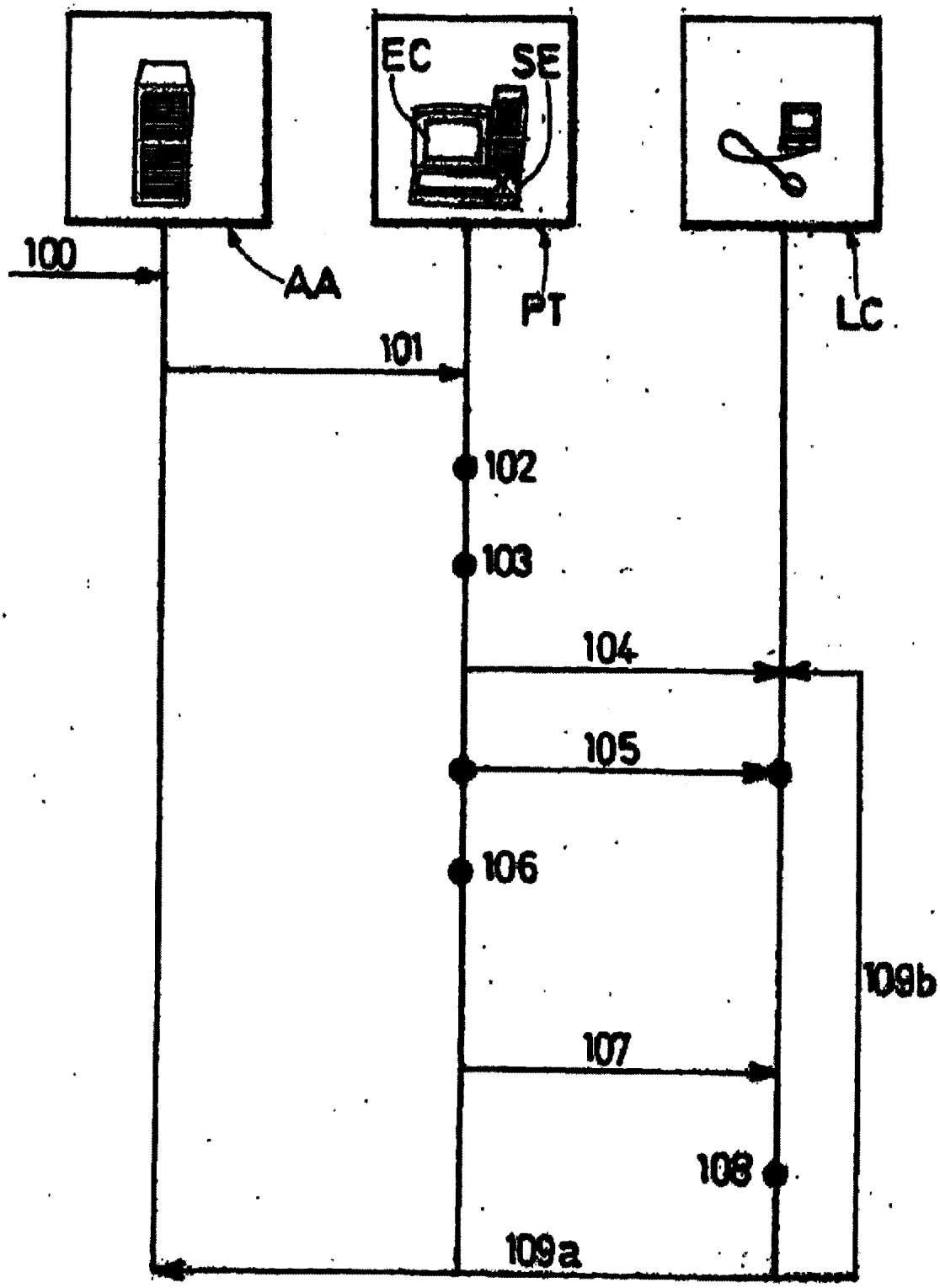

FIG.2

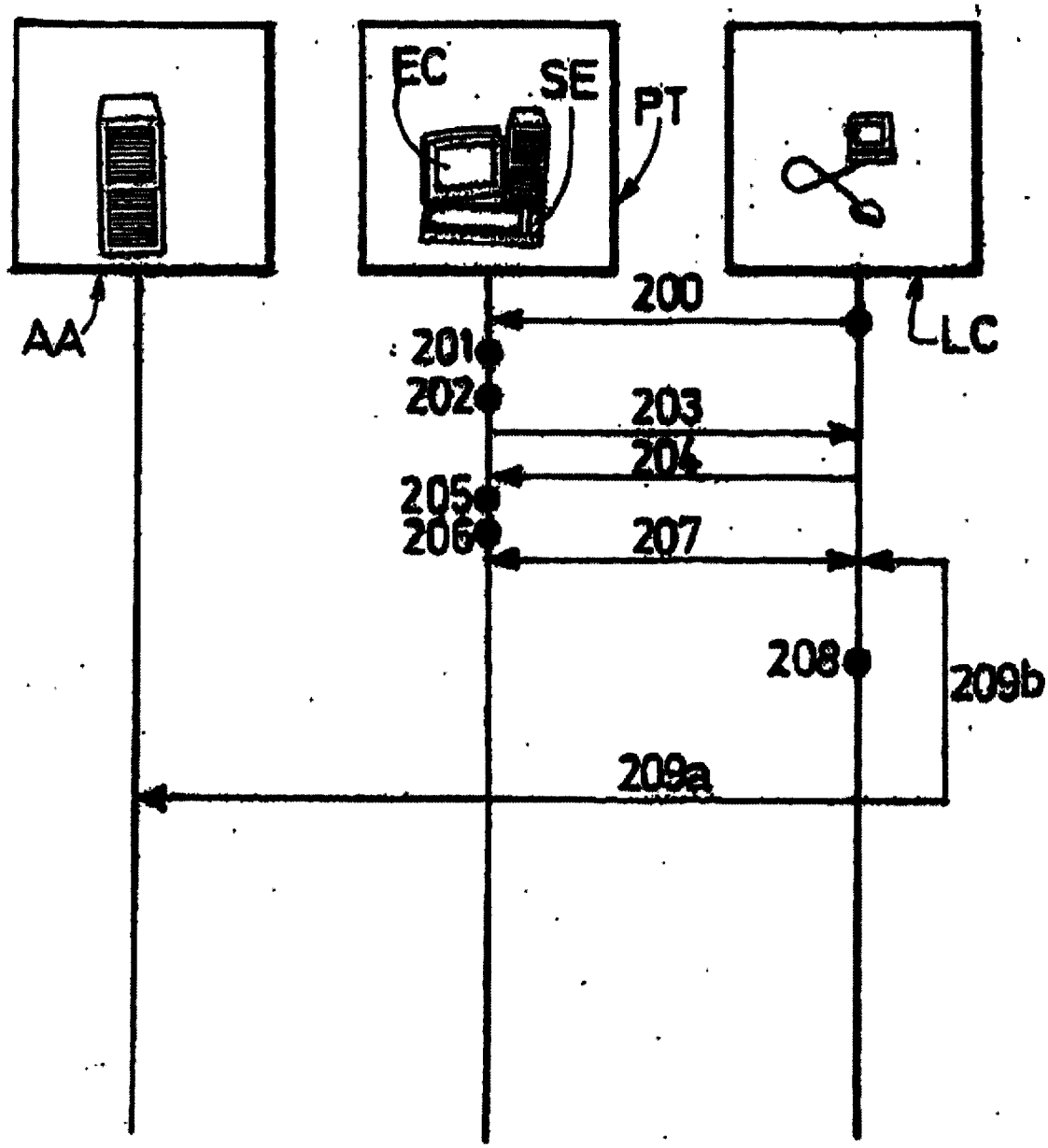

FIG.3

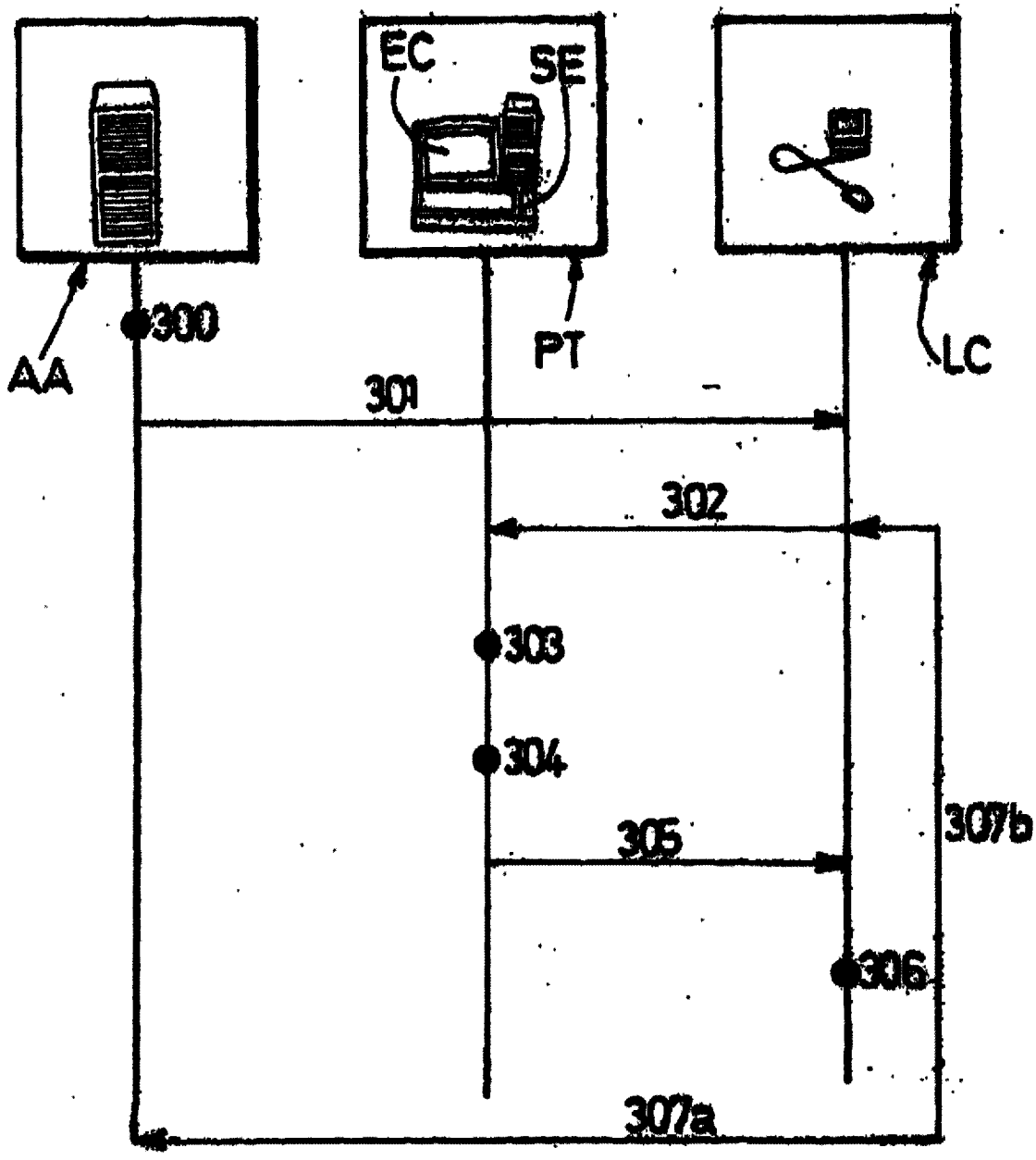

FIG.4