(19) OFICINA ESPAÑOLA DE PATENTES Y MARCAS

ESPAÑA

(11) Número de publicación: **2 428 402**

(51) Int. CI.:

G07B 17/00 (2006.01)

(12) TRADUCCIÓN DE PATENTE EUROPEA T3

(96) Fecha de presentación y número de la solicitud europea: **15.11.2001 E 01995530 (1)**

(97) Fecha y número de publicación de la concesión europea: **24.07.2013 EP 1337974**

(54) Título: **Procedimiento para proveer envíos postales de marcas de franqueo**

(30) Prioridad:

15.11.2000 DE 10056599

(45) Fecha de publicación y mención en BOPI de la traducción de la patente:
07.11.2013

(73) Titular/es:

DEUTSCHE POST AG (100.0%)
Charles-de-Gaulle-Strasse 20
53113 Bonn, DE

(72) Inventor/es:

LANG, JÜRGEN y
MEYER, BERND

(74) Agente/Representante:

CARPINTERO LÓPEZ, Mario

DESCRIPCIÓN

Procedimiento para proveer envíos postales de marcas de franqueo

La invención se refiere a un procedimiento para proveer envíos postales de marcas de franqueo, en el que un sistema de cliente carga un importe de tasa desde un centro de transmisión de valores mediante una línea de datos, controlando el sistema de cliente la impresión de marcas de franqueo en envíos postales y enviando el centro de transmisión de valores un paquete de datos al sistema de cliente.

Un procedimiento genérico se conoce por la solicitud internacional de patente WO 98 14907.

El documento EP0927963 indica un procedimiento para proveer envíos postales de marcas de franqueo, controlando el sistema de cliente una impresión de marcas de franqueo en envíos postales y enviando el centro de transmisión de valores un paquete de datos al sistema de cliente y comprobándose una validez de las marcas de franqueo en un centro de cartas mediante un análisis de datos contenidos en la marca de franqueo.

Otro procedimiento se conoce por la patente alemana DE 31 26 785 C2. En este procedimiento se produce una generación de una señal de recarga determinada para un franqueo de envíos postales en una zona separada de un centro de transmisión de valores explotado por una empresa de transporte de correos.

La solicitud alemana de patente no publicada 100 20 566.6/53 también se refiere a un procedimiento para proveer envíos postales de marcas de franqueo.

En este procedimiento, un sistema de cliente carga mediante una línea de datos desde un centro de transmisión de valores un importe de tasa en forma de un paquete de datos, que será usado por el sistema de cliente para la generación de marcas de franqueo. Este procedimiento se caracteriza porque en el sistema de cliente se generan datos que están cifrados de tal modo que el centro de transmisión de valores puede descifrarlos, porque los datos son enviados desde el sistema de cliente al centro de transmisión de valores y porque el centro de transmisión de valores descifra los datos y vuelve a cifrar a continuación los datos nuevamente con una clave que no conoce el sistema de cliente transmitiendo los datos así cifrados a continuación al sistema de cliente. Una forma de realización preferible de este procedimiento se caracteriza porque el cifrado en el sistema de cliente se realiza empleándose un número aleatorio, que sirve como clave de autentificación. Además, el procedimiento está caracterizado porque e número aleatorio se genera en un módulo de seguridad, al que un usuario del sistema de cliente no tiene acceso.

Puesto que los números aleatorios de este tipo que sirven de clave de autentificación desempeñan un papel importante respecto a la seguridad de manipulación del sistema global, es de gran importancia la calidad o “aleatoriedad” con la que se generan estos números aleatorios. En la práctica, de ello resulta la problemática que los módulos de seguridad, que están disponibles en gran número en los sistemas de cliente y que por razones económicas sólo ofrecen espacio para funcionalidades internas y algoritmos limitados, deben cumplir los requisitos estrictos de la calidad del número aleatorio.

En particular debe evitarse que personas no autorizadas conozcan el número aleatorio, puesto que por el conocimiento del número aleatorio sería posible generar marcas de franqueo que parecen ser válidas de forma abusiva sin pago, también sin el uso del módulo de seguridad.

La invención tiene el objetivo de realizar un procedimiento genérico de tal modo que se evite una generación abusiva de marcas de franqueo.

Según la invención, este objetivo se consigue porque el centro de transmisión de valores genera una clave y transmite la clave al sistema de cliente, porque en el sistema de cliente se generan datos que se cifran con la clave de tal modo que el centro de transmisión de valores puede descifrarlos, porque los datos son enviados desde el sistema de cliente al centro de transmisión de valores y porque el centro de transmisión de valores descifra los datos y cifra a continuación los datos nuevamente con una clave que el sistema de cliente no conoce, transmitiendo los datos así cifrados a continuación al sistema de cliente.

Para evitar un abuso gracias a la posible predictibilidad de números aleatorios de mala calidad que se forman en un módulo de seguridad, el número aleatorio se genera también de forma central en el centro de transmisión de valores para todos los módulos de seguridad en cada proceso de carga. En el marco de la comunicación de datos electrónica entre el centro de transmisión de valores y el módulo de seguridad correspondiente en el sistema de cliente, la clave se transmite de forma cifrada y con firma digital. La puesta a disposición de un número aleatorio de alta calidad puede garantizarse mejor en el centro de transmisión de valores central que en el módulo de seguridad en el sistema de cliente.

Un forma de realización especialmente ventajosa del procedimiento según la invención está caracterizada porque en el sistema de cliente se generan datos para la identificación y la autentificación así como para la acción deseada, que están cifrados de tal modo que el centro de transmisión de valores puede descifrarlos, porque los datos son enviados desde el sistema de cliente al centro de transmisión de valores y porque el centro de transmisión de valores descifra los datos y vuelve a cifrar a continuación los datos nuevamente con una clave que el sistema de

cliente no conoce, transmitiendo los datos así cifrados a continuación junto con otros datos cifrados que se añaden, pero que pueden ser descifrados por el sistema de cliente, al sistema de cliente.

Una forma de realización preferible del procedimiento según la invención está caracterizada porque el cifrado en el centro de transmisión de valores se realiza empleándose un número aleatorio.

Es recomendable que el número aleatorio se cifre junto con una clave de sesión emitida por el sistema de cliente y una clave pública del sistema de cliente. Además, el procedimiento está caracterizado porque el centro de transmisión de valores firma los datos con una clave privada.

Además, es ventajoso que el descifrado se realice en un módulo de seguridad en el sistema de cliente, al que el cliente no tiene acceso.

Otra forma de realización ventajosa del procedimiento está caracterizada porque el número aleatorio descifrado se almacena en el módulo de seguridad del sistema de cliente al que el cliente no tiene acceso.

El sistema de cliente está configurado preferiblemente de tal modo que no es capaz de descifrar por completo los datos enviados por el centro de transmisión de valores, pudiendo descifrar estos datos, no obstante, un centro de cartas en el que se comprueba el franqueo correcto de los envíos postales.

El centro de transmisión de valores puede estar configurado de distintas maneras. El concepto centro de transmisión de valores comprende tanto centros de transmisión de valores conocidos como nuevas formas de centros de transmisión de valores.

La invención se refiere en particular a aquellos centros de transmisión de valores mediante los cuales puede accederse directamente a una línea de comunicación de datos, como a internet o a servidores de datos conectadas con líneas telefónicas.

Una forma de realización ventajosa del procedimiento y una configuración preferible del centro de transmisión de valores están caracterizadas porque el cifrado en el centro de transmisión de valores se realiza empleándose un número aleatorio.

Es recomendable que el número aleatorio se genere en una zona asegurada del centro de transmisión de valores.

Una configuración preferible del sistema de cliente y del centro de transmisión de valores está caracterizada porque el número aleatorio se cifra con una clave de sesión emitida por el centro de transmisión de valores y una clave pública del módulo de seguridad del sistema de cliente.

Es recomendable que el centro de transmisión de valores firme los datos con una clave privada.

Una configuración preferible del sistema de cliente y del centro de transmisión de valores está caracterizada porque la clave privada está almacenada en la zona especialmente asegurada del centro de transmisión de valores.

Es recomendable que los datos se transmitan con cada requerimiento de un importe de tasa del sistema de cliente al centro de transmisión de valores.

Una forma de realización ventajosa del procedimiento, una configuración preferible del sistema de cliente y del centro de transmisión de valores están caracterizadas porque el centro de transmisión de valores identifica el sistema de cliente con ayuda de los datos transmitidos.

Es recomendable que el centro de transmisión de valores envíe los datos cifrados por el mismo al sistema de cliente.

Una configuración preferible del sistema de cliente y del centro de transmisión de valores está caracterizada porque los datos enviados por el centro de transmisión de valores al sistema de cliente presentan un primer componente que no puede ser descifrado por el sistema de cliente y porque los datos presentan además una segunda parte que puede ser descifrada por el sistema de cliente.

Es recomendable que la parte de datos que puede ser descifrada en el sistema de cliente contenga informaciones acerca de la identidad del sistema de cliente.

Es recomendable que la parte de datos que puede ser descifrada en el sistema de cliente contenga el número aleatorio formado en el centro de transmisión de valores.

Una configuración preferible del sistema de cliente y del centro de transmisión de valores está caracterizada porque la parte de datos que puede ser descifrada por el sistema de cliente contiene informaciones acerca del importe de tasa.

Es recomendable que un envío de datos desde el sistema de cliente al centro de transmisión de valores sólo se realice si en el sistema de cliente deba cargarse un importe que ascienda a una suma mínima.

Una forma de realización ventajosa del procedimiento, una configuración preferible del sistema de cliente y del centro de transmisión de valores están caracterizadas porque en el centro de transmisión de valores se forma un valor “hash”.

Es recomendable que el valor “hash” se forme teniéndose en cuenta indicaciones acerca de los datos del envío.

Una forma de realización ventajosa del procedimiento, una configuración preferible del sistema de cliente y del centro de transmisión de valores están caracterizadas porque el valor “hash” se forma teniéndose en cuenta un número aleatorio recibido y almacenado de forma intermedia.

Es recomendable que el valor “hash” se forme teniéndose en cuenta un número de identificación del proceso de carga.

Una forma de realización ventajosa del procedimiento, una configuración preferible del sistema de cliente y del centro de transmisión de valores están caracterizadas porque la marca de franqueo contiene datos lógicos.

Es recomendable que la marca de franqueo contenga informaciones acerca de datos del envío.

Una forma de realización ventajosa del procedimiento, una configuración preferible del sistema de cliente y del centro de transmisión de valores están caracterizadas porque los datos lógicos contienen informaciones acerca del número aleatorio cifrado.

Es recomendable que los datos lógicos contengan informaciones acerca del número de identificación de proceso de carga cifrado.

Una forma de realización ventajosa del procedimiento, una configuración preferible del sistema de cliente y del centro de transmisión de valores están caracterizadas porque los datos lógicos contienen informaciones acerca del valor “hash”.

Una configuración preferible del sistema de cliente y del centro de transmisión de valores está caracterizada porque la marca de franqueo contiene tanto las informaciones transmitidas por el centro de transmisión de valores como los datos introducidos por el generador de documentos.

Es recomendable realizar el procedimiento de tal modo o de configurar el sistema de cliente o el centro de transmisión de valores de tal modo que la marca de franqueo contenga un valor “hash”, que esté formado por una combinación de un valor transmitido por el centro de especificación y valores introducidos por el generador de documentos.

Una configuración preferible del sistema de cliente y del centro de transmisión de valores está caracterizada porque incluye las siguiente etapas de procedimiento: El sistema de cliente o el módulo de seguridad conectado con el sistema de cliente inicia un proceso de carga, transmitiendo la identidad del generador de documentos y/o del sistema de cliente empleado por él al centro de transmisión de valores.

Una forma de realización ventajosa del procedimiento, una configuración preferible del sistema de cliente y del centro de transmisión de valores están caracterizadas porque en el centro de transmisión de valores se forma un número aleatorio.

Es recomendable realizar el procedimiento de tal modo o de configurar el sistema de cliente o el centro de transmisión de valores de tal modo que el centro de transmisión de valores forme un número de identificación de carga y lo cifre junto con el número aleatorio generado por un lado de tal modo que sólo el centro de cartas pueda descifrarlo generando a continuación un número de identificación de carga.

Una configuración preferible del sistema de cliente y del centro de transmisión de valores está caracterizada porque el centro de transmisión de valores cifra el número de identificación de carga formado junto con el número aleatorio generado por otro lado de tal modo que sólo el módulo de seguridad en el sistema de cliente pueda descifrarlo.

Una configuración preferible del sistema de cliente y del centro de transmisión de valores está caracterizada porque en la zona especialmente asegurada del centro de transmisión de valores se forma un valor “hash” a partir del número de identificación de carga y de otros datos.

Es recomendable realizar el procedimiento de tal modo o de configurar el sistema de cliente o el centro de transmisión de valores de tal modo que la marca de franqueo se genere de tal modo que contenga el valor “hash”.

Una forma de realización ventajosa del procedimiento, una configuración preferible del sistema de cliente y del centro de transmisión de valores están caracterizadas porque la validez de las marcas de franqueo se comprueba en el centro de cartas.

Es recomendable realizar el procedimiento de tal modo o de configurar el sistema de cliente o el centro de transmisión de valores de tal modo que la comprobación en el centro de cartas se realice mediante un análisis de

datos contenidos en la marca de franqueo.

Una forma de realización ventajosa del procedimiento, una configuración preferible del sistema de cliente y del centro de transmisión de valores están caracterizadas porque la estación de comprobación forma un valor “hash” a partir de los datos contenidos en la marca de franqueo y comprueba si este valor “hash” coincide con un valor “hash” contenido en la marca de franqueo y registra en caso de no coincidencia la marca de franqueo como falsificada.

Otras ventajas, particularidades y variantes recomendables de la invención resultan de la descripción expuesta a continuación de un ejemplo de realización preferible con ayuda de los dibujos.

En los dibujos muestran:

La figura 1 un diagrama esquemático de un procedimiento según la invención;

La figura 2 el diagrama esquemático representado en la figura 1 resaltándose las partes que participan en un proceso de franqueo;

la figura 3 interfaces del sistema de franqueo representado en la figura 1 y en la figura 2 y

la figura 4 un diagrama esquemático de los mecanismos de seguridad empleados en el procedimiento.

El ejemplo de realización expuesto a continuación describe la invención con ayuda de un empleo previsto en el área de Deutsche Post AG. No obstante, por supuesto también es posible emplear la invención para el franqueo de otros documentos, en particular para un empleo en el área de otras empresas de correos.

La invención pone a disposición una posible nueva forma de franqueo, con la que los clientes pueden imprimir marcas de franqueo digitales en cartas, postales, etc., usando un PC convencional con impresora y software y dado el caso hardware adicional, así como un acceso a internet.

Un pago para compensar el valor de las marcas de franqueo impresas por el cliente puede realizarse de distintas formas. Por ejemplo, se reduce un saldo almacenado. Este saldo está almacenado preferiblemente de forma digital. Un almacenamiento digital se realiza por ejemplo en una tarjeta de cliente especial, una tarjeta bancaria estándar o en una memoria virtual, que se encuentra por ejemplo en el ordenador del usuario. Preferiblemente se carga el importe del saldo antes de realizarse impresiones de valores de franqueo. La carga del importe del saldo se realiza en una forma de realización especialmente preferible en un proceso de carga en cuenta.

En la figura 1 está representado un desarrollo esquemático de un franqueo según la invención de envíos postales. El procedimiento comprende varias etapas, que pueden completarse preferiblemente formando un ciclo completo. Si bien esto es especialmente recomendable, no es necesario. El número de ocho etapas representado a continuación también es ventajoso, aunque tampoco necesario.

1. Los clientes de la empresa de correos cargan con el PC (dado el caso, usando un software/hardware adicional, por ejemplo una tarjeta inteligente con microprocesador) un importe de un valor a través de internet.

2. Se realiza un cobro del importe de un valor, por ejemplo mediante cargo en la cuenta del cliente.

3. Del importe de un valor almacenado en las instalaciones del cliente en un monedero electrónico pueden imprimirse valores de franqueo válidos de cualquier importe mediante la impresora propia hasta que se haya agotado el saldo.

4. La marca de franqueo impresa por el cliente contiene datos legibles, así como un código de barras legible por máquina, que es usado por Deutsche Post para comprobar la validez.

5. El envío postal franqueado puede ser suministrado mediante las posibilidades puestas a disposición por Deutsche Post, por ejemplo buzones y sucursales de correos.

6. El código de barras indicado en la marca de franqueo, preferiblemente un código de barras 2D, es leído en el centro de cartas mediante una máquina para leer direcciones. Durante la producción se realiza una comprobación de la validez basada en la plausibilidad lógica.

7. Los datos leídos en la marca de franqueo se transmiten a un sistema subordinado, entre otras cosas para asegurar el pago.

8. Entre los importes de liquidación cargados y los envíos producidos se realiza una comparación para la detección de abusos.

En el procedimiento de franqueo participan preferiblemente varias partes, estando representada una distribución especialmente recomendable de las partes en la figura 2.

Las partes representadas son un cliente, un sistema de cliente y una empresa de correos.

El sistema de cliente comprende el hardware y el software empleado por el cliente para el franqueo por PC. El sistema de cliente regula en interacción con el cliente la carga y el almacenamiento de los importes de liquidación y la impresión de la marca de franqueo. Los requisitos de admisión regulan detalles del sistema de cliente.

La empresa de correos se encarga de la producción de los envíos y realiza el aseguramiento necesario del pago.

Un centro de transmisión de valores puede estar configurado de distintas formas:

- La explotación de un centro de transmisión de valores permite en combinación con la arquitectura de seguridad del franqueo por PC el empleo de procedimientos de cifrado simétricos en la marca de franqueo. De este modo se reduce considerablemente el tiempo de comprobación necesario de la validez de una marca de franqueo. Para el empleo de un procedimiento simétrico es necesaria la explotación de un centro de transmisión de valores y de los centros de cartas por parte de la misma organización. Una producción acelerada de este modo no es posible al usarse elementos de seguridad asimétricos en la marca de franqueo.

- La realización de todos los requisitos de seguridad necesarios, entre otras cosas para evitar manipulaciones internas y externas:
  A diferencia del sellado impreso por parte del remitente, la comunicación se realiza mediante el internet abierto y potencialmente inseguro. Los ataques a las vías de comunicación y los servidores de internet así como posibilidades internas de manipulación requieren mayores medidas de seguridad.
  Gracias a una gestión central, predeterminada por la empresa de correos de claves criptográficas es posible una mejora de la seguridad. Las claves relevantes en la producción en el centro de cartas pueden cambiarse en cualquier momento y pueden variarse las longitudes de las claves.

- Las comprobaciones para asegurar el pago pueden realizarse según un procedimiento de comprobación uniforme y en cualquier momento.

- Pueden comunicarse rápidamente nuevos abonados del contrato y cambios en los contratos a todos los sistemas necesarios de la empresa de correos.

Un aseguramiento del pago se realiza preferiblemente detectándose los componentes de las marcas de franqueo.

Para ello, una base de datos central entrega datos convenidos (datos del cliente/sistema de cliente) al sistema, que es necesario para la comprobación del aseguramiento correcto del pago.

El alcance de los datos a almacenar es definido por la empresa de correos, en particular el proveedor del servicio postal teniendo en cuenta las disposiciones legales, como la normativa de protección de datos de la empresa del servicio postal (PDSV). En principio pueden almacenarse según la misma todos los datos que son necesarios para la determinación correcta, la liquidación y la evaluación, así como para la comprobación de que las sobretasas postales son correctas. En principio son todas las informaciones acerca del envío, sin el nombre del destinatario y dado el caso el número de calle/número de apartado de correo del destinatario.

Un sistema subordinado comprueba si los importes del saldo contenidos en el sistema de cliente realmente se reducen restándose los importes de tasa que se imprimen como marcas de franqueo.

Para una detección de los datos convenidos está previsto preferiblemente un sistema de detección.

Los datos convenidos para el franqueo por PC con los datos maestros correspondientes de los clientes y del sistema de cliente (p.ej. ID del módulo de seguridad) se ponen a disposición y se actualizan mediante una base de datos que puede emplearse por ejemplo también para otros tipos de franqueo

Al usarse una base de datos de franqueo existente, se implemente por ejemplo una zona parcial separada para el franqueo por PC en la base de datos. Los datos se ponen a disposición en el centro de transmisión de valores y el sistema de aseguramiento del pago en el centro de cartas.

Es especialmente recomendable que el sistema contenga interfaces, que permitan un intercambio de datos e informaciones con otros sistemas.

En la figura 3 están representadas tres interfaces.

Las interfaces se denominan “Especificación”, “Marca de franqueo” y “Cobro”. Mediante una interfaz de liquidación se intercambian datos de liquidación entre el sistema de cliente y el proveedor de servicios de correos. Mediante la interfaz de liquidación pude cargarse por ejemplo un importe.

La interfaz de liquidación determina como están configuradas las marcas de franqueo para que puedan ser leídas y comprobadas en centros de cartas o centros de transporte.

En la implementación de interfaces representada en la figura 3, están separadas la interfaz de liquidación y la interfaz de cobro. No obstante, también es posible unir la interfaz de liquidación y la interfaz de cobro, por ejemplo

en caso de hacer la liquidación mediante tarjetas bancarias, tarjetas de crédito o dinero digital, en particular monedas digitales.

La interfaz de cobro determina como se realiza una liquidación de los importes de tasa transmitidos a través de la interfaz de liquidación. Los otros parámetros del procedimiento de franqueo no dependen de la interfaz de cobro elegida, aunque mediante una interfaz de cobro eficiente aumenta la eficiencia del sistema global. Las posibilidades de cobro preferibles son cargos en cuenta y facturas.

A continuación, se explicará como pueden conseguirse mediante requisitos de seguridad en cuanto al contenido, específicos según el usuario, los objetivos de seguridad del procedimiento de franqueo.

Este concepto está enfocado a la especificación técnica de los requisitos de seguridad del sistema. Procesos no relevantes para la seguridad, como el inicio, cierre y cambio de sesión de clientes, que no deben realizarse mediante el sistema de cliente, pueden determinarse por separado. Los procesos técnicos entre el sistema de cliente y el fabricante del sistema de cliente se determinan preferiblemente de tal modo que cumplan el estándar de seguridad aquí descrito.

Mediante el procedimiento según la invención se consiguen los objetivos de seguridad indicados a continuación.

- Se detectan como inválidas las marcas de fantasía o borrosas, es decir, marcas de franqueo que no contienen datos plausibles respecto al envío o que son ilegibles por otras razones.
- Pueden detectarse posteriormente duplicados, es decir, copias exactas de marcas de franqueo válidas con datos plausibles respecto al envío.
- Se impide un aumento del importe del saldo disponible para el sistema de cliente. También pueden detectarse posteriormente y pueden demostrarse con preferencia posteriormente con ayuda de una lista de protocolos cambios del importe del saldo.
- Se detectan usos no autorizados y no se cargan en la cuenta del usuario legítimo en caso de un uso no autorizado por parte de terceros.
- Entre ellos se encuentra el uso abusivo de datos electrónicos transmitidos legítimamente o de marcas de franqueo válidas, generadas legítimamente sin el conocimiento del usuario legítimo.
- Entre ellos se encuentra el uso abusivo del sistema de cliente mediante cambios del programa.
- Entre ellos se encuentra el uso no autorizado del sistema de cliente por parte de agentes de software ajenos a través de internet.
- Entre ellos se encuentra la averiguación de PINs mediante software de ataque (troyanos).
- Entre ellos se encuentran los ataques por sobrecarga (Denial-of-Service-Attacks, DoS), por ejemplo mediante la simulación de la identidad del centro de transmisión de valores o manipulación del proceso de carga de modo que el dinero se carga en la cuenta pero no se abre un saldo.
- Se impide la carga no autorizada de importes de liquidación se impide mediante medidas preventivas técnicas en el centro de transmisión de valores. Una carga no autorizada de importes de liquidación podría realizarse p.ej. mediante:
- Simulación de la identidad del centro de transmisión de valores de correos para aumentar el monedero propio en el sistema de cliente por parte del cliente.
- Simulación de un sistema de cliente certificado mediante un sistema de cliente manipulado o inventado, de modo que el autor del delito consigue conocimientos de secretos críticos para la seguridad del módulo de seguridad pudiendo realizar a continuación falsificaciones sin llamar la atención.
- Grabación en directo de la comunicación correcta entre un sistema de cliente y el centro de transmisión de valores y repetición de esta comunicación con fines abusivos (ataque por reproducción o replay attack).
- manipulación de la comunicación que tiene lugar entre el sistema de cliente y el centro de transmisión de valores en tiempo real (corrientes de datos entrantes y salientes en el sistema de cliente) de modo que el sistema de cliente parte de un importe cargado más elevado que el centro de transmisión de valores.
- Abuso de números de identificación de clientes de modo que terceros cargan importes de valor a cargo de un cliente.
- Gestión incompleta de una anulación.

Los dos primeros problemas de seguridad se resuelven sustancialmente mediante el concepto del sistema y mediante medidas en el sistema global, los últimos tres se resuelven preferiblemente mediante la implementación de software y hardware del módulo de seguridad.

A continuación, se describirán configuraciones preferibles de un hardware que aumente los estándares de seguridad.

- Propiedades básicas del hardware

1. Todos los cifrados, descifrados, cambios de cifrados, autorizaciones de firmas y procedimientos de comprobación criptográficos se realizan en zonas especialmente protegidas contra accesos no autorizados de un módulo de seguridad criptográfico en el sistema de cliente y/o en una zona asegurada del centro de transmisión de valores. Las claves correspondientes también están depositadas en zonas de seguridad de este tipo.

2. Los datos y secuencias relevantes para la seguridad (por ejemplo claves, programas) son protegidos contra cambios no autorizados y los datos secretos (por ejemplo claves, PINs) contra lectura no autorizada. Esto se garantiza preferiblemente mediante las siguientes medidas:

- El tipo de construcción del módulo de seguridad, eventualmente en cooperación con mecanismos de seguridad del software del módulo de seguridad,
- La carga de programas en los módulos de seguridad sólo durante la fabricación o el aseguramiento criptográfico del proceso de carga,
- El aseguramiento criptográfico de la carga de datos relevantes para la seguridad, en particular de claves criptográficas.
- Los datos secretos en los módulos de seguridad también deben estar protegidos contra la lectura mediante ataques que impliquen la destrucción del módulo.

a. La protección de datos y programas contra cambios o lectura en el módulo de seguridad debe ser tan elevada, que por unos costes justificables durante la vida útil del módulo no sean posibles ataques, debiendo valorarse si las ventajas resultantes compensan los costes necesarios para una defensa satisfactoria.

b. El módulo de seguridad no debe poder ejecutar funciones no deseadas.

- Se impiden funciones secundarias no deseadas y canales de datos adicionales, en particular interfaces, que transmitan informaciones de forma no deseada (side channels).
Gracias a la construcción del módulo de seguridad queda garantizado que un atacante no pueda leer mediante interfaces previstas para otros fines informaciones acerca de datos y claves que han de mantener secretos.
La existencia de side channels se comprueba mediante tests correspondientes. Posibilidades típicas que se comprueban son las siguientes:

1. Single Power Attack (SPA) y Differential Power Attack (DPA), que intentan deducir de cambios del consumo de corriente durante cálculos criptográficos si hay datos secretos.
2. Timing Attacs, que intentan deducir de la duración de los cálculos criptográficos si hay datos secretos.

Las propiedades preferibles del procesamiento de datos se indicarán a continuación:

- Control de secuencia

Es especialmente recomendable realizar un control de secuencia. Este puede realizarse por ejemplo mediante una máquina de estado, por ejemplo según el estándar FIPS PUB 140-1. De este modo queda garantizado que las secuencias de las transacciones especificadas y los datos relevantes para la seguridad del sistema usados durante la secuencia no puedan ser manipuladas.

Las instancias que participan, en particular el usuario, no deben ser engañadas por un módulo de seguridad respecto a las secuencias de las transacciones.

Si se ha realizado por ejemplo el proceso de carga de un importe de un valor en forma de varios procesos parciales con llamadas individuales del módulo de seguridad, el control de secuencia debe garantizar que estos procesos parciales sólo se realicen en el orden admisible.

Los datos de acceso que se usan para el control de secuencia son relevantes para la seguridad y son almacenados por lo tanto preferiblemente en una zona asegurada contra manipulaciones del módulo de seguridad.

- Integridad de los mensajes

1. Todas las informaciones relevantes para la seguridad en los mensajes están protegidas con procedimientos adecuados contra cambios no autorizados antes o durante la transmisión en los componentes del sistema.
2. Los cambios de informaciones relevantes para la seguridad se detectan durante la transmisión entre componentes del sistema de pago asistido por tarjetas inteligentes. Deben tener lugar las reacciones correspondientes a las violaciones de la integridad.
3. Se detecta la carga no autorizada de mensajes. También en el caso de mensajes recargados deben tener lugar las reacciones correspondientes.

El hecho de poder detectar cambios no autorizados así como la recarga de mensajes queda garantizado para los mensajes estándar del sistema mediante las definiciones del concepto del sistema. El software del módulo de seguridad debe garantizar que la detección se realice realmente y que tenga lugar la reacción correspondiente. Para mensajes específicos del fabricante relevantes para la seguridad (por ejemplo en el marco de la personalización del mantenimiento del módulo de seguridad) se definen y aplican mecanismos adecuados correspondientes.

Las informaciones relevantes para asegurar la integridad de los mensajes se almacenan preferiblemente en una zona asegurada contra manipulaciones del módulo de seguridad. Las informaciones de este tipo son en particular características de identificación y autenticidad, contadores de secuencias o importes de tasas.

- Mantenimiento del secreto de PINs y claves criptográficas

1. Aunque el PIN no debería transmitirse en forma de texto abierto salvo en las zonas aseguradas, se tolera preferiblemente la transmisión en texto abierto en el franqueo por PC para aumentar la facilidad de manejo del sistema global y el uso de componentes hardware existentes, no asegurados en el sistema de cliente (teclado, monitor). No obstante, han de reducirse a un mínimo los componentes locales del sistema, en los que los PINs se procesan o almacenan en texto abierto. No debe realizarse una transmisión no asegurada del PIN.
2. Las claves criptográficas no deben transmitirse nunca en texto abierto por vías electrónicas de transmisión en un entorno no asegurado. Si se usan o almacenan en componentes del sistema, deben estar protegidas contra una lectura y un cambio no autorizados.
3. Ningún componente del sistema debe ofrecer una posibilidad para la determinación de un PIN gracias a una búsqueda exhaustiva.

- Protocolización

1. En el sistema de cliente se protocolizan de forma interna todos los datos que se necesitan para la reconstrucción de las secuencias correspondientes. Además, se protocolizan también los casos de errores, que sugieren una sospecha de manipulación.
2. Los datos de protocolos almacenados deben estar protegidos contra cambios no autorizados y deben poderse transmitir de forma auténtica a una instancia que los evalúa.

- Procesamiento de otras aplicaciones
  Si en los módulos de seguridad se procesan al mismo tiempo otras aplicaciones, esto no debe influir en la seguridad del sistema de franqueo por PC.
  La seguridad de los datos puede aumentar gracias a las siguientes medidas:
- Borrado de datos secretos de memorias temporales
- Implementación segura de funciones específicas según el fabricante (p.ej. en el marco de la personalización); por ejemplo el uso de Triple-DES o de un procedimiento simétrico seguro para el cifrado de datos secretos de personalización, integración de claves en texto abierto en forma de secretos divididos (p.ej. mitades de claves) según el principio de los cuatro ojos.
- No deben existir funciones adicionales inseguras (por ejemplo cifrado o descifrado o firmas de datos a elegir libremente con claves del sistema); no debe ser posible un intercambio de funciones de claves.

Otros aspectos

- Además de los módulos de seguridad usados en los sistemas de cliente, también deben examinarse otros módulos de seguridad: En particular deben examinarse los módulos de seguridad de las distintas estaciones de certificación (CAs) en las instalaciones de los fabricantes de los módulos de seguridad.
- También debe examinarse la parte del PC del software del cliente respecto a sus tareas relevantes para la seguridad (p.ej. entrada de PIN).
- El fabricante de un sistema de cliente debe prever un procedimiento que garantice la transmisión asegurada del PIN de módulos de seguridad a los usuarios (por ejemplo envío de cartas con el PIN). Debe comprobarse la seguridad y el cumplimiento de un concepto de este tipo.
- Seguridad del entorno del fabricante, en particular integración de clave etc.; encargados de la seguridad, de una forma más general: admisión de las medidas de seguridad respecto a la organización de los fabricantes según un procedimiento definido. Concretamente:

Gestión de claves

1. Deben determinarse reglamentos para la distribución, administración y eventualmente para el cambio por turnos y para la sustitución de claves.
2. Las claves respecto a las cuales hay sospecha de riesgo ya no deben usarse en todo el sistema.

Las medidas preferibles en la fabricación y personalización de módulos de seguridad son las siguientes:

1. La fabricación y personalización (primera integración de claves secretas, eventualmente de datos específicos del usuario) de módulos de seguridad deben tener lugar en un entorno de producción que impida que

- haya riesgos para las claves durante la personalización,
- el proceso de personalización se realice de forma abusiva o no autorizada,
- se incorporen software o datos no autorizados,
- se roben módulos de seguridad.

2. Debe estar garantizado que en el sistema no puedan integrarse componentes no autorizados que realicen funciones relevantes para la seguridad.
3. Debe registrarse continuamente el desarrollo de la vida de todos los módulos de seguridad.

Explicación:
El registro del desarrollo de la vida de un módulo de seguridad comprende preferiblemente:

- datos de fabricación y personalización
- situación en cuanto a los lugares/tiempos
- reparación y mantenimiento,
- puesta fuera de servicio
- pérdida o robo de memorias de datos que contienen el módulo de seguridad, como archivos, llaves de hardware (dongle), criptografía, servidor o tarjetas inteligentes
- datos de fabricación y personalización
- integración de nuevas aplicaciones
- cambio de aplicaciones
- cambio de claves
- puesta fuera de servicio,
- pérdida o robo.

Arquitectura de seguridad

Para el franqueo por PC está prevista una arquitectura de seguridad básica, que reúne las ventajas de distintos conceptos existentes y que ofrece con medios sencillos una mayor medida de seguridad.

La arquitectura de seguridad comprende con preferencia sustancialmente tres unidades, que están representadas en una disposición preferible en la figura 4:

- Un centro de transmisión de valores en el que se conoce la identidad del cliente y de su sistema de cliente.
- Un módulo de seguridad que garantiza gracias al hardware/software que no puede ser manipulado por el cliente la seguridad en el sistema de cliente (p.ej. llave de hardware o tarjeta inteligente en soluciones offline o servidores equivalentes en soluciones online).
- Un centro de cartas en el que se comprueba la validez de las marcas de franqueo, o se detectan manipulaciones en el importe de un valor, así como en la marca de franqueo.

Las distintas etapas del procedimiento que se realizan en el centro de transmisión de valores, el sistema de cliente y el centro de cartas deben representarse a continuación en forma de un diagrama esquemático. El proceso de comunicación técnico exacto difiere no obstante de esta representación esquemática (p.ej. varias etapas de comunicación para obtener una transmisión aquí representada). En particular, se da por supuesto en esta representación que hay una comunicación confidencial e íntegra entre interlocutores identificados y autentificados de una comunicación.

Sistema de cliente

0. En el interior del centro de carga se genera una clave y se transmite a continuación al sistema de cliente. La transmisión de la clave se produce preferiblemente de forma cifrada y dado el caso con una firma digital. En particular, es recomendable que la clave esté en un sobre digital.

1. Desde el módulo de seguridad se transmite un número de identificación unívoco (ID del módulo de seguridad) del sistema de cliente al centro de transmisión de valores cifrado de tal modo que sólo el centro de transmisión de valores sea capaz de realizar un descifrado. En una forma de realización especialmente preferible, se cifra la

consulta con la clave pública del centro de transmisión de valores y se provee de una firma digital con la clave privada del módulo de seguridad. De este modo se evita que la consulta tenga la misma forma en cada carga de un importe de liquidación y pueda usarse para una carga abusiva de importes de liquidación (ataque de reproducción).

2. Las informaciones tratadas de forma criptográfica del sistema de cliente se transmiten al centro de transmisión de valores en el marco de la carga de un importe de liquidación. Ni el cliente ni terceros pueden descifrar estas informaciones.

En la práctica, se aplica el cifrado asimétrico con la clave pública del interlocutor de la comunicación (centro de transmisión de valores o módulo de seguridad).

En caso de la posibilidad de un intercambio previo de claves también es posible un cifrado simétrico.

Centro de transmisión de valores

3. En el centro de transmisión de valores se descifra entre otras cosas el número de identificación del módulo de seguridad (ID del módulo de seguridad).

4. Mediante consulta en el franqueo de la base de datos, el ID del módulo de seguridad se asigna a un cliente de Deutsche Post.

5. En el centro de transmisión de valores se genera un número aleatorio.

En el centro de transmisión de valores se forma un número de identificación de proceso de carga, que contiene las partes del ID del módulo de seguridad, la suma de un importe de liquidación, etc.

6. El número de identificación de carga se cifra, por un lado, junto con el número aleatorio generado de tal modo que el sistema de cliente no sea capaz de descifrarlo. En la práctica, el cifrado se realiza con una clave simétrica según TDES, que existe exclusivamente en el centro de transmisión de valores, así como en los centros de cartas. El uso del cifrado simétrico en este momento está justificado por el requerimiento de procedimientos rápidos de descifrado por la producción.

7. El número de identificación de carga se cifra, por otro lado, junto con el número aleatorio generado de tal modo que sólo el módulo de seguridad en el sistema de cliente sea capaz de descifrarlo.

8. Las parejas del número de identificación del proceso de carga y del número aleatorio cifradas de distintas formas se transmiten al sistema de cliente. Ni el cliente ni terceros pueden descifrar estas informaciones. Gracias a la administración única de la clave propia de correos, preferiblemente simétrica, en el centro de transmisión de valores y en los centros de cartas, la clave puede cambiarse en cualquier momento y las longitudes de las claves pueden cambiarse en caso de necesidad. De este modo queda garantizada de forma sencilla una elevada seguridad de manipulación.

Sistema de cliente

9. En el módulo de seguridad del sistema de cliente se descifra y almacena el número aleatorio, que estaba cifrado de tal modo que pudo descifrarlo el módulo de seguridad en el sistema de cliente.

10. En el marco de la realización de una marca de franqueo, el cliente registra las informaciones específicas del envío o los datos de envío (p.ej. porte, tipo de envío, etc.) que se transmiten al módulo de seguridad.

11. Dentro de la zona asegurada del centro de transmisión de valores se forma un valor “hash”, entre otras a partir de las siguientes informaciones

- extractos de los datos de envío (p.ej. porte, tipo de envío, fecha, código postal, etc.),
- el número aleatorio almacenado de forma intermedia (que se recibió en el marco de la carga de un importe de liquidación)
- y, dado el caso, el número de identificación del proceso de carga.

10. En la marca de franqueo se han adoptado entre otros los siguientes datos:

- Extractos de los datos de envío en texto abierto (p.ej. porte, tipo de envío, fecha, código postal, etc.),
- el número aleatorio cifrado y el número de identificación del proceso de carga cifrado del centro de transmisión de valores y
- el valor “hash” formado en el módulo de seguridad a partir de los datos de envío, el número aleatorio recibido y almacenado de forma intermedia y el número de identificación del proceso de carga.

Centro de cartas

11. En el centro de cartas se comprueban en primer lugar los datos de envío. Si los datos de envío adoptados en la marca de franqueo no coinciden con el envío, existe un franqueo erróneo, una marca de fantasía o borrosa. El envío ha de pasarse al aseguramiento del pago.

12. En el centro de cartas se descifran el número aleatorio y el número de identificación del proceso de carga que se han entregado en el marco del importe de liquidación al sistema de cliente. Para ello, en el centro de cartas se necesita sólo una única clave (simétrica). En caso de usarse claves individuales habría que usar, no obstante, en lugar de ello una pluralidad de claves.

13. En el centro de cartas se forma según el mismo procedimiento que en el módulo de seguridad un valor "hash" a partir de las siguientes informaciones:

- extractos de los datos de envío,
- el número aleatorio descifrado
- el número de identificación del proceso de carga descifrado.

14. En el centro de cartas se comparan el valor "hash" formado propiamente y el transmitido. Si coinciden los dos, el valor "hash" transmitido se ha formado con el mismo número aleatorio que también se ha transmitido al centro de transmisión de valores en el marco de la carga del importe de liquidación. Por consiguiente, se trata tanto de un importe de liquidación auténtico, válido como de datos de envío que se han dado a conocer al módulo de seguridad (comprobación de validez). Por el esfuerzo, el descifrado, la formación de un valor "hash" y la comparación de dos valores "hash" corresponden teóricamente al de una comprobación de una firma. Debido al descifrado simétrico se obtiene, no obstante, una ventaja en cuanto al tiempo en comparación con la comprobación de la firma.

15. Respecto a una comprobación por pares en el sistema subordinado pueden determinarse posteriormente desviaciones entre importes de liquidación cargados e importes de franqueo (comprobación respecto a duplicados de envíos, formación de saldos en el sistema subordinado).

La arquitectura de seguridad básica representada no comprende la administración asegurada por separado de los importes de liquidación (función de monedero), el aseguramiento de la comunicación entre el sistema de cliente y el centro de transmisión de valores, la identificación mutua de sistema de cliente y centro de transmisión de valores ni la inicialización para el comienzo de un servicio seguro de un nuevo sistema de cliente.

Ataques contra la arquitectura de seguridad

La arquitectura de seguridad descrita es segura frente a ataques por lo siguiente:

- Terceros no pueden usar la comunicación correcta grabada en directo en internet (copiada) entre un sistema de cliente y el centro de transmisión de valores para fines fraudulentos (ataques por reproducción).
- Terceros o clientes no pueden simular frente al centro de transmisión de valores el uso de un sistema de cliente correcto mediante un sistema de cliente manipulado. Cuando un tercero o un cliente simula la transmisión de un número aleatorio y de un ID de safe-box, que no se generaron en un módulo de seguridad, sino que han llegado a su conocimiento, la carga de los importes de liquidación falla por la identificación realizada por separada del cliente legítimo mediante nombre de usuario y contraseña o por el conocimiento de la clave privada del módulo de seguridad, que el cliente no debe conocer bajo ningún concepto. (Por lo tanto, el proceso de inicialización para la generación de claves en el módulo de seguridad y la certificación de la clave pública mediante el proveedor del sistema de cliente deben realizarse de forma adecuada)
- Terceros o clientes no pueden cargar con un centro de transmisión de valores simulado importes de liquidación válidos en un sistema de cliente. Cuando un tercero o un cliente simula la funcionalidad del centro de transmisión de valores, éste centro de transmisión de valores simulado no consigue generar un número de identificación de proceso de carga cifrado que pueda descifrarse correctamente en el centro de cartas. Además, no puede falsificarse el certificado de la clave pública del centro de transmisión de valores.
- Omitiendo el centro de transmisión de valores, los clientes no pueden generar una marca de franqueo cuyo número de identificación de proceso de carga esté cifrado de tal modo que pueda descifrarse válidamente en el centro de cartas.

Para aumentar la seguridad de datos, en particular durante la búsqueda, debe usarse un número elevado de números aleatorios para la formación de valores "hash".

● Por lo tanto, la longitud del número aleatorio es lo más grande posible y es preferiblemente al menos de 16 byte (128 bit). La arquitectura de seguridad empleada es superior a los procedimientos conocidos, gracias a la posibilidad de emplear claves específicas para el cliente, sin que sea necesario tener preparadas claves en estaciones previstas para el descifrado, en particular centros de cartas, Esta configuración ventajosa es una diferencia importante con los sistemas conocidos según el Information-Based Indicia Program(IBIP).

Ventajas de la arquitectura de seguridad

Las siguientes características caracterizan la arquitectura de seguridad descrita en comparación con el modelo IBIP de los EEUU:

- La seguridad propiamente dicha se garantiza en los sistemas de Deutsche Post (centro de transmisión de valores, centro de cartas, sistema de aseguramiento del pago), por lo que está completamente en el área de influencia del Deutsche Post.
- En la marca de franqueo no se aplican firmas, sino datos cifrados (de forma simétrica) técnicamente equivalentes e igual de seguros y valores “hash”. Para ello, en el caso más sencillo se usa sólo una clave simétrica, que está sólo en el área de influencia del Deutsche Post, por lo que es fácilmente intercambiable.
- En el centro de cartas es posible una comprobación de todas las características de franqueo (no sólo por muestreo).
- El concepto de seguridad está basado en un ciclo de comprobación sencillo, cerrado en sí, que concuerda con un sistema subordinado adaptado a ello.
- El sistema permite detectar duplicados que de otra forma apenas podrían determinarse.
- Con este procedimiento pueden detectarse con gran precisión las marcas de fantasía inválidas.
- Además de la comprobación de plausibilidad, en todas las marcas de franqueo puede realizarse una comprobación del número de identificación del proceso de carga en tiempo real.

Tipos de envío

Con el franqueo por PC pueden franquearse todos los productos del proveedor de servicio de envío, como por ejemplo “carta nacional” (incluidas prestaciones adicionales) y “Marketing Directo nacional” según una definición previa por parte del proveedor de servicios de envío.

También es posible un uso para otras formas de envío, como envíos de paquetes y envíos urgentes.

El importe de tasa máximo que puede cargarse mediante el centro de transmisión de valores se fija en un importe adecuado. El importe puede elegirse según las necesidades del cliente y la necesidad de seguridad del proveedor de servicios postales. Mientras que para un empleo en el campo de clientes privados es especialmente adecuado un importe de tasas de un máximo de varios centenares de DM, para los empleos en las instalaciones de clientes grandes están previstos importes de tasa sustancialmente más elevados. Un importe del orden de aproximadamente DM 500,- es adecuado tanto para hogares privados exigentes como para autónomos y pequeñas empresas. El valor almacenado en el monedero no debería superar desde el punto de vista de la ingeniería de sistemas el doble del importe de un valor.

Envíos franqueados de forma incorrecta

Cartas, sobres, etc. ya impresos, franqueados de forma incorrecta y no aptos para el transporte con una marca de franqueo válida se abonarán al cliente.

Mediante medidas adecuadas, por ejemplo mediante un sellado de los envíos que llegan al centro de cartas es posible determinar si un envío ya fue transportado. De este modo se impide que clientes reciban de vuelta por parte del destinatario envíos ya transportados y los presenten para el abono al proveedor de servicios postales, por ejemplo Deutsche Post AG.

La devolución a un punto central del proveedor de servicios de envío, por ejemplo de Deutsche Post, permite un alto grado de aseguramiento del pago mediante una comparación de los datos con importes de liquidación y el conocimiento de las razones de devolución más frecuentes. De este modo existe dado el caso la posibilidad de un reajuste mediante un cambio de los requisitos de introducción con el objetivo de reducir la cuota de devoluciones.

Valdez de valores de franqueo

Por razones relacionados con el aseguramiento del pago, los valores de liquidación comprados por el cliente tienen una validez de por ejemplo sólo 3 meses. Una advertencia correspondiente debe incluirse en el convenio acordado con el cliente. Cuando los valores de franqueo no se consumen en 3 meses, el sistema de cliente debe entrar en contacto con el centro de transmisión de valores para realizar nuevas marcas de franqueo. En este contacto, al igual que en una carga correcta de importes de liquidación, el importe restante de un importe de liquidación anterior se suma al importe de liquidación nuevamente emitido y se pone a disposición del cliente con un nuevo número de identificación del proceso de carga.

Tratamiento especial en la empresa

En principio, las marcas de franqueo pueden presentar cualquier forma, en la que pueden reproducirse las informaciones contenidas en las mismas. No obstante, es recomendable configurar las marcas de franqueo de tal modo que presenten al menos por zonas la forma de códigos de barras. En la solución del código de barras 2D representada y el aseguramiento del pago que resulta de ello, deben tenerse en cuenta las siguientes

particularidades en la producción:

Los envíos franqueados por PC pueden suministrarse mediante todas las posibilidades de suministro, también mediante el buzón.

Gracias a la fijación de requisitos de admisión para fabricantes de componentes del sistema de franqueo relevantes para las interfaces, en particular para fabricantes y/o explotadores de sistemas de cliente, aumenta aún más el cumplimiento de las medidas de seguridad descritas.

Normas, estándares y especificaciones de orden superior International Postage Meter Approval Requirements (IPMAR)

Preferiblemente se aplican tanto las normas de la versión más actual del documento International Postage Meter Approval Requirements (IPMAR), UPU S-30 como todas las normas y estándares a los que se remite en este documento. En la medida de lo posible, para el sistema de cliente es recomendable el cumplimiento de todos los requisitos allí indicados.

Digital Postage Marks: Applications, Security & Design En principio, se aplican tanto las prescripciones de la versión actual del documento Digital Postage Marks: Applications, Security & Design (UPU: Technical Standards Manual) como todas las normas y/o estándares a los que se remite en este documento. Para el sistema de cliente es recomendable el cumplimiento del contenido “normativo”, así como tener en cuenta en la mayor medida posible el contenido “informativo” de este documento.

Preferiblemente, también se aplicarán las regulaciones y disposiciones de la empresa de servicios de envíos.

Gracias a una admisión de sólo aquellos sistemas que cumplen tanto todas las disposiciones legales como todas las normas y estándares del proveedor de servicios de envíos, se garantiza la seguridad de los datos y al mismo tiempo la fiabilidad del sistema y su facilidad de manejo.

Otras leyes, reglamentos, directivas, prescripciones, normas y estándares

En principio, se aplican todas las leyes, reglamentos, directivas, prescripciones, normas y estándares de la versión respectivamente válida, que han de tenerse en cuenta para el desarrollo y el servicio de un sistema de cliente técnico en la realización concreta.

Interoperabilidad de la ingeniería de sistemas

La interoperabilidad de la ingeniería de sistemas se refiere a la capacidad de funcionamiento de las interfaces del sistema de cliente o al cumplimiento de las prescripciones especificadas en las descripciones de las interfaces.

Interfaz importe de liquidación vía de comunicación, protocolos

La comunicación a través de la interfaz importe de liquidación se realiza preferiblemente mediante el internet público basándose en los protocolos TCP/IP y HTTP. Opcionalmente, el intercambio de datos puede realizarse de forma cifrada por HTTP mediante SSL (https). Aquí está representado el proceso teórico de una transmisión necesaria.

El intercambio de datos se realiza preferiblemente, a ser posible, mediante archivos codificados por HTML y XML. Los contenidos en forma de textos y gráficos de las páginas HTML deben representarse en el sistema de cliente.

Es recomendable recurrir en las páginas de comunicación a una versión HTML comprobada en la práctica y de renunciar al uso de marcos (frames), objetos incrustados (applets, ActiveX etc.) y dado el caso GIFs animados.

Inicio de sesión para la carga de un importe de liquidación (primera transmisión del módulo de seguridad al centro de transmisión de valores)

En el marco de la primera transmisión del módulo de seguridad al centro de transmisión de valores, el certificado del módulo de seguridad, así como un indicador de acción A se transmiten de forma no cifrada y sin firma.

Acuse de recibo del inicio de sesión (primera respuesta del centro de transmisión de valores al módulo de seguridad)

El acuse de recibo del centro de transmisión de valores contiene el certificado propio del centro de transmisión de valores, una clave de sesión cifrada y la firma digital de la clave de sesión cifrada.

Segunda transmisión del módulo de seguridad al centro de transmisión de valores

En el marco de esta transmisión, el módulo de seguridad envía la clave de sesión nuevamente cifrada y el juego de datos cifrado con datos de uso (suma de un importe de liquidación previamente cargado, valor restante del importe de liquidación actual, registro ascendente de todos los importes de liquidación, último número de identificación del proceso de carga) al centro de transmisión de valores (todo cifrado de forma asimétrica con la clave pública del centro de transmisión de valores). Al mismo tiempo, el módulo de seguridad envía la firma digital de estos datos

cifrados al centro de transmisión de valores. Al mismo tiempo, el sistema de cliente puede enviar otros protocolos de uso o perfiles de uso no cifrados y no firmados al centro de transmisión de valores.

Es recomendable que los datos de uso se registren en un protocolo de uso y que el protocolo de uso y/o las entradas allí anotadas sean provistos de una firma digital.

Segunda respuesta del centro de transmisión de valores al módulo de seguridad

El centro de transmisión de valores transmite el número aleatorio cifrado de forma simétrica y el número de identificación del proceso de carga cifrado de forma simétrica al módulo de seguridad. Además, el centro de transmisión de valores transmite el número de identificación del proceso de carga formado con la clave pública del módulo de seguridad, el número aleatorio generado, las informaciones de login para el módulo de seguridad, así como una nueva clave de sesión al módulo de seguridad. Además, todos los datos transmitidos son provistos de una firma digital.

Tercera transmisión del módulo de seguridad al centro de transmisión de valores

En el marco de la tercera transmisión, el módulo de seguridad transmite la nueva clave de sesión, el nuevo número de identificación del proceso de carga junto con los datos de uso para la confirmación de la comunicación correcta, todo de forma cifrada y provisto de una firma digital al centro de transmisión de valores.

Tercera respuesta del centro de transmisión de valores al módulo de seguridad

En la tercera respuesta, el centro de transmisión de valores confirma el éxito de la transmisión sin la aplicación de procedimientos criptográficos.

Desinstalación

El cliente debe tener la posibilidad de desinstalar el sistema de cliente.

La descripción técnica detallada de la interfaz importe de liquidación se realiza con la concepción del centro de transmisión de valores propiedad de la empresa de correos.

Protocolo de uso y perfil de uso

En el sistema de cliente debe generarse en el marco de cada generación de una marca de franqueo una entrada en el protocolo, que debería contener todos los datos de la marca de franqueo correspondiente, provistos de una firma digital. Además debería registrarse en el protocolo cada estado de error del módulo de seguridad de tal modo que se note el borrado manual de la entrada en la comprobación.

El perfil de uso contiene un resumen tratado de los datos de uso desde la última comunicación con el centro de transmisión de valores.

Cuando un sistema de cliente está dividido en un componente que se encuentra en las instalaciones del cliente y un componente central (que se encuentra p.ej. en internet), el perfil de uso debería llevarse preferiblemente en el componente central.

Interfaz marca de franqueo componentes y realizaciones

El sistema de cliente debe ser capaz de generar marcas de franqueo por PC, que correspondan exactamente a las especificaciones de Deutsche Post o al marco de los estándares CEN y UPU habituales.

Las marcas de franqueo por PC están formadas preferiblemente por los siguientes tres elementos:

- Un ortocódigo, código de barras o código matricial bidimensional, en el que están representadas las informaciones específicas del envío de forma legible por máquina. (Objetivo: automatización en la producción y aseguramiento del pago de Deutsche Post.)
- Texto en abierto, que reproduce partes importantes de la información del ortocódigo de forma legible. (Objetivo: posibilidad de control para el cliente, así como en la producción y el aseguramiento de pago del Deutsche Post.)
- Una marca que caracteriza el proveedor de los servicios de envío, por ejemplo Deutsche Post, como por ejemplo un cuerno postal.

Especificación del contenido de datos

Es recomendable que el ortocódigo y el texto abierto de la marca de franqueo por PC contengan las siguientes informaciones:

		En el código de barras	En texto abierto	Observación
1	Empresa de correos (Licensing Post Identifier)	Sí	No	
2	Tipo de franqueo (Licensing Plate Type)	Sí	No	
3	Versión y versión de precios/productos	Sí	No	
4	Número de licencia del Safe-Box-ID (PSD Identifier)	Sí	Sí	En el texto abierto: los primeros 5 byte del Safe-Box-ID en representación hexadecimal
5	Nº correlativo del envío (Message Identifier)	Sí	No	Respecto al Safe-Box
6	Indicador de fase de clave	Sí	No	
7	Cadena criptográfica	Sí	No	
8	Clave de producto	Sí	No	
9	Pago	Sí	Sí	Texto abierto en ASCII
10	Fecha de franqueo	Sí	Sí	Texto abierto en ASCII
11	Código postal del destinatario	Sí	No	
12	Calle/apartado de correo del destinatario	Sí	No	Las primeras y últimas tres posiciones de la dirección
13	Valor “hash” truncado	Sí	No	SHA-1

Tabla: Contenido de la marca de franqueo por PC

Aquí sólo se describe el contenido de la marca de franqueo. Las prescripciones del proveedor de servicios de envío para el contenido de las indicaciones de la dirección mantienen su validez sin cambios.

Especificación de la realización física en papel (layout)

La marca de franqueo está fijada de forma ventajosa en el campo para la dirección, alineada a la izquierda, por encima de la dirección en el envío.

El campo para la dirección se especifica en la versión respectivamente válida de las normas del proveedor de servicios de envío. En particular son posibles los siguientes franqueos:

- Impresión en el sobre de la carta
- impresión en etiquetas adhesivas o
- uso de sobres con ventana, de modo que la impresión en la carta pueda verse completamente a través de la ventana.

Preferiblemente, para los distintos elementos de la marca de franqueo es válido:

- Se usa en primer lugar el ortocódigo del tipo Data Matrix, cuyos puntos de matriz deberían presentar una longitud de canto de al menos 0,5 milímetros
  Respecto a los requisitos para la técnica de lectura, debería aplicarse preferiblemente un código de barras 2D en forma de la Data Matrix con un tamaño mínimo de píxeles de 0,5. Una opción dado el caso recomendable es reducir el tamaño de píxel a 0,3 mm.
  En un tamaño de representación de 0,5 mm por píxel, resulta una longitud de canto de todo el código de barras de aprox. 18 a 20 mm, si todos los datos se reciben de la forma descrita. Si se consigue leer códigos de barras con un tamaño de píxel de 0,3 mm en el ALM, la longitud de canto puede reducirse a aprox. 13 mm.
  Es posible una ampliación posterior de las especificaciones al uso de otro código de barras (p.ej. Aztec) con los mismos contenidos de datos.

Una forma de realización preferible del layout y del posicionamiento de los distintos elementos de la marca de franqueo está representada a continuación a título de ejemplo en la figura 5.

La magnitud “más crítica” es la altura de la ventana representada de un sobre de ventana con un tamaño de 45 mm x 90 mm. Aquí está representado un código de Data Matrix con una longitud de canto de aprox. 13 mm, que al usarse los campos de datos propuestos sólo es posible con una resolución de píxeles de 0,3 mm. Un código con una longitud de canto de 24 mm no deja suficiente espacio para indicaciones relacionadas con la dirección con la altura disponible.

Calidad de impresión y legibilidad

El responsable de la impresión impecable de la marca de franqueo es el fabricante del sistema de cliente en el marco del procedimiento de admisión, así como el cliente en el servicio posterior. Esto deberá indicarse al cliente mediante advertencias adecuadas en el manual de usuario y en un sistema de ayuda. En particular, esto es válido para la adhesión limpia de etiquetas debiendo impedirse también que se desplacen (partes) de la marca de franqueo quedando fuera de la zona visible de los sobres con ventana.

La legibilidad por máquina de las marcas de franqueo depende de la resolución de impresión usada y del contraste. Si deben aplicarse en lugar de negro también otros colores, debe contarse con un menor coeficiente de lectura. Hay que partir de que el coeficiente de lectura requerido con una resolución de 300 dpi (“dots per inch”) en la impresora puede garantizarse con un elevado contraste de la impresión. Esto corresponde a aproximadamente 120 elementos de imagen por centímetro.

Impresiones de prueba

El sistema de cliente debe ser capaz de producir marcas de franqueo que en su realización y tamaño correspondan a marcas de franqueo válidas, aunque no estén previstas para el envío, sirviendo en cambio para impresiones de control y el ajuste fino de la impresora.

El sistema de cliente está configurado preferiblemente de tal modo que las impresiones de prueba se distingan de una forma que puede ser detectada por la empresa de envíos de las marcas de franqueo reales. Para ello, se aplica por ejemplo en el centro de la marca de franqueo la inscripción “MUESTRA – no enviar”. Al menos dos terceras partes de los códigos de barras deben ocultarse mediante la inscripción o de otro modo.

Además de las marcas de franqueo auténticas (pagadas), no deben hacerse impresiones cero con excepción de las impresiones de prueba que se marcan de forma separada.

Requisitos del sistema de cliente; sistema base; resumen y funcionalidad:

El sistema base sirve como elemento de unión entre los otros componentes del franqueo por PC, es decir, el centro de transmisión de valores, el módulo de seguridad; la impresora y el cliente. Está formado por uno o varios sistemas de ordenadores, por ejemplo PCs, que dado el caso también pueden estar conectados entre sí formando una red.

El sistema base garantiza también el uso confortable del sistema global por parte del cliente.

Requisitos de la estructura y la seguridad:

El sistema base dispone preferiblemente de cuatro interfaces:

1. Mediante la interfaz importe de liquidación descrita se realiza la comunicación con el centro de transmisión de valores.

2. Mediante una interfaz con el módulo de seguridad se intercambian todas las informaciones que deben indicarse al módulo de seguridad (importe de liquidación o número de identificación del proceso de carga, datos específicos del envío respecto a franqueos individuales). Además, se intercambian mediante estas interfaces todos los datos con el módulo de seguridad (datos procesados de forma criptográfica).

3. La impresora se controla mediante una interfaz con la misma.

4. Mediante una interfaz para el usuario o cliente (Graphical User Interface, GUI), éste debe poder iniciar todos los procesos relevantes en interacción con la mayor ergonomía posible.

En el sistema base deberían almacenarse y procesarse además los siguientes datos:

- Ajustes/datos específicos del usuario,
- protocolos de uso y perfiles de uso detallados,
- al usar SSL: certificados intercambiables, con los que puede verificarse la validez de los certificados SSL y
- todas las informaciones relevantes acerca de los productos y precios del proveedor de servicios de envío.

Alcance de funciones y secuencias

El sistema base soporta preferiblemente las siguientes secuencias:

- Primera instalación con ayuda del usuario,
- identificación del usuario, en particular frente al módulo de seguridad; dado el caso con autorizaciones diferentes para la carga de importes de liquidación y la realización de marcas de franqueo,
- dado el caso, la administración de varios usuarios,
- apoyo para el usuario al cargar importes de liquidación (aquí apoyo para la reproducción de informaciones que son enviadas desde el centro de transmisión de valores en forma de archivos codificados por HTML),
- apoyo del usuario al surgir problemas durante la carga de importes de liquidación,
- administración del importe de un valor transparente para el usuario (resumen de la cuenta),
- administración de protocolo de usos, tratamiento de perfiles de uso y transmisión de protocolos o perfiles de uso,
- apoyo del usuario al generar e imprimir la marca de franqueo (representación de una muestra de la marca de franqueo a imprimir en la pantalla – WYSIWYG),
- cálculo del pago asegurado por plausibilidad según la información del servicio al cliente de Deutsche Post,
- sistema electrónico de ayuda,
- actualización automática de las informaciones relevantes acerca de los productos y precios de Deutsche Post en caso de cambios, así como información al cliente de la actualización que se realiza y termina,
- se impide técnicamente la impresión repetida de una sola marca de franqueo y
- desinstalación del sistema de cliente.

Módulo de seguridad

Tarea y nivel de seguridad

El módulo de seguridad garantiza como “módulo criptográfico” en el sentido de FIPS PUB 140, Security Requirements for Cryptographic Modules la seguridad propiamente dicha del sistema de cliente. Está formado por hardware, software, firmware o una combinación de éstos y alberga la lógica criptográfica y los procesos criptográficos, es decir, la administración y aplicación de procedimientos criptográficos, así como el almacenamiento del importe de valor asegurado contra manipulaciones. Los requisitos que debe cumplir el módulo de seguridad

- se definen respecto al estándar de seguridad mediante normas adecuadas, como por ejemplo FIPS PUB 140 y
- respecto al cumplimiento de estándares postales definidos mediante la publicación UPU “International Postage Meter Approval Requirements (IPMAR) basada en FIPS PUB 140.

Para la introducción y el servicio en un sistema de cliente debe certificarse correspondientemente un módulo de seguridad como módulo criptográfico según FIPS PUB 140, preferiblemente según el nivel de seguridad 3 (Security Level 3) en el marco del procedimiento de introducción.

Procesos del módulo de seguridad

Además de las operaciones habituales, para la inicialización y la comunicación con el centro de transmisión de valores y la desactivación el módulo de seguridad debería soportar preferiblemente sustancialmente los siguientes procesos que se describirán más detalladamente en la parte final del anexo Descripción técnica del sistema de cliente:

- generación de clave
- emisión de la clave pública
- almacenamiento del certificado
- generación de la firma
- comprobación de la firma
- comprobación del certificado
- almacenamiento temporal del certificado
- cifrado asimétrico
- descifrado asimétrico
- generación del número aleatorio
- almacenamiento de una clave de sesión
- almacenamiento de dos números de identificación de un proceso de carga
- almacenamiento del valor de registro actual de los importes de liquidación
- almacenamiento del valor de registro ascendente
- identificación del usuario
- emisión del estado de la validez de los importes de liquidación
- emisión del estado del valor de registro de los importes de liquidación

- formación “hash” de los datos específicos del envío
- deducción de los valores del registro de los importes de liquidación cargados
- protocolización de errores
- autocomprobación
- desactivación

Impresiones de prueba

El módulo de seguridad no se usa en la impresión de prueba, por lo que tampoco se establece contacto con el mismo.

Impresora

Según las especificaciones del fabricante del sistema de cliente, la impresora puede ser una impresora estándar corriente en el mercado o una impresora especial.

La mayor parte de las impresoras láser y de chorro de tinta debería ser apropiada en principio para el franqueo por PC. Deberían recomendarse impresoras con una resolución de al menos 300 dpi (dots per inch).

Procesos internos del sistema de cliente

Secuencia para la generación de marcas de franqueo. Mediante el sistema de cliente, el cliente realiza los siguientes procesos parciales durante la generación de marcas de franqueo:

- Establecimiento de la conexión con el módulo de seguridad: Mediante el sistema base se establece una conexión con el módulo de seguridad.
- Identificación del usuario: El usuario se identifica con contraseña/PIN personalmente en el módulo de seguridad y lo activa de este modo.
- Entrada de las informaciones especificas del envío: Con apoyo del sistema de cliente, el cliente introduce las informaciones específicas del envío necesarias en el sistema base, que transmite los datos importantes al módulo de seguridad.
- Generación de la marca de franqueo: El sistema base genera una marca de franqueo a partir de los datos específicos del envío y los datos procesados de forma criptográfica del módulo de seguridad.
- Protocolización de la realización de marcas de franqueo: Cada retransmisión realizada con éxito se registra en un protocolo de uso del sistema base. Al dividirse el sistema de cliente en un componente local en las instalaciones de cliente y un componente central (p.ej. en internet), el protocolo de uso debe llevarse en el componente central.
- Interrupción de la comunicación: Cuando se han realizado todas las marcas de franqueo requeridas, se interrumpe la comunicación. Al volver a realizar marcas de franqueo, debe realizarse nuevamente la identificación del usuario de la forma anteriormente descrita.
- Impresiones de prueba: Como alternativa a este procedimiento es posible dejar avanzar la guía del usuario hasta que pueda mostrarse en la pantalla una muestra de una marca de franqueo (WYSIWYG) y hasta que pueda imprimirse una impresión de prueba (no válida). Es en una fase posterior cuando se realizará el proceso anteriormente indicado de la integración del módulo de seguridad.

El uso del sistema técnico va acompañado de medidas organizativas adecuadas, de modo que un envío múltiple técnicamente registrable de una marca de franqueo se considera también una infracción contra las condiciones comerciales del remitente.

Además, es ventajoso prever parámetros técnicos adecuados para la impresión de las marcas de franqueo, en particular respecto a la calidad de la impresión, para que puedan registrarse mejor las marcas de franqueo en dispositivos automáticos de detección.

La comprobación de los sistemas puede estar basada en sistemas de aseguramiento de la calidad adecuados, en particular según las normas ISO 9001 y siguientes.

Lista de signos de referencia:

BZ Centro de cartas
KS Sistema de cliente
LZ Centro de carga

REIVINDICACIONES

1. Procedimiento para proveer envíos postales de marcas de franqueo, en el que un sistema de cliente carga un importe de tasa desde un centro de transmisión de valores mediante una línea de datos, controlando el sistema de cliente la impresión de marcas de franqueo en envíos postales y enviando el centro de transmisión de valores un paquete de datos al sistema de cliente y generando el centro de transmisión de valores una clave y transmitiendo la clave al sistema de cliente, y porque en el sistema de cliente se generan datos que son cifrados con la clave de tal modo que el centro de transmisión de valores puede descifrarlos, y porque los datos son enviados desde el sistema de cliente al centro de transmisión de valores, descifrando el centro de transmisión de valores los datos y generando el centro de transmisión de valores un número aleatorio, **caracterizado porque** en el centro de transmisión de valores se forma un valor “hash”, cifrando el centro de transmisión de valores los datos teniendo en cuenta el número aleatorio así como una clave que el sistema de cliente no conoce como una clave que conoce el módulo de seguridad del sistema de cliente y transmitiendo los datos así cifrados a continuación al sistema de cliente y porque se comprueba una validez de las marcas de franqueo en un centro de cartas mediante un análisis de los datos contenidos en la marca de franqueo, formando una estación de comprobación un valor “hash” a partir de los datos contenidos en la marca de franqueo y comprobando la misma si este valor “hash” coincide con un valor “hash” contenido en la marca de franqueo y registrando la misma la marca de franqueo como falsificada en caso de que no coincidan.

2. Procedimiento según la reivindicación 1, **caracterizado porque** el número aleatorio se genera en una zona asegurada del centro de transmisión de valores.

3. Procedimiento según una o las dos reivindicaciones 2 o 3, **caracterizado porque** el número aleatorio se cifra con una clave de sesión y una clave pública.

4. Procedimiento según una o varias de las reivindicaciones anteriores, **caracterizado porque** el centro de transmisión de valores firma los datos con una clave privada.

5. Procedimiento según la reivindicación 4, **caracterizado porque** la clave privada está almacenada en la zona especialmente asegurada del centro de transmisión de valores.

6. Procedimiento según una o varias de las reivindicaciones anteriores, **caracterizado porque** los datos se transmiten con cada requerimiento de un importe de tasa desde el sistema de cliente al centro de transmisión de valores.

7. Procedimiento según una o varias de las reivindicaciones anteriores, **caracterizado porque** el centro de transmisión de valores identifica el sistema de cliente con ayuda de los datos transmitidos.

8. Procedimiento según una o varias de las reivindicaciones anteriores, **caracterizado porque** el centro de transmisión de valores envía los datos cifrados por el mismo al sistema de cliente.

9. Procedimiento según la reivindicación 8, **caracterizado porque** los datos enviados por el centro de transmisión de valores al sistema de cliente presentan un primer componente que no puede ser descifrado por el sistema de cliente y porque los datos presentan además una segunda parte, que puede ser descifrada por el sistema de cliente.

10. Procedimiento según la reivindicación 9, **caracterizado porque** la parte de los datos que puede ser descifrada por el sistema de cliente contiene el número aleatorio e informaciones acerca del proceso de carga.

11. Procedimiento según una o las dos reivindicaciones 9 o 10, **caracterizado porque** la parte de los datos que puede ser descifrada por el sistema de cliente contiene informaciones acerca de la suma a la que ascienden las tasas.

12. Procedimiento según una o varias de las reivindicaciones anteriores, **caracterizado porque** en cada transmisión de datos desde el centro de transmisión de valores al sistema de cliente se transmite un importe que basta para la generación de varias marcas de franqueo.

13. Procedimiento según la reivindicación 12, **caracterizado porque** el valor “hash” formado en el centro de transmisión de valores se forma teniéndose en cuenta las indicaciones acerca de los datos del envío.

14. Procedimiento según una o varias de las reivindicaciones 12 o 13, **caracterizado porque** el valor “hash” se forma teniéndose en cuenta un número aleatorio recibido y almacenado de forma intermedia.

15. Procedimiento según una o varias de las reivindicaciones 12 a 14, **caracterizado porque** el valor “hash” se forma teniéndose en cuenta un número de identificación del proceso de carga.

16. Procedimiento según una o varias de las reivindicaciones anteriores, **caracterizado porque** la marca de franqueo contiene datos lógicos.

17. Procedimiento según la reivindicación 16, **caracterizado porque** la marca de franqueo contiene informaciones

acerca de datos de envío.

18. Procedimiento según una o varias de las reivindicaciones 16 o 17, **caracterizado porque** los datos lógicos contienen informaciones acerca del número aleatorio cifrado.

19. Procedimiento según una o varias de las reivindicaciones 16 a 18, **caracterizado porque** los datos lógicos contienen informaciones acerca del número de identificación del proceso de carga cifrado.

20. Procedimiento según una o varias de las reivindicaciones 16 a 19, **caracterizado porque** los datos lógicos contienen informaciones acerca del valor “hash”.

21. Procedimiento según una o varias de las reivindicaciones anteriores, **caracterizado porque** la marca de franqueo contiene tanto informaciones transmitidas desde el centro de transmisión de valores como datos introducidos por el generador del documento.

22. Procedimiento según una o varias de las reivindicaciones anteriores, **caracterizado porque** la marca de franqueo contiene un valor “hash”, que se forma a partir de una combinación de un valor transmitido por el centro de especificación y el valor introducido por el generador del documento.

23. Procedimiento según una o varias de las reivindicaciones anteriores, **caracterizado porque** comprende las siguiente etapas de procedimiento: En el centro de transmisión de valores o en una zona asegurada, conectada con el centro de transmisión de valores se genera un secreto y se transmite a continuación junto con las informaciones acerca del proceso de carga al módulo de seguridad en el sistema de cliente.

24. Procedimiento según la reivindicación 23, **caracterizado porque** el sistema de cliente descifra el número aleatorio cifrado.

25. Procedimiento según la reivindicación 24, **caracterizado porque** el número de identificación de carga se transmite al sistema de cliente.

26. Procedimiento según la reivindicación 25, **caracterizado porque** en el módulo de seguridad se forma un valor “hash” a partir del número de identificación de carga y de otros datos.

27. Procedimiento según la reivindicación 26, **caracterizado porque** la marca de franqueo se genera de tal modo que contiene el valor “hash”.

28. Procedimiento según la reivindicación 1, **caracterizado porque** en el análisis de los datos contenidos en la marca de franqueo se comprueba si contienen datos cifrados del centro de transmisión de valores.

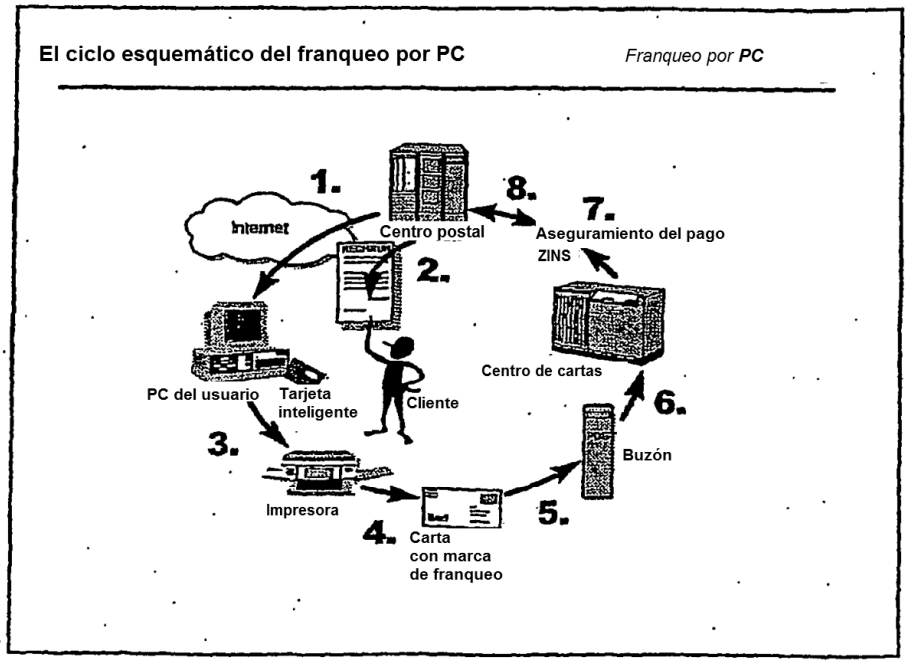

El ciclo esquemático del franqueo por PC
Franqueo por PC
1.
Internet
Centro postal
8.
7.
Aseguramiento del pago
ZINS
2.
Centro de cartas
PC del usuario
Tarjeta
inteligente
Cliente
6.
3.
Buzón
Impresora
5.
4.
Carta
con marca
de franqueo

Figura 1

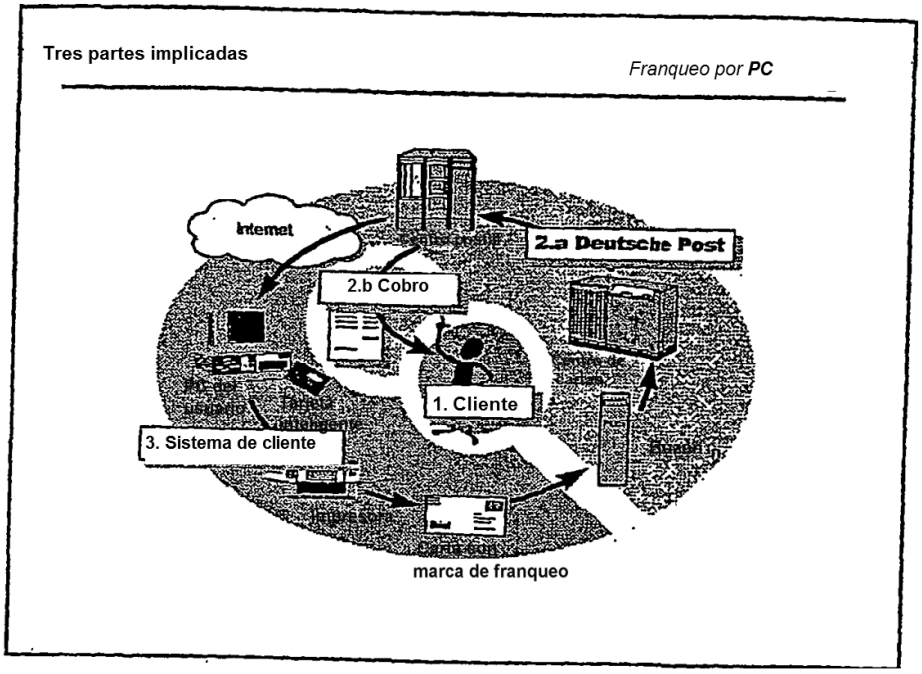

Tres partes implicadas
Franqueo por PC
Internet
2.a Deutsche Post
2.b Cobro
1. Cliente
3. Sistema de cliente
marca de franqueo

Figura 2

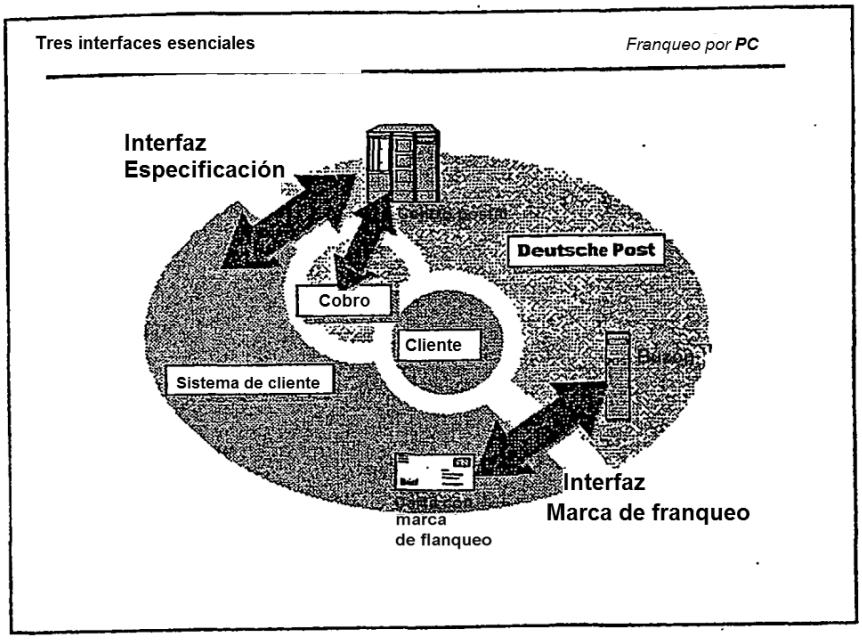
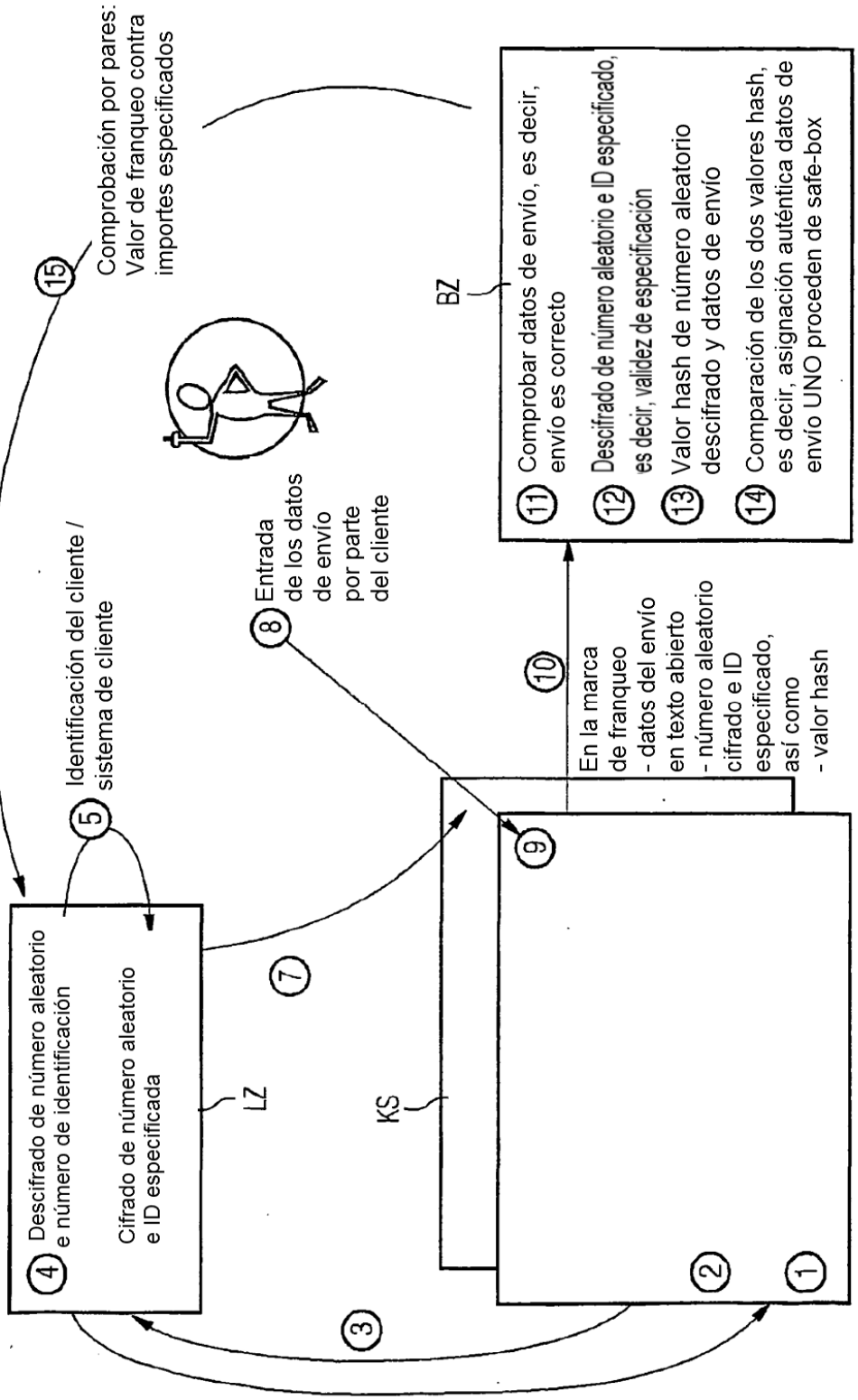

Tres interfaces esenciales
Franqueo por PC
Interfaz
Especificación
Deutsche Post
Cobro
Cliente
Sistema de cliente
Interfaz
Marca de franqueo
marca
de flanqueo

Figura 3


15
Comprobación por pares:
Valor de franqueo contra
importes especificados
BZ
11
Comprobar datos de envío, es decir,
envío es correcto
12
Descifrado de número aleatorio e ID especificado,
es decir, validez de especificación
13
Valor hash de número aleatorio
descifrado y datos de envío
14
Comparación de los dos valores hash,
es decir, asignación auténtica datos de
envío UNO proceden de safe-box
5
Identificación del cliente /
sistema de cliente
8
Entrada
de los datos
de envío
por parte
del cliente
10
En la marca
de franqueo
- datos del envío
en texto abierto
- número aleatorio
cifrado e ID
especificado,
así como
- valor hash
4
Descifrado de número aleatorio
e número de identificación
Cifrado de número aleatorio
e ID especificada
LZ
7
KS
9
3
2
1