(19) OFICINA ESPAÑOLA DE PATENTES Y MARCAS

ESPAÑA

(11) Número de publicación: **2 743 047**

(51) Int. CI.:

H04L 9/32 (2006.01)
G09C 5/00 (2006.01)

(12) TRADUCCIÓN DE PATENTE EUROPEA T3

(96) Fecha de presentación y número de la solicitud europea: **16.12.2014 E 14198205 (8)**

(97) Fecha y número de publicación de la concesión europea: **22.05.2019 EP 2894811**

(54) Título: **Procedimiento para garantizar la autenticidad, la integridad y el anonimato de un enlace a datos, en particular en la presentación del enlace a datos en forma de un código óptico bidimensional**

(30) Prioridad:

19.12.2013 DE 102013114493

(45) Fecha de publicación y mención en BOPI de la traducción de la patente:
18.02.2020

(73) Titular/es:

DEUTSCHE TELEKOM AG (100.0%)
Friedrich-Ebert-Allee 140
53113 Bonn , DE

(72) Inventor/es:

BURLAGA, ROLAND

(74) Agente/Representante:

ELZABURU, S.L.P

DESCRIPCIÓN

Procedimiento para garantizar la autenticidad, la integridad y el anonimato de un enlace a datos, en particular en la presentación del enlace a datos en forma de un código óptico bidimensional

Los códigos ópticos, como, por ejemplo, los códigos de barras se usan ampliamente en muchos ámbitos, en particular en la identificación de productos. Permiten, mediante escáneres ópticos, la detección rápida y fiable de los datos codificados en ellos, como ocurre en los procesos logísticos o en la venta de productos en sistemas con cajas. A diferencia de muchos otros procedimientos modernos de identificación sin contacto, como RFID, NFC o similares, los códigos ópticos son muy económicos y fáciles de aplicar en los procesos de impresión convencionales sobre prácticamente cualquier tipo de productos y documentos. A menudo incluso se pegan en diferentes etapas del procedimiento, aplicando (mediante adhesivo) el correspondiente código por etapa sobre la anterior.

En entornos de producto típicos y de logística, los códigos se utilizan en sistemas cerrados, es decir, existe una confianza en la autenticidad y la integridad del código óptico en la detección (escáner), ya sea a través del reconocimiento de la gama de productos y la «liberación» del producto por parte de la empleada / el empleado que se encuentra en la caja y la clienta / el cliente en el entorno típico de venta al por menor, o bien dentro de cadenas de logística o dentro de plantas de producción, en donde se garantiza de otra forma que el producto que lleva el código no puede ser alterado o falsificado.

Sin embargo, en los últimos años también se han usado códigos ópticos en combinación con comunicaciones electrónicas, sistemas de pago, sistemas de cupones o sistemas de entradas para confirmar transacciones de una segunda forma independiente de la comunicación de datos o para presentar referencias a informaciones electrónicas (por ejemplo, en Internet) sobre impresos o carteles publicitarios. Fuera del ámbito de la identificación de productos y de los procesos logísticos está especialmente extendido el uso de la variante Quick Response Codes (QR-Codes) de la empresa Denso (Japón). Estos códigos ópticos 2D se utilizan en anuncios publicitarios, sobre productos o en impresos para hacer referencia a informaciones adicionales que se encuentran en Internet.

Para ello contienen un enlace a datos que está codificado, preferiblemente un enlace a Internet típico en forma de URL (Uniform Resource Locators). Los códigos pueden ser escaneados fácilmente por un dispositivo móvil moderno, como, por ejemplo, un terminal de telecomunicaciones moderno en forma de teléfono inteligente (*smartphone*) con cámara y un software que puede analizar dichos códigos. El software de escaneo abre —en caso de que se trate de un enlace a Internet codificado— el correspondiente sitio web en un navegador web móvil en un dispositivo móvil.

Debido a la creciente difusión de estos códigos en todos los aspectos de la vida, se han vuelto interesantes para quienes llevan a cabo ataques con fines delictivos contra usuarios; el objetivo de dichos ataques es acceder a informaciones valiosas como, por ejemplo, iniciar sesión en cuentas bancarias o similares (el denominado «phishing»).

El objeto de la presente solicitud es dificultar este tipo de ataques. Para ello se propone proporcionar una comprobación de la autenticidad y la integridad de los datos útiles que contiene el código óptico.

El objeto se consigue mediante un procedimiento y un producto correspondiente en forma de programa de ordenador tal y como se reivindica en las reivindicaciones independientes. En las reivindicaciones dependientes se definen formas de realización preferidas. El documento US 2012/0308003 A1 muestra un procedimiento para crear y leer un código óptico en donde el mensaje del código se cifra adicionalmente al ser transmitido. Por medio de una clave pública, también mostrada en el código, se puede descifrar el mensaje cifrado y comparar con el mensaje original. Si ambos concuerdan, el código se verifica correctamente. Esta verificación puede llevarse a cabo, por ejemplo, utilizando un teléfono inteligente convencional.

El documento WO 99/33221 describe un dispositivo de firma para generar firmas digitales de documentos y describe, además, medidas de seguridad para el envío de firmas digitales a través de una red que no es segura, generando valores HASH de los elementos que componen los datos y cifrándolos, de manera que los datos de identificación del usuario (U), que son recibidos por un usuario presente físicamente, se incorporan adicionalmente a la firma digital.

El documento US 7,093,130 B1 da a conocer un procedimiento para generar entradas digitales a prueba de falsificación para un evento, en donde el vendedor de entradas y el punto de venta generan, cifran e intercambian entre sí diferentes datos durante el procesamiento de las etapas individuales de la transacción. Para verificar la entrada, desde el ordenador del vendedor de entradas se genera un valor *hash* mediante una función *hash*, a partir de un número R y se transmite al punto de venta. El punto de venta cifra este valor y lo aplica a la entrada digital junto con el número R. Para leer y verificar la entrada digital es necesario un lector conectado a un ordenador del vendedor de entradas. El lector solicita al ordenador del vendedor de entradas un código de descifrado y la función *hash* calcula un valor *hash* por medio de una función *hash* —que había sido usada originalmente por el ordenador del vendedor de entradas— y lo compara con el valor *hash* aplicado sobre la entrada digital.

El procedimiento según la invención permite códigos ópticos a prueba de falsificación, en particular, códigos 2D, los cuales pueden ser reconocidos por el usuario como íntegros y auténticos, incluso sin conexión en línea, en decir, sin una constatación directa con una base de datos o un servicio de Internet. Se requiere un software, que funcione en el dispositivo móvil, que compruebe la integridad y la autenticidad de los datos antes de hacer una petición para abrir un

enlace o de emitir datos codificados en el código 2D.

El procedimiento según la invención no modifica el procedimiento de codificación conocido para códigos ópticos, sino que asegura las informaciones contenidas de una manera similar al procedimiento de firma digital. Las sumas de comprobación u otros datos adicionales introducidos a través del procedimiento de codificación permanecen inalterados y competen a este procedimiento. El procedimiento según la invención se aplica a los datos útiles contenidos en el código óptico. Los datos útiles, desde el punto de vista del código óptico, deben contener también las propiedades de seguridad y en adelante se denominarán, por simplicidad, código de confianza o «trustcode».

Un código de confianza para su presentación en un código óptico puede estar formado esquemáticamente de la siguiente manera:

DATA#CAID#HALG#KALG#SIGNATURE

Los elementos se definen como:

: Símbolo de delimitación que no puede ser ningún símbolo permitido del conjunto de símbolos admisibles que representan los otros elementos;

DATA : Datos / información que se representa(n) con el código de confianza y cuya autenticidad e integridad se aseguran;

CAID : Codificación, para el procedimiento, fijada y conocida para todas las partes, de una instancia de certificación de confianza que confirma la autenticidad del código de confianza, es decir, la denominada autoridad de certificación (*certification authority*). Para tener en cuenta las pequeñas cantidades almacenadas de código óptico se utilizará una representación comprimida de una enumeración clara de las autoridades de certificación posibles;

HALG : Codificación comprimida e inequívoca del algoritmo *hashing* criptográfico utilizado para comprobar la integridad de DATA;

KALG : Codificación comprimida e inequívoca del algoritmo de cifrado asimétrico utilizado para comprobar la integridad de DATA;

SIGNATURE : La unión cifrada del valor *hash* HASH con el algoritmo de cifrado asimétrico denominado KALG, que se calcula sobre DATA por medio del algoritmo *hashing* criptográfico determinado con HALG, y

TOKEN, un valor aleatorio que se determina en el momento de la generación del código de confianza por parte de una instancia de confianza en el sitio de la autoridad de certificación, en caso de que sea necesario, ampliado por un denominado procedimiento *padding* si este es necesario para la seguridad del algoritmo de cifrado asimétrico KALG.

En adelante se indica con «cliente» la unidad formada por usuario, dispositivo móvil para escaneado y software que decodifica un código óptico con la característica de seguridad «código de confianza», mientras que con «servidor» se indica la unidad formada por el proveedor del servicio, dispositivos técnicos / instancias técnicas y autoridad de certificación que codifica el código óptico con la característica de seguridad «código de confianza» que contiene.

Generación del código de confianza

El servidor genera el código de confianza a partir de los datos DATA que se le pasan de un sitio de confianza, calculando primero el valor *hash* HASH según el algoritmo *hashing* criptográfico HALG configurado del lado del servidor. Un valor aleatorio TOKEN de mayor entropía se anexa al valor *hash* HASH (determinado preferiblemente después de un procedimiento criptográfico reconocido como valor aleatorio suficientemente aleatorio) correspondiente al formato configurado del lado del servidor. El valor aleatorio TOKEN se guarda en el lado del servidor vinculado con el código de confianza emitido para la futura verificación desde el lado del servidor.

Si el algoritmo de cifrado asimétrico KALG configurado del lado del servidor lo requiere, se aplica a la unión de HASH y TOKEN un procedimiento *padding* definido para el algoritmo.

Después, este resultado o la unión de HASH y TOKEN se cifra a SIGNATURE según el algoritmo de cifrado asimétrico configurado correspondiente mediante el uso de la clave privada de la autoridad de certificación.

El servidor emite los elementos así determinados del código de confianza alineados y preferiblemente separados entre sí, a través del símbolo de delimitación configurado #, como código de confianza. Estas etapas del procedimiento se muestran a modo de ejemplo en la figura 1.

Verificación del código de confianza

Un cliente, que dispone de la autoridad de certificación a través de la clave pública, puede comprobar la integridad y la autenticidad del código de confianza contenido en un código óptico, calculando por su parte un valor *hash* HASH 2 según el algoritmo *hashing* criptográfico HALG codificado en el código de confianza a través de DATA y comparándolo

con el HASH cifrado en SIGNATURE. Si los valores son idénticos, entonces el código de confianza es auténtico y puede ser escaneado por el emisor de confianza.

El cliente determina el valor HASH precalculado por el servidor contenido en SIGNATURE, cifrando correspondientemente la SIGNATURE del algoritmo de cifrado asimétrico KALG codificado en el código de confianza con la clave conocida pública de la instancia de certificación de confianza «autoridad de certificación».

En caso de que sea necesario se debe eliminar, en función del procedimiento de cifrado asimétrico seleccionado, un *padding* de los datos descifrados.

Puesto que el algoritmo *hashing* criptográfico codificado en el código de confianza proporciona un resultado inequívoco de longitud fija, este puede aislarse fácilmente, en comparación con el valor calculado por el cliente, a partir de la unión de HASH y TOKEN dentro de SIGNATURE.

En este proceso, el cliente determina al mismo tiempo el valor TOKEN que puede usar para una posible comunicación adicional del servidor para la identificación de cliente y código de confianza del lado del servidor.

Identificación de un código de confianza reconocido por el cliente en el canal de retorno en el lado del servidor

Cuando el cliente, debido a un reconocimiento correcto y a la autenticidad y la integridad del código de confianza comprobado correctamente, establece un canal de retorno y/o una comunicación con el servidor, entonces se puede utilizar el valor TOKEN determinado para indicar al servidor el reconocimiento correcto y la relación con un determinado código de confianza.

Para ello, el cliente cifra el TOKEN con la ayuda del algoritmo de cifrado asimétrico KALG codificado en el código de confianza y con la clave pública de la autoridad de certificación, e inserta el valor calculado como REPLY en una sintaxis predefinida para la comunicación en el canal de retorno.

El servidor puede descifrar el valor REPLY por medio de la clave privada de la autoridad de certificación y aislar así el TOKEN que compara con el valor TOKEN_C creado y guardado por él durante la creación del código de confianza. Si el servidor encuentra el TOKEN, puede asignar el mensaje de respuesta inequívoco de un código de confianza generado anteriormente y al mismo tiempo reconocer que el cliente ha reconocido correctamente el código de confianza. Estas etapas del procedimiento se muestran a modo de ejemplo en la figura 2.

Aplicación práctica para enlaces en códigos OR

Un enlace a datos codificado en un código OR, en particular como enlace a Internet en forma de una URL puede asegurarse muy fácilmente con el procedimiento según la invención si el enlace URL deseado se considera como DATA y se trata correspondientemente. Cuando el enlace URL además está diseñado de forma que manda de vuelta la comunicación del código de confianza al servidor y el cliente utiliza todo el código de confianza como URL en la petición tras comprobar correctamente la autenticidad y la integridad, y además incluye el valor REPLY con el símbolo de delimitación definido en el código de confianza, el servidor puede reconocer el éxito de la comprobación del lado del cliente y la pertenencia a un código de confianza generado previamente y presentar al cliente otro resultado que cuando se produce la petición sin la REPLY, tal y como se muestra a modo de ejemplo en la figura 2.

En particular, la sintaxis descrita en el procedimiento según la invención es adecuada para que también los clientes que no pueden reconocer ni verificar el código de confianza, puedan abrir un enlace contenido. En caso de ausencia del REPLY, el servidor puede reconocer que la petición procede de un cliente sin comprobación de seguridad y puede presentar a este cliente otro resultado, en particular otras informaciones.

REIVINDICACIONES

1. Procedimiento para asegurar la autenticidad y la integridad de datos (DATA) de un código óptico que incluye las siguientes etapas:

- Generar una firma (SIGNATURE) para un código de confianza que sirve para asegurar la autenticidad y la integridad de los datos (DATA) presentados en el código óptico que incluye:

i. calcular un valor *hash* (HASH) por medio de un algoritmo *hashing* criptográfico (HALG) para los datos (DATA), de manera que los datos (DATA) incluyen un enlace a datos, en particular un enlace;

ii. añadir un valor aleatorio (TOKEN) al valor *hash* (HASH), unir y cifrar el valor *hash* (HASH) y el valor aleatorio (TOKEN) por medio de una clave privada de un algoritmo de cifrado asimétrico (KALG);

- Generar el código de confianza para la presentación en el código óptico, de manera que el código de confianza presenta:

i. una información sobre una instancia de certificación (CAID);

ii. una información sobre el algoritmo *hash* (HALG) utilizado;

iii. una información sobre el algoritmo de cifrado asimétrico (KALG) utilizado;

iv. los datos (DATA);

v. la firma generada (SIGNATURE)

- Asegurar la autenticidad y la integridad de los datos, en particular de un enlace a través de las siguientes etapas:

i. leer y procesar el código de confianza por medio de un dispositivo de telecomunicación móvil, en particular un teléfono inteligente (*smartphone*);

ii. determinar el algoritmo *hashing* (HALG) utilizado sobre el código de confianza por medio del dispositivo de telecomunicación móvil;

iii. calcular un segundo valor *hash* (HASH 2) sobre datos (DATA) por medio del dispositivo de telecomunicación;

iv. determinar una clave pública para el algoritmo de cifrado asimétrico (KALG) utilizado;

v. descifrar la firma (SIGNATURE) por medio de la clave pública;

vi. aislar el valor hash (HASH) de la firma descifrada (SIGNATURE);

vii. comparar el valor *hash* (HASH) con el segundo valor *hash* (HASH 2), de manera que en caso de que coincidan el valor *hash* (HASH) y el segundo valor *hash* (HASH 2) se abra la dirección de red contenida en el enlace a datos;

viii. aislar el valor aleatorio (TOKEN) de la firma descifrada;

ix. cifrar el valor aleatorio (TOKEN) por medio de la clave pública para un valor aleatorio cifrado (TOKEN_V);

x. añadir el valor aleatorio cifrado (TOKEN_V) en una sintaxis predefinida en la comunicación con un servidor;

xi. descifrar el valor aleatorio cifrado (TOKEN_V) recibido desde el servidor por medio de la clave privada del algoritmo de cifrado asimétrico (KALG) utilizado y comparar el valor aleatorio cifrado para la verificación del código de confianza con una copia almacenada del valor aleatorio (TOKEN_C).

2. Procedimiento según la reivindicación 1, **caracterizado porque** antes del cifrado de la unión del valor *hash* (HASH) y el valor aleatorio (TOKEN) se aplica un procedimiento *padding* (PADDING) definido para el algoritmo de cifrado asimétrico (KALG) utilizado.

3. Procedimiento según la reivindicación 2, **caracterizado porque** en caso de que no coincidan el valor aleatorio (TOKEN) y la copia del valor aleatorio (TOKEN_C) o en caso de que no se reciba el valor aleatorio cifrado (TOKEN_V), se proporciona otro resultado a cuando coinciden el valor aleatorio (TOKEN) y la copia del valor aleatorio (TOKEN_C).

4. Producto en forma de programa de ordenador que ejecuta un procedimiento según cualquiera de las reivindicaciones 1 a 3, que se carga e implementa en un servidor.

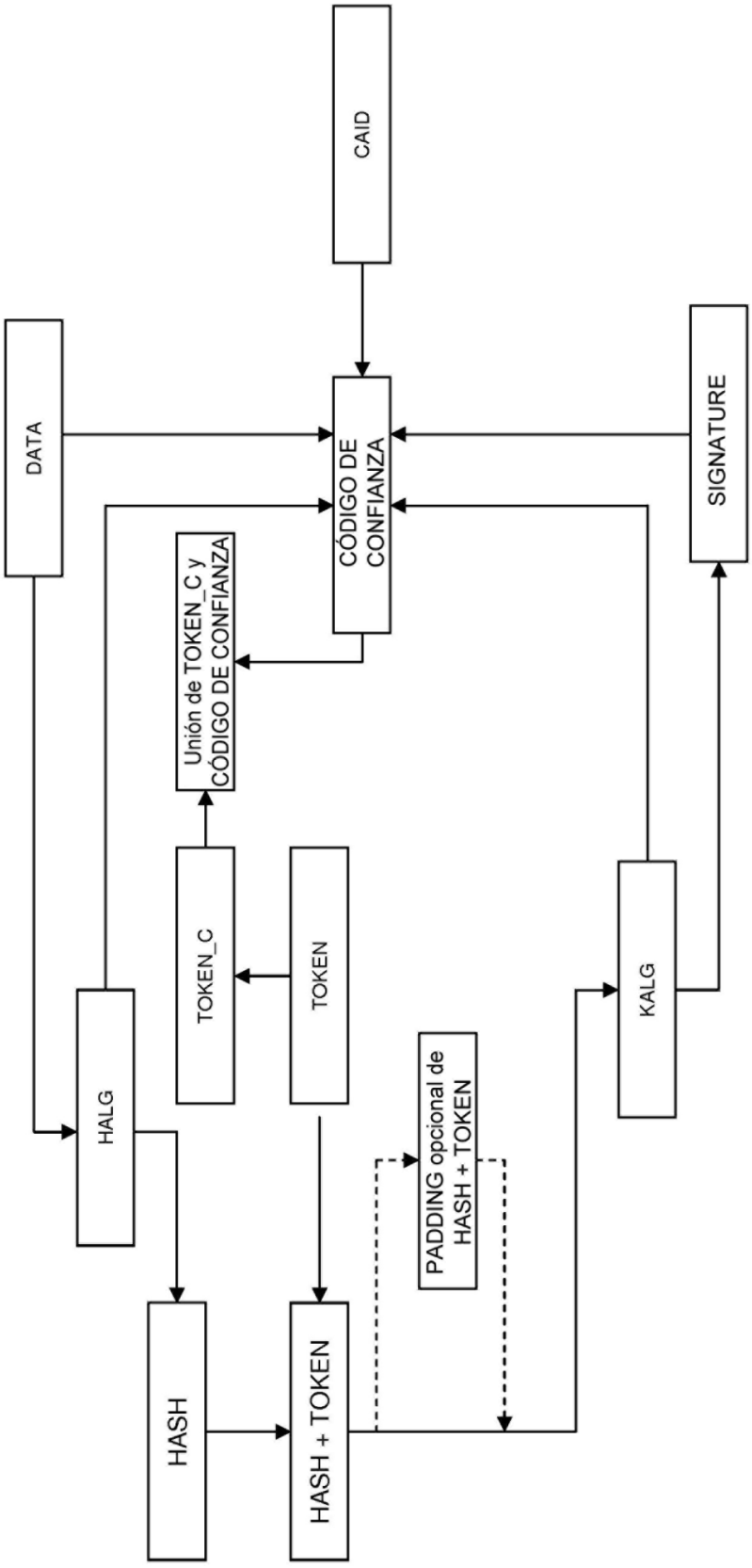
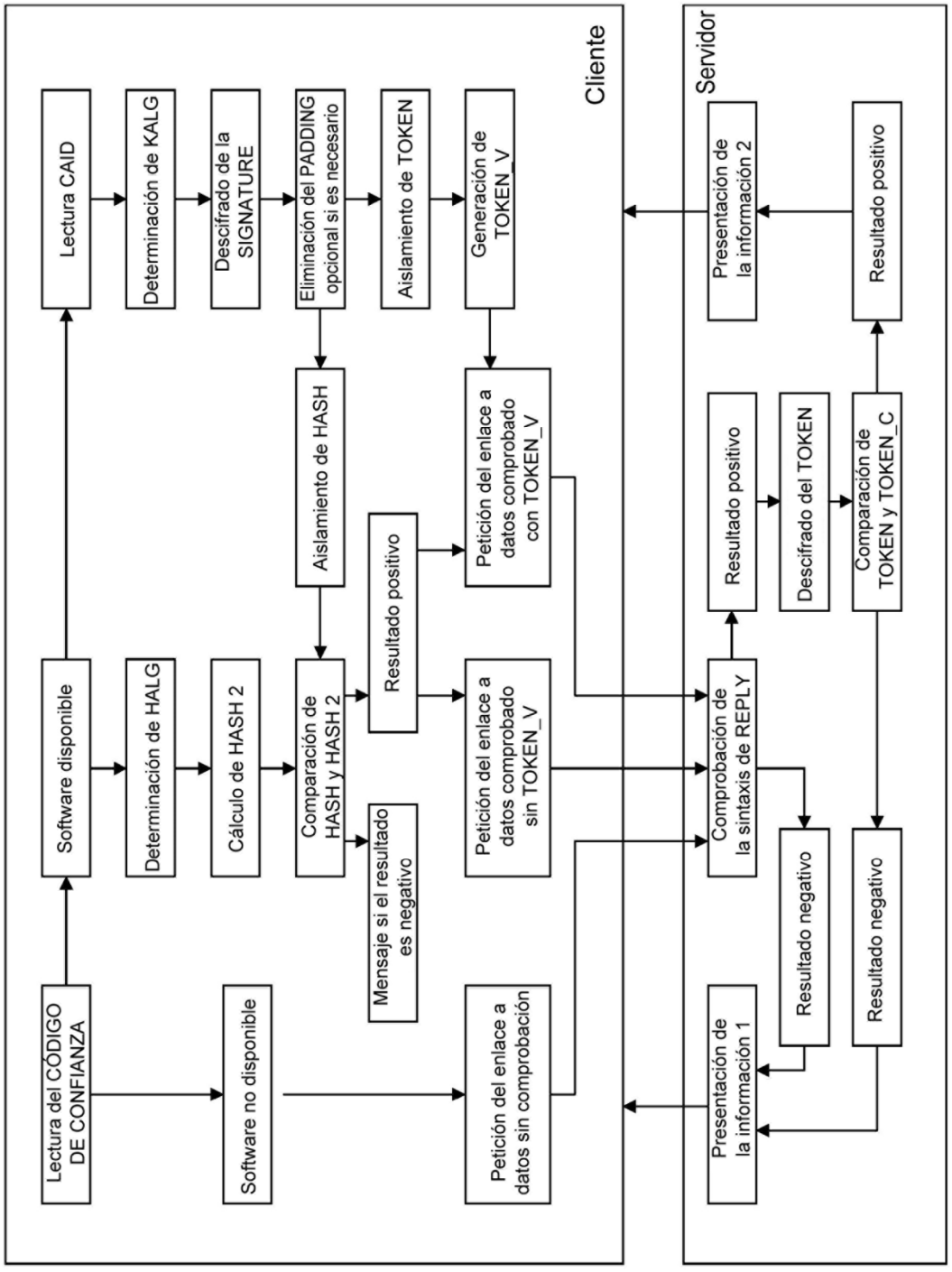

CAID
DATA
CÓDIGO DE CONFIANZA
SIGNATURE
Unión de TOKEN_C y CÓDIGO DE CONFIANZA
TOKEN_C
TOKEN
HALG
KALG
PADDING opcional de HASH + TOKEN
HASH
HASH + TOKEN

Figura 1

Figura 2


Cliente
Servidor
Lectura del CÓDIGO DE CONFIANZA
Software disponible
Software no disponible
Lectura CAID
Determinación de HALG
Determinación de KALG
Cálculo de HASH 2
Descifrado de la SIGNATURE
Comparación de HASH y HASH 2
Eliminación del PADDING opcional si es necesario
Aislamiento de HASH
Mensaje si el resultado es negativo
Aislamiento de TOKEN
Resultado positivo
Generación de TOKEN_V
Petición del enlace a datos comprobado con TOKEN_V
Petición del enlace a datos comprobado sin TOKEN_V
Petición del enlace a datos sin comprobación
Presentación de la información 1
Comprobación de la sintaxis de REPLY
Resultado negativo
Resultado positivo
Descifrado del TOKEN
Comparación de TOKEN y TOKEN_C
Resultado negativo
Presentación de la información 2
Resultado positivo