(19) OFICINA ESPAÑOLA DE PATENTES Y MARCAS

ESPAÑA

(11) Número de publicación: **2 599 615**

(51) Int. CI.:

G06F 21/32 (2013.01)
G06F 21/62 (2013.01)

(12) TRADUCCIÓN DE PATENTE EUROPEA T3

(86) Fecha de presentación y número de la solicitud internacional: **29.04.2009 PCT/GB2009/050438**

(87) Fecha y número de publicación internacional: **05.11.2009 WO09133397**

(96) Fecha de presentación y número de la solicitud europea: **29.04.2009 E 09738427 (5)**

(97) Fecha y número de publicación de la concesión europea: **27.07.2016 EP 2272021**

(54) Título: **Memoria caché de datos segura**

(30) Prioridad:

29.04.2008 GB 0807753

(45) Fecha de publicación y mención en BOPI de la traducción de la patente:
02.02.2017

(73) Titular/es:

CRYPTOMATHIC LTD (100.0%)
329 Cambridge Science Park Milton Road
Cambridge, Cambridgeshire CB4 0WG, GB

(72) Inventor/es:

BOND, MICHAEL

(74) Agente/Representante:

CARPINTERO LÓPEZ, Mario

DESCRIPCIÓN

Memoria caché de datos segura

Campo de la invención

La presente invención versa, en general, sobre procedimientos, un aparato y código de programa de ordenador para introducir datos de forma segura en una memoria caché, en particular para almacenar datos sensibles privados y/o de seguridad, tales como datos biométricos de documentos de identidad electrónicos.

Antecedentes

Los documentos de identidad electrónicos son documentos físicos de ID aumentados con información almacenada electrónicamente; por ejemplo, aumentados con chips de tarjeta inteligente con interfaces con contactos o sin contactos. Ejemplos incluyen pasaportes electrónicos, documentos nacionales de identidad, carnés de conducir y tarjetas sanitarias. El chip de tarjeta inteligente puede llevar a cabo diversas funciones, incluyendo la autentificación de la identidad de los usuarios, proporcionar resistencia a falsificaciones y almacenar datos. Crucialmente, muchos esquemas de identidad electrónicos usan chips de tarjeta inteligente con almacenamiento como base de datos distribuida de datos personales y biométricos para la identidad del tenedor de la tarjeta. Cada tarjeta podría almacenar hasta 80 KB de datos.

La Organización de Aviación Civil Internacional (OACI) ha producido un conjunto de normativas para el almacenamiento de datos biométricos en Documentos de Viaje de Lectura Mecánica (MRTD), formateados de una manera que protege su integridad con una firma digital procedente de la autoridad emisora. El formato de los datos almacenados y de la metainformación asociada comprende la “Estructura Lógica de Datos” (LDS).

Aunque hay muchas ventajas en el uso de un sistema de tarjetas inteligentes como una base de datos distribuida, también hay inconvenientes. En particular, lleva mucho tiempo leer datos de chips de tarjeta inteligente debido a las limitaciones en el ancho de banda de la interfaz sin contactos. Puede llevar más de diez segundos leer grupos de datos biométricos de un documento de identidad electrónico. Con un chip y un soporte lógico de lectura deficientemente emparejados puede llevar más de 20 segundos. Ni siquiera la interfaz de contactos con una tarjeta soporta velocidades de transferencia de datos particularmente elevadas, y la cantidad de datos personales y biométricos que puede ser necesario almacenar crece rápidamente al competir por establecerse diferentes esquemas biométricos (huella dactilar, iris, etc.).

Una alternativa a un esquema a base de chips inteligentes para documentos de identidad es mantener un almacén central de datos. La tecnología de clave pública es de aplicación clara en cualquiera de los dos escenarios para permitir a los verificadores comprobar la integridad de los datos recuperados del almacén central. Sin embargo, para el propio almacén hay inquietudes considerables de seguridad y privacidad. Además, hay problemas de conectividad que considerar cuando los documentos de identidad deben ser verificados en entornos remotos, o si la base de datos central adolece de un fallo de comunicaciones.

Sería necesario que el contenido de tales bases de datos estuviera sujeto a leyes de protección de datos, pero es susceptible de uso indebido y de perversión de sus fines (uso legal para un fin distinto de la razón original por la que fueron reunidas en su origen). Aunque los estados son libres de aplicar sus propios programas centrales de recogida de datos biométricos, la UE ha requerido que los datos biométricos sensibles recuperados de pasaportes de la UE por los estados miembros no deben ser almacenados por sistemas de inspección.

Se conocen procedimientos de creación de almacenes cifrados de datos por los documentos WO98/47259 y US6577735. “Cryptographic protection of databases”, en Applied Cryptography (XP002958299), describe el cifrado de una base de datos de filiación usando datos de la base de datos de filiación. “Crossing Borders: Security and Privacy Issues of the European e-Passport”, de Hoepman et al (XP19047433), describe esquemas para mejorar la seguridad de los pasaportes electrónicos.

Afirmaciones de la invención

Según un aspecto de la invención, se proporciona un procedimiento de introducción en memoria caché de forma segura de datos almacenados en un documento de identidad electrónico según la reivindicación 1.

Según otro aspecto de la invención, se proporciona un sistema de introducción en memoria caché según la reivindicación 9.

El uso de tal memoria caché acelera tremendamente el procedimiento de inspección soslayando por entero la necesidad de leer datos, salvo durante la primera inspección. El procedimiento y sistema de introducción en memoria caché anteriores crean una memoria caché cifrada de datos biométricos en la que cada entrada puede ser objeto de acceso únicamente en presencia del documento de identidad original en el que se originó. El uso de tal memoria caché cifrada representa un punto medio viable entre un esquema totalmente distribuido en el que no se almacena dato alguno y un esquema totalmente centralizado en el que todos los datos son almacenados

centralmente. La introducción de datos en una memoria caché local puede producirse para datos que han sido leídos de documentos de identidad en un ámbito local, nacional o incluso internacional.

Los datos pueden ser almacenados en la memoria caché bajo un seudónimo o un identificador anónimo, por lo que dichos datos no son personalmente identificables en la memoria caché. Se puede considerar que el identificador es una clave de consulta para los datos, porque permite que un sistema de inspección consulte datos, pero el identificador no está pensado para ser una clave criptográfica. Por ejemplo, puede que en la memoria caché se almacene únicamente parte de los datos, pudiendo omitirse la cabeza de cada fichero de datos. Así, sería inviable recuperar los datos sin acceso al documento original.

Dicho documento electrónico puede comprender un compendio de datos, es decir, un fichero que compendie los datos almacenados en el mismo. Dicho compendio de datos puede incluir comprobaciones criptográficas aleatorias de otros datos almacenados, o una firma digital y la totalidad o parte de dicho compendio de datos puede ser usada calcular una clave criptográfica única para dichos datos biométricos. Por ejemplo, puede aplicarse una función de deducción de clave a este compendio de datos para generar una clave segura para cifrar los datos del pasaporte. Tal clave solo puede ser creada nuevamente a partir del compendio de datos únicamente cuando está presente el documento electrónico. También se puede aplicar una función de deducción de identificador a este compendio de datos para generar un identificador para los datos.

Dichos datos biométricos pueden comprender datos de información facial y/o de huellas dactilares y la totalidad o parte de dicho compendio de datos, por ejemplo una firma digital, pude ser usada para calcular una clave criptográfica única para dichos datos biométricos.

Por ejemplo, el documento de identidad electrónico puede ser un pasaporte electrónico de la UE compatible con la OACI, que puede contener dieciséis grupos de datos diferentes de información biométrica (por ejemplo de información facial, de huellas dactilares y/o de iris), biográfica y adicional, tal como datos de firma. Cualquiera y/o la totalidad de estos grupos de datos pueden ser introducidos en memoria caché. Tales pasaportes también comprenden un compendio de datos en forma de un “Objeto de Seguridad de Documento” (SO_D), que es una especie de “fichero compendiado” que contiene una firma digital. El SO_D protege la integridad de la información almacenada en el pasaporte electrónico y es leído antes de que se lean ningún grupo grande de datos de un pasaporte electrónico. El SO_D contiene datos imprevisibles de entropía elevada y, así, la clave criptográfica única puede ser deducida del objeto de seguridad del documento, por ejemplo de la firma digital.

Dicha clave criptográfica única puede ser un valor de comprobación aleatoria. Cifrar la totalidad o parte de dichos datos puede comprender salar dichos datos. Deducir un valor de comprobación aleatoria y salar son técnicas criptográficas estándar. Una función de comprobación aleatoria es una transformación que toma una entrada y devuelve una cadena de tamaño fijo a la que se denomina valor de comprobación aleatoria. El valor de comprobación aleatoria puede ser una representación concisa de un mensaje o un documento más largo a partir del cual se calcula y, así, a veces se lo denomina “compendio del mensaje”. El compendio del mensaje es una especie de huella dactilar digital del documento mayor, dado que es única a ese documento. En criptografía, una sal comprende bits aleatorios que son usados como una de las entradas a una operación criptográfica para aumentar la entropía de la entrada.

En el ejemplo específico de los pasaportes electrónicos, el SO_D incluye comprobaciones aleatorias de los datos biométricos y de la propia firma digital. Estas comprobaciones aleatorias pueden ser usadas para calcular dicha clave criptográfica única, por ejemplo la mitad del valor de comprobación aleatoria puede ser salada y luego generar la comprobación aleatoria usando técnicas criptográficas estándar óptimas.

Algunos de los datos almacenados en un documento electrónico pueden ser protegidos por otros mecanismos para impedir el acceso no autorizado a tales datos. En consecuencia, puede no ser suficiente usar información compendiada para calcular la clave criptográfica única, dado que tal información introduce efectivamente en memoria caché el resultado del acceso autorizado a los datos. En tales circunstancias, parte de los propios datos, por ejemplo la cabeza del fichero de los datos en sí, puede ser usada para crear la clave criptográfica única para los datos. De esta manera, el emisor del documento siempre puede revocar el acceso a los datos controlados por acceso (suponiendo que el emisor del documento audite efectivamente que la memoria caché de datos segura está debidamente implementada).

Por ejemplo, los datos de huellas dactilares en los pasaportes de la UE están protegidos contra el acceso no autorizado a través de un mecanismo de seguridad del conjunto de programas de EAC denominado “Autenticación del terminal”, que requiere un sistema de inspección para demostrar que está autorizado para recuperar los datos. Si la comprobación aleatoria de los datos de huellas dactilares almacenadas en el SO_D es usada para calcular la clave criptográfica única, esta comprobación aleatoria siempre está disponible para un inspector del pasaporte electrónico sin pasar por el procedimiento de autenticación del terminal. Por lo tanto, el almacenamiento de datos de huellas dactilares usando únicamente la firma electrónica introduce en efecto en memoria caché el resultado (con éxito) de la autenticación del terminal. Así, aunque la autenticación del terminal sea retirada del sistema de inspección, sigue pudiendo acceder a los datos de huellas dactilares. En este ejemplo, los datos biométricos, es decir, datos de

huellas dactilares, están en forma de imagen y la clave criptográfica única para dicha imagen puede ser calculada usando parte de dicha imagen sola o en combinación con dicha firma electrónica.

Según otro aspecto de la invención, se proporciona un procedimiento de recuperación de datos según se define en la reivindicación 6.

En otras palabras, los datos (salvo los necesarios para crear la clave) en el documento electrónico son recuperados de la memoria caché de datos segura y no del propio documento. Según se ha explicado anteriormente, esto acelera muchísimo el tiempo requerido para acceder a los datos del documento. Es posible soslayar la necesidad de leer todos los datos, salvo durante la primera inspección del documento, es decir, durante la creación de la memoria caché de datos.

Según otro aspecto de la invención, se proporciona un procedimiento de verificación o inspección de un documento electrónico según se define en la reivindicación 7.

Según otro aspecto de la invención, se proporciona un sistema de recuperación de datos para recuperar información según se define en la reivindicación 12.

Según otro aspecto de la invención, se proporciona un sistema de verificación para verificar un documento electrónico según se define en la reivindicación 13.

El sistema de verificación puede estar asociado con una clave criptográfica secreta conocida únicamente por el propio sistema de verificación y esta clave criptográfica secreta puede incorporarse al cálculo para deducir la clave criptográfica única para los datos.

La invención proporciona, además, código de control de procesador para implementar los procedimientos anteriormente descritos, por ejemplo en un sistema de ordenadores de uso general o en un procesador de señales digitales (DSP). El código puede ser proporcionado en un soporte tal como un disco, CD-ROM o DVD-ROM, memoria programada, tal como memoria de solo lectura (soporte lógico inalterable). El código (y/o los datos) para implementar realizaciones de la invención puede comprender código fuente, objeto o ejecutable en un lenguaje convencional de programación (interpretado o compilado), tal como C, o código ensamblador, código para configurar o controlar un ASIC (circuito integrado para aplicaciones específicas) o una FPGA (matriz de puertas programables *in situ*) o código para un lenguaje de descripción de soporte físico, tal como Verilog (marca comercial) o VHDL (lenguaje descriptivo de soporte físico de circuitos integrados de altísima velocidad). Como apreciará una persona experta, tal código y/o tales datos pueden ser distribuidos entre varios componentes acoplados en comunicación mutua.

Breve descripción de los dibujos

La Figura 1 es una vista general de un diagrama de bloques de un sistema de inspección que incorpora una memoria caché de datos segura;
la Figura 2 es una variación de la Figura 1 para su uso en un sistema de inspección usado en aplicaciones de pasaportes electrónicos;
la Figura 3 ilustra el cálculo de una clave criptográfica única para los datos del pasaporte electrónico de la Figura 2;
la Figura 4 es un diagrama esquemático que muestra cómo se comunican los sistemas de inspección locales, nacionales e internacionales con una memoria caché de datos segura;
la Figura 5 muestra un diagrama esquemático de los componentes de un sistema de inspección de la Figura 1 o la Figura 2; y
la Figura 6 es un diagrama de flujo de las etapas de la creación de una memoria caché de datos segura, la recuperación de información de la misma y de verificación de un documento.

Descripción detallada de los dibujos

La Figura 1 muestra un sistema 10 de inspección para inspeccionar un documento electrónico que contiene un chip inteligente 12 en el que se almacenan datos 14, que incluyen un compendio de datos y datos sin tratar. El chip inteligente 12 puede tener una interfaz con contactos o sin contactos. El sistema de inspección accede a datos electrónicos contenidos en el chip inteligente 12 mediante tecnología estándar que en la actualidad es un enlace 16 de bajo ancho de banda. Bajo ancho de banda significa bajo ancho de banda en proporción a la cantidad de datos que deben ser transmitidos.

El sistema 10 de inspección también está conectado a una memoria caché 18 de datos segura que puede ser local al sistema de inspección o puede ser una memoria caché compartida a la que el sistema de inspección esté conectado, por ejemplo mediante una conexión en línea. Cada entrada en la memoria caché comprende un identificador ID 20 y los datos cifrados sin tratar $\{\text{datos sin tratar}\}_K$ 22 cifrados usando una clave criptográfica única K. La comunicación entre el sistema 10 de inspección y la memoria caché 18 de datos segura es un enlace

bidireccional para que el sistema de inspección pueda añadir entradas a la memoria caché y consultar información almacenada en la memoria caché.

Según se representa mediante líneas discontinuas, tanto el identificador ID como la clave criptográfica única K usada para cifrar los datos se deducen del compendio de datos contenidos en el chip inteligente. La clave se deduce usando un mecanismo 24 de deducción de clave, que puede ser una función de comprobación aleatoria u otra función criptográfica estándar aplicada al compendio de datos. De modo similar, el identificador se deduce usando un mecanismo 26 de deducción de identificador, que puede aplicar una función de comprobación aleatoria u otra función similar al compendio de datos. Los mecanismos de deducción tanto de la clave como del identificador forman parte de un procesador 28 que puede ser local del sistema de inspección o estar alejado del mismo.

En la Figura 2, el sistema de la Figura 1 ha sido adaptado para el ejemplo de un pasaporte electrónico 32 de la UE compatible con la OACI. Los datos 34 almacenados en tal pasaporte 32 contienen dieciséis grupos diferentes de información biométrica, biográfica y adicional. Dos de los grandes grupos de datos biométricos que han de almacenarse en los pasaportes electrónicos de la UE compatibles con el Control Extendido de Acceso (EAC) son:

Grupo 2 de datos (DG2): Información facial
Grupo 3 de datos (DG3): Información de huellas dactilares

Antes de que estos grandes grupos de datos sean leídos de un pasaporte electrónico se lee en primer lugar el "Objeto de Seguridad del Documento" (SO_D). El "Objeto de Seguridad del Documento" (SO_D) es una especie de "fichero compendiado" que contiene una firma digital y protege la integridad de la información almacenada en el pasaporte electrónico. Dado que el fichero compendiado contiene datos imprevisibles de entropía elevada, incluyendo comprobaciones aleatorias de datos biométricos y la propia firma digital, se puede aplicar a estos datos una función de deducción de clave para generar una clave segura para cifrar los datos del pasaporte. Tal clave solo podría ser recreada en posesión del fichero compendiado.

En el ejemplo específico de pasaportes electrónicos, los valores de comprobación aleatoria calculados sobre cada grupo de datos pueden ser usados como claves criptográficas para cifrar los datos sin tratar del grupo de datos antes de introducirlos en la memoria caché. Los valores de comprobación aleatoria también pueden ser usados como un seudónimo o identificador para impedir que el grupo de datos sea personalmente identificable en la base de datos.

En un ejemplo particular, el DG2 puede ser almacenado de forma segura dividiendo por la mitad la comprobación aleatoria de los datos H(DG2). La primera mitad es usada como identificador ID=left(H(DG2)) para una tabla (no criptográfica) de comprobaciones aleatorias para almacenar el grupo de datos. A continuación, el grupo de datos es cifrado usando una clave criptográfica deducida de la segunda mitad de la comprobación aleatoria, es decir, K=right(H(DG2)). Se usan técnicas criptográficas estándar óptimas para tal cifrado, incluyendo la adición de sal. Filas ejemplares en una tabla de memoria caché contendrían la siguiente clave o identificador de consulta y los siguientes datos cifrados:

left(hash(DG2))	encrypt(right(hash(DG2)), saltiDG2)

De esta manera, se puede calcular la clave y descifrar el grupo de datos únicamente en posesión del pasaporte electrónico real (cuyo Objeto de Seguridad de Documento contiene las comprobaciones aleatorias de los grupos de datos). Es inviable predecir el valor de esta comprobación aleatoria de un grupo de datos biométricos, ni siquiera conociendo la identidad del ciudadano a partir de la cual se han creado los grupos de datos. Normalmente, los datos son un fichero JPEG, una imagen WSQ o un fichero de imagen similar, y tales ficheros de imágenes son codificaciones altamente redundantes desde una perspectiva semántica. En consecuencia, contienen muchos datos imprevisibles y, así, tienen una entropía elevada.

Algunos datos de tarjetas inteligentes que una inspección podría querer introducir en una memoria caché están protegidos por mecanismos de control de acceso. Por ejemplo, los datos de huellas dactilares en los pasaportes de la UE están almacenados en el grupo 3 de datos (DG3) y están protegidos contra un acceso no autorizado por medio de un mecanismo de seguridad del conjunto de programas de EAC denominado "Autenticación del terminal", que requiere un sistema de inspección para demostrar que está autorizado para recuperar los datos. Sin embargo, la comprobación aleatoria de los datos de huellas dactilares está disponible para un inspector del pasaporte electrónico en el objeto de seguridad del documento sin pasar por el procedimiento de autenticación del terminal. Por lo tanto, el almacenamiento de datos de huellas dactilares usando el anterior esquema introduce en efecto en memoria caché el resultado (con éxito) de la autenticación del terminal. En casos en los que el mecanismo de control de acceso podría ser evitado después del primer acceso con éxito, la Figura 3 muestra cómo deduce la clave K el mecanismo 24 de deducción.

La comprobación aleatoria de los datos H(EF.DG3) 32 que está disponible en el objeto de seguridad del documento se combina con la cabeza del fichero en sí. Es importante incluir una cabeza suficientemente grande del fichero 40 para subsumir datos adecuados de entropía elevada en la comprobación aleatoria. La cantidad de cabeza usada

debe extenderse sobre la cabecera 42 del fichero, las cabeceras biométricas CBEFF 44 y las cabeceras 46 de imagen y parte de la propia imagen 48. Así, los datos de entropía elevada procedentes de un fichero compendiado que no está sujeto al control de acceso, junto con la cabeza del propio fichero en sí que está sujeto a control de acceso son usados como entrada a la función de deducción de clave.

El primer par de centenares de bytes del grupo de los datos de huellas dactilares es concatenado con la comprobación aleatoria del DG3 para crear una clave que solo puede ser recreada después de realizar el debido procedimiento de control de acceso. Por lo tanto, el emisor del documento siempre puede revocar el acceso de otro país a los datos controlados por acceso (suponiendo que el emisor del documento audite efectivamente que el inspector esté implementando el esquema debidamente). En este ejemplo, la tabla de la memoria caché contendría filas de la forma siguiente:

left(hash(DG3))	encrypt(hash(head(DG3)), salt||DG3)

La Figura 4 ilustra cómo puede conectarse el sistema 10 de inspección a una o más memorias cachés de datos seguras. El sistema de inspección puede comunicarse con una memoria caché de datos segura en forma de una memoria caché local 101 embebida en el propio sistema de inspección. El sistema de inspección puede comunicarse con una memoria caché externa, por ejemplo una memoria caché 102 de puerto o nacional o una memoria caché internacional 103, a través de Internet o de una red privada usando técnicas estándar. Para las memorias cachés externas 102,103, puede haber sincronización por redes para añadir datos a las memorias cachés.

La viabilidad de tal esquema de memoria caché, en particular para dispositivos desconectados, depende de los requisitos de almacenamiento para los datos recuperados del chip inteligente. Para demostrar la viabilidad, tómense por ejemplo los datos normalmente almacenados en un pasaporte electrónico EAC de la UE:

Imagen facial 20KB
Imágenes de huellas dactilares 15KB cada una (habitualmente dos)

Esto da un máximo normal de 50KB de datos por tenedor de pasaporte. Almacenar una base de datos biométricos cifrados para 200 millones de viajeros requerirá 50KB * 200 millones = 9,3 terabytes. En la práctica, la distribución de la frecuencia de viaje para los tenedores de pasaporte es muy sesgada. En consecuencia, el espacio disponible de memoria caché puede elegirse en función de los precios de almacenamiento y de otras inquietudes operativas, asignándose el espacio en la memoria caché a los usuarios más frecuentes. Hay abundantes algoritmos apropiados de población y sustitución de la memoria caché. Puede realizarse una introducción en la memoria caché en múltiples capas entre sistemas de inspección locales, puertos de entrada, regiones nacionales o incluso con cooperación internacional usando sincronización por redes.

Para sistemas de inspección portátiles que no puedan acceder a memoria cachés externas mediante conectividad inalámbrica, podría ponerse fácilmente una memoria caché local 101 de los datos biométricos cifrados de los 100.000 viajeros más frecuentes en una tarjeta de almacenamiento flash de 4GB.

Obsérvese de nuevo que la memoria caché no contiene ninguna información personalmente identificable y que, aunque contiene datos cifrados, una vez que la clave es descartada, estos datos son, efectivamente, borrados. Conceptualmente, los datos en sí ya no están retenidos en el sistema más de lo que lo estaría una copia en RAM de un dato biométrico una vez que se desconecte la corriente eléctrica de un PC.

Pueden usarse dos mecanismos adicionales para reducir los requisitos de almacenamiento de la memoria caché y para controlar la distribución y el uso de la memoria caché (en el supuesto caso de que el creador de una memoria caché no desease compartir los datos de su memoria caché). En primer lugar, cuando la cabeza de cada grupo de datos con control de acceso es leída para su inclusión en el procedimiento de deducción de clave de almacenamiento, no es preciso que esta cabeza esté incluida en la propia entrada de la memoria caché, ahorrando así varios cientos de bytes por registro biométrico (un ahorro pequeño como este se amplía cuando se almacenan registros para miles de millones de tenedores de pasaporte). También demuestra, además, la imposibilidad de recuperar los datos biométricos sin acceso al documento original, ya que falta por completo parte del mismo.

En segundo lugar, puede incorporarse una clave criptográfica secreta conocida únicamente a los sistemas válidos de inspección como entrada a la función de deducción de clave durante la construcción de entradas de memoria caché y tras la recuperación. Esto hace imposible que terceros obtengan aceleración accediendo a datos de la memoria caché sin operar un sistema de inspección autorizado.

Por último, ha habido cierta inquietud de que si las naciones precisan pasar a sistemas biométricos de diez huellas dactilares, aunque el DG3 tres puede almacenar fácilmente muchas más imágenes, hay que generar una comprobación aleatoria de todo el grupo de datos, no de partes individuales del mismo. Esto quiere decir que si un inspector solo desea leer las huellas dactilares de los dos dedos índice de un conjunto mayor, no puede garantizarse la integridad de estas imágenes sin leer todo el conjunto. Leer un conjunto de diez huellas dactilares a través de una

interfaz sin contactos podría llevar más de 60 segundos, por lo que las ventajas de la introducción en memoria caché en este contexto se amplían aún más.

La Figura 5 muestra los componentes del sistema de inspección. El sistema 10 de inspección comprende un procesador 50 acoplado a la memoria 52 de código y datos, un sistema 54 de entrada/salida (que comprende, por ejemplo, interfaces a la memoria caché de datos y/o interfaces para conectarse a la interfaz del chip inteligente) y a una interfaz 56 de usuario que comprende, por ejemplo, un teclado y/o un ratón. El código y/o los datos almacenados en la memoria 52 pueden ser proporcionados en un medio extraíble 58 de almacenamiento. En operación, los datos incluyen datos recogidos en los documentos de identidad electrónicos y el código comprende código para procesar estos datos para generar la memoria caché de datos, recuperar datos de la memoria caché y/o verificar el documento según el procedimiento mostrado en la Figura 6, descrita a continuación.

La Figura 6 muestra un diagrama de flujo de los diversos procedimientos que usan los sistemas descritos anteriormente. En la etapa S200, un documento electrónico es inspeccionado por el sistema y en la etapa 202 el sistema determina si esta es o no la primera vez que un documento ha sido inspeccionado. Si esta es la primera vez que el sistema ha visto este documento, se crea una memoria caché de datos segura según se define en las etapas S204 a S210. En la etapa S204, se leen todos los datos que han de ser almacenados en la memoria caché de datos. En la etapa S206, se crea usando parte de los datos leídos, por ejemplo usando el compendio del documento, una clave única para los datos que han de almacenarse. Los datos que han de almacenarse son entonces cifrados con esta clave única en la etapa S208. Los datos cifrados son almacenados en una memoria caché de datos en la etapa S210 y la clave única es descartada por el sistema. Según se ha explicado anteriormente, posteriormente los datos de la memoria caché únicamente pueden ser recuperados cuando el sistema está en presencia del documento electrónico original.

Si el sistema ha visto el documento (y almacenado información del documento en la memoria caché de datos) previamente, en la etapa S214 solo se leen del documento los datos requeridos para recalcular la clave única. En la etapa S216, se calcula la clave única a partir de estos datos leídos, y en la etapa S218, se descifran los datos de la memoria caché de datos usando esta clave. Así, los datos del documento electrónico son recuperados de la memoria caché y no del documento, por lo que se accede a los datos más rápidamente. El procedimiento de recuperación de datos de la memoria caché es definido, así, en las etapas S214 a S218.

Las etapas S212 y S220 muestran la etapa de verificación del documento y de su tenedor cuando se ve un documento por vez primera o en un momento posterior. En la etapa S212, el documento es verificado usando datos leídos del propio documento, mientras que, en cambio, en la etapa S220 el documento es verificado usando datos de la memoria caché en vez de procedentes del documento mismo. En ambos casos, sigue requiriéndose el documento original como parte del procedimiento de verificación, dado que no es posible acceder a los datos de la memoria caché sin el documento original para calcular la clave única.

La anterior descripción describe un mecanismo para introducir de forma segura en una memoria caché datos de tarjetas inteligentes en sistemas de inspección que leen datos almacenados en tarjetas inteligentes. El uso de tal mecanismo acelera tremendamente la velocidad de inspección de documentos de regreso sustituyendo la fase de transferencia de datos de la tarjeta inteligente con una consulta en la memoria caché. Debido a las características específicas de seguridad del mecanismo, la memoria caché no crea un riesgo de seguridad ni de privacidad. El mecanismo funciona encriptando los datos introducidos en la memoria caché con una clave deducida de datos de entropía elevada almacenados en el documento, y luego desechando la clave, de modo que la entrada de la memoria caché solo pueda ser descifrada en presencia del documento real.

Sin duda, a la persona experta se le ocurrirán muchas otras alternativas efectivas. Se entenderá que la invención no está limitada a las realizaciones descritas y que abarca modificaciones evidentes para los expertos en la técnica que se encuentren en el espíritu y el alcance de las reivindicaciones adjuntas a la presente memoria.

REIVINDICACIONES

1. Un procedimiento de introducción en memoria caché de datos de forma segura almacenados en un documento (32) de identidad electrónico, comprendiendo el procedimiento:

leer datos biométricos (34) de dicho documento electrónico;
usar la totalidad o parte de dichos datos biométricos para calcular una clave criptográfica única para dichos datos;
cifrar la totalidad o parte de dichos datos biométricos con dicha clave criptográfica única;
descartar dicha clave criptográfica única después del cifrado e
introducir dichos datos biométricos cifrados en una memoria caché de datos, requiriendo el descifrado de datos cifrados la presencia de dicho documento de identidad electrónico para recalcular dicha clave criptográfica única de dicho documento de identidad electrónico.

2. Un procedimiento según la reivindicación 1, en el que dicho documento de identidad electrónico comprende un compendio de datos y el procedimiento comprende el uso de la totalidad o de parte de dicho compendio de datos para calcular una clave criptográfica única para dichos datos biométricos.

3. Un procedimiento según la reivindicación 2, en el que dichos datos biométricos comprenden datos de información facial y/o de huellas dactilares y el procedimiento comprende el uso de la totalidad o de parte de dicho compendio de datos para calcular una clave criptográfica única para dichos datos de información facial y/o de huellas dactilares.

4. Un procedimiento según las reivindicaciones 2 o 3, en el que dicho documento de identidad electrónico comprende datos firmados digitalmente y datos biométricos en forma de imagen y el procedimiento comprende el cálculo de una clave criptográfica única para dicha imagen usando parte de dicha imagen y dichos datos firmados digitalmente.

5. Un procedimiento según una cualquiera de las reivindicaciones precedentes, que comprende el almacenamiento de dichos datos cifrados en la memoria caché con un identificador anónimo, por lo que dichos datos no son personalmente identificables en la memoria caché.

6. Un procedimiento de recuperación de datos biométricos almacenados como datos cifrados en una memoria caché de datos segura en el que dichos datos cifrados han sido creados llevando a cabo el procedimiento de una cualquiera de las reivindicaciones 1 a 5 precedentes, comprendiendo el procedimiento de recuperación de datos:

leer algunos datos biométricos de un documento de identidad electrónico;
usar la totalidad o parte de dichos datos biométricos leídos para recalcular una clave criptográfica única para dichos datos cifrados; y
recuperar datos biométricos almacenados como datos cifrados en una memoria caché segura creada usando el procedimiento de una cualquiera de las reivindicaciones 1 a 5 precedentes consultando dichos datos cifrados en dicha memoria caché de datos segura y descifrando dichos datos cifrados consultados usando dicha clave criptográfica única recalculada.

7. Un procedimiento de verificación de un documento de identidad electrónico, comprendiendo el procedimiento:

crear una memoria caché de datos segura llevando a cabo el procedimiento de una cualquiera de las reivindicaciones 1 a 5;
llevar a cabo el procedimiento de la reivindicación 6 para recuperar datos biométricos, mediante lo cual se aplica la etapa de la reivindicación 6 de recuperación de datos biométricos almacenados como datos cifrados en una memoria caché de datos segura a dicha memoria caché de datos segura creada; y
verificar dicho documento de identidad electrónico usando dichos datos biométricos recuperados.

8. Un soporte que lleva código de control de procesador para implementar, cuando se ejecuta, el procedimiento de una cualquiera de las reivindicaciones 1 a 7.

9. Un sistema de introducción en memoria caché para proporcionar una memoria caché (18, 101, 102, 103) de datos segura para los datos biométricos almacenados en un documento de identidad electrónico, comprendiendo el sistema de introducción en memoria caché:

una entrada configurada para recibir datos biométricos que han de ser introducidos en memoria caché a partir de un documento de identidad electrónico;
un procesador (28) configurado para:

usar la totalidad o parte de dichos datos biométricos recibidos para calcular una clave criptográfica única para dichos datos biométricos;
cifrar la totalidad o parte de dichos datos biométricos con dicha clave criptográfica única; y

descartar dicha clave criptográfica única después del cifrado y

una salida configurada para enviar dichos datos biométricos cifrados a una memoria caché de datos, requiriendo el descifrado de datos cifrados la presencia de dicho documento electrónico para recalcular dicha clave criptográfica única a partir de dicho documento de identidad electrónico, por lo cual dicha memoria caché de datos es segura.

10. Un sistema de introducción en memoria caché según la reivindicación 9, en el que dichos datos biométricos comprenden información facial y dicho sistema proporciona una memoria caché de datos segura para dicha información facial.

11. Un sistema de introducción en memoria caché según las reivindicaciones 9 o 10, en el que dichos datos biométricos comprenden datos de huellas dactilares y dicho sistema proporciona una memoria caché de datos segura para dichos datos de huellas dactilares.

12. Un sistema de recuperación de datos para recuperar datos biométricos almacenados como datos biométricos cifrados en una memoria caché de datos segura creada por el sistema de introducción en memoria caché de una cualquiera de las reivindicaciones 9 a 11, comprendiendo el sistema de recuperación de datos:

un sistema (10) de inspección para leer algunos datos biométricos de un documento de identidad electrónico; y
un procesador configurado para:

usar la totalidad o parte de dichos datos biométricos leídos para recalcular una clave criptográfica única para dichos datos;
consultar datos biométricos cifrados en dicha memoria caché de datos segura; y
descifrar dichos datos biométricos cifrados consultados usando dicha clave criptográfica única recalculada para obtener datos biométricos.

13. Un sistema de verificación para verificar un documento de identidad electrónico, comprendiendo el sistema de verificación:

una memoria caché (18, 101, 102, 103) de datos segura creada por el sistema de introducción en memoria caché según una cualquiera de las reivindicaciones 9 a 11;
un sistema de recuperación de datos según la reivindicación 12 para recuperar datos biométricos; y
un medio de verificación configurado para verificar dicho documento de identidad electrónico usando datos biométricos recuperados por dicho sistema de recuperación de datos.

14. Un sistema de verificación según la reivindicación 13, en forma de dispositivo portátil.

15. Un sistema de verificación según las reivindicaciones 13 o 14, en el que dicha memoria caché (102, 103) de datos segura está alejada de dicho procesador y dicho sistema de verificación comprende una conexión inalámbrica entre dicho procesador y dicha memoria caché de datos segura.

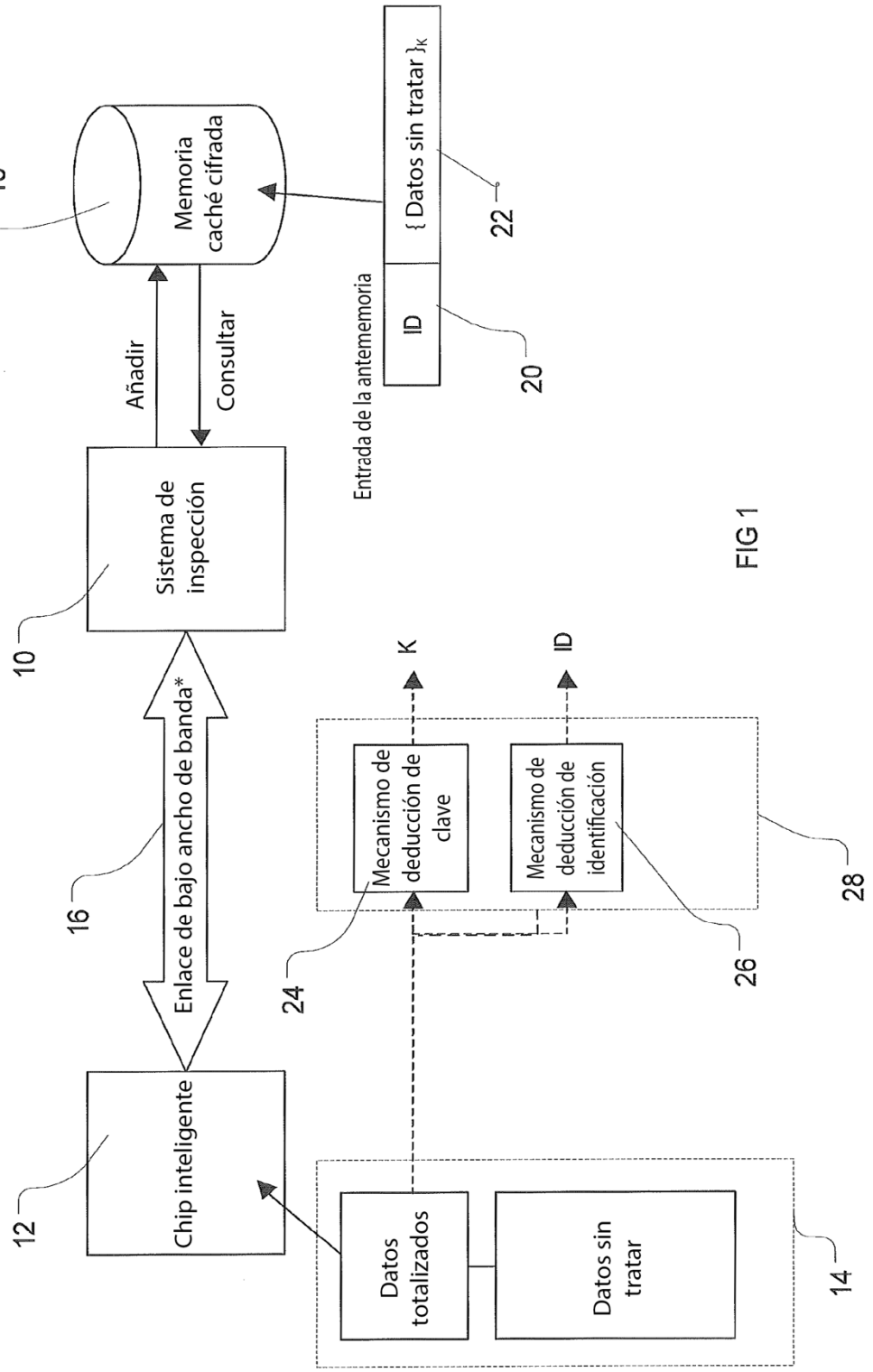
18
Memoria caché cifrada
{ Datos sin tratar }K
22
Entrada de la antememoria
ID
20
Añadir
Consultar
Sistema de inspección
10
Enlace de bajo ancho de banda*
16
Chip inteligente
12
K
ID
Mecanismo de deducción de clave
Mecanismo de deducción de identificación
24
26
28
Datos totalizados
Datos sin tratar
14

FIG 1

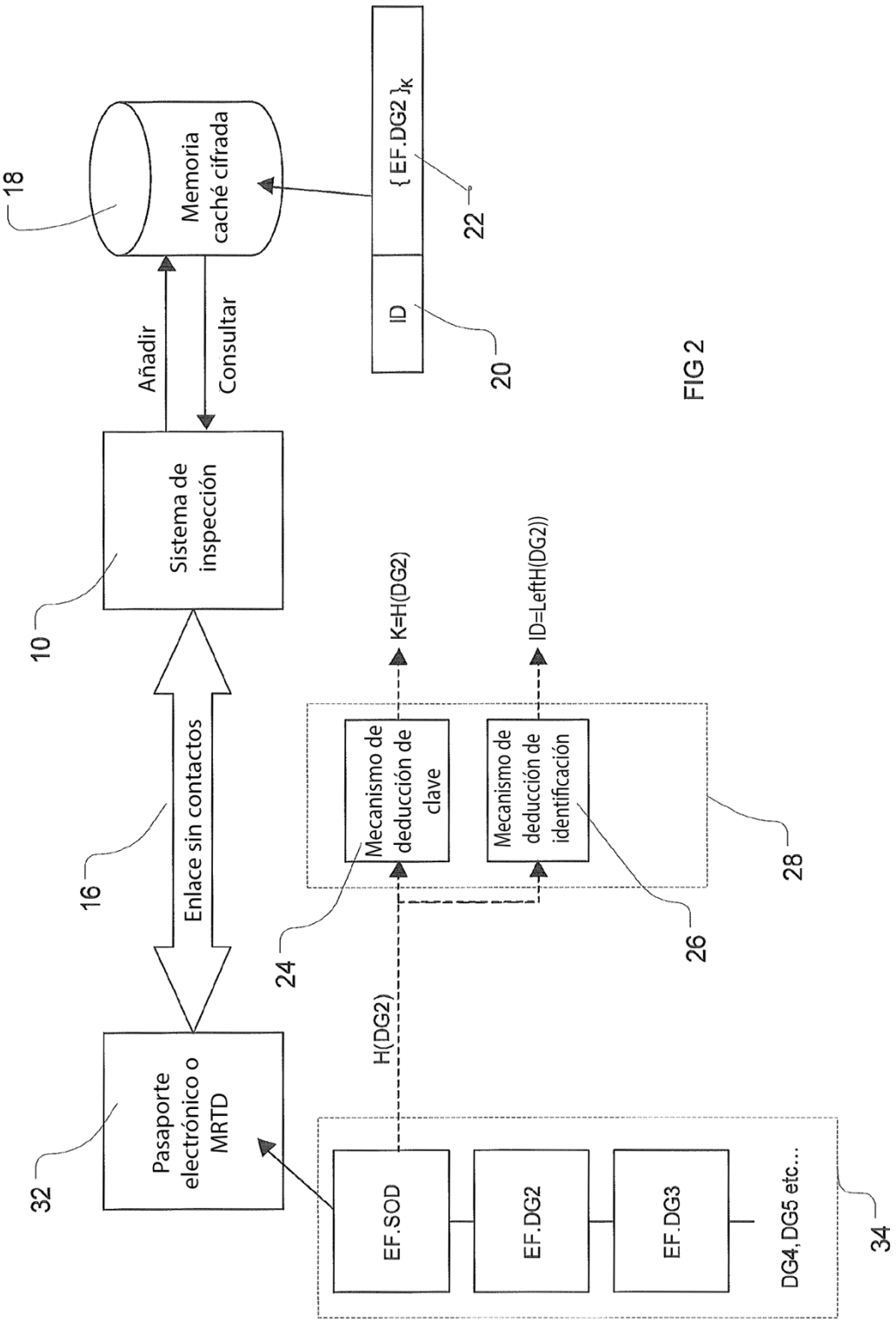
18
Memoria caché cifrada
{ EF.DG2 }K
22
ID
20
Añadir
Consultar
Sistema de inspección
10
16
Enlace sin contactos
Pasaporte electrónico o MRTD
32
K=H(DG2)
ID=LeftH(DG2))
Mecanismo de deducción de clave
Mecanismo de deducción de identificación
28
24
26
H(DG2)
EF.SOD
EF.DG2
EF.DG3
DG4, DG5 etc...
34

FIG 2

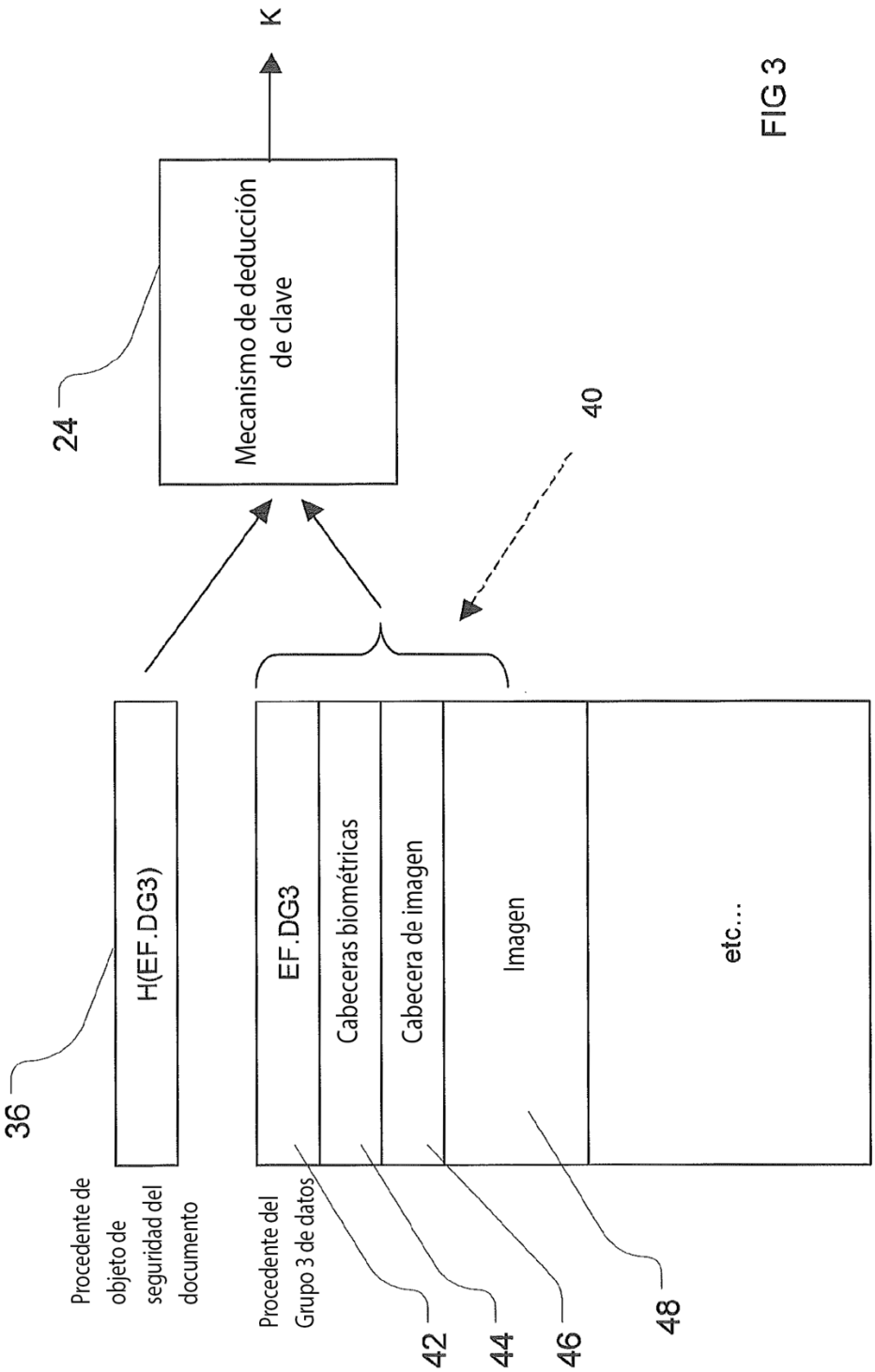
K
Mecanismo de deducción de clave
24
40
H(EF.DG3)
36
EF.DG3
Cabeceras biométricas
Cabecera de imagen
Imagen
etc...
Procedente de objeto de seguridad del documento
Procedente del Grupo 3 de datos
42
44
46
48

FIG 3

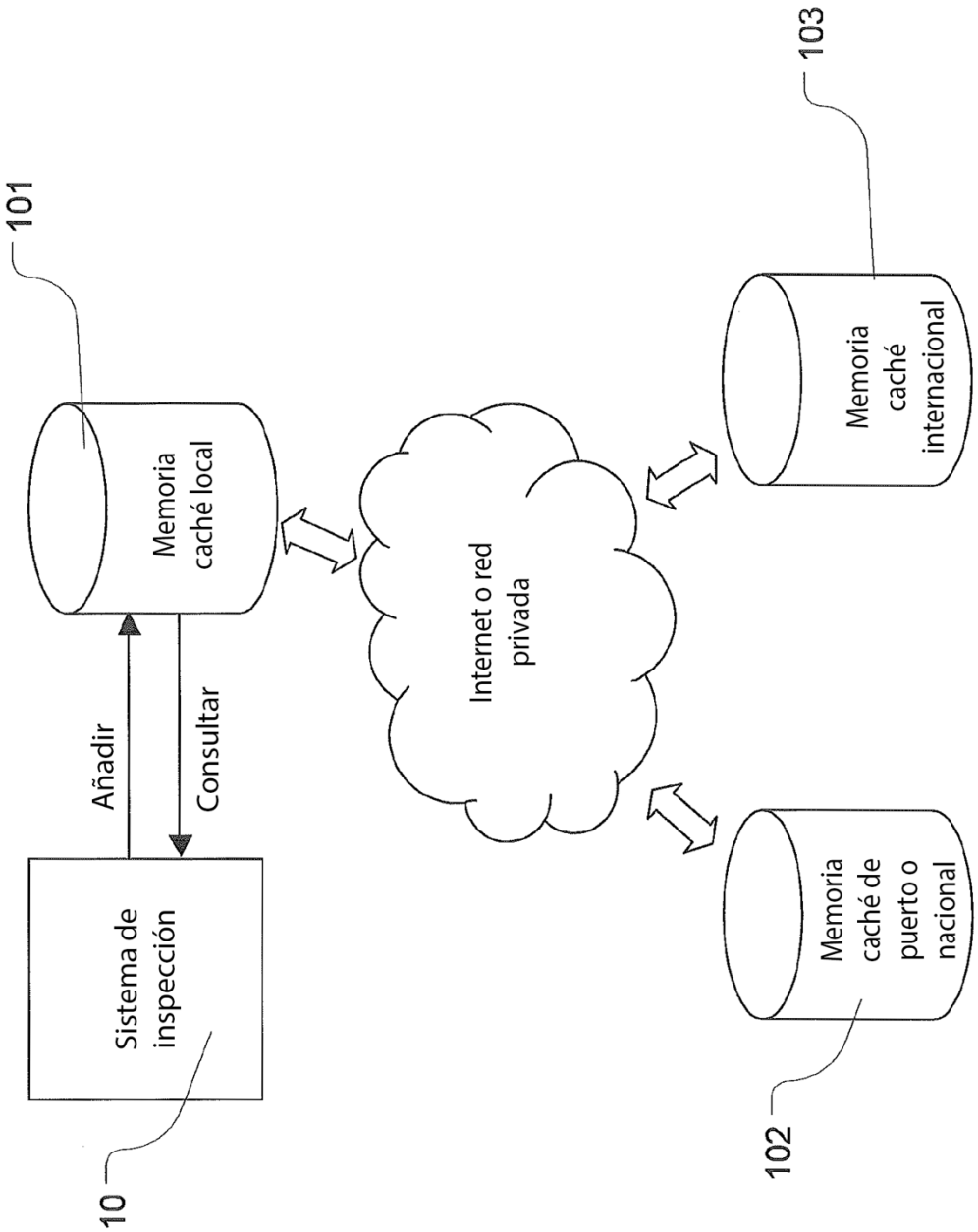
101
Memoria caché local
Añadir
Consultar
Sistema de inspección
10
Internet o red privada
103
Memoria caché internacional
Memoria caché de puerto o nacional
102

FIG 4

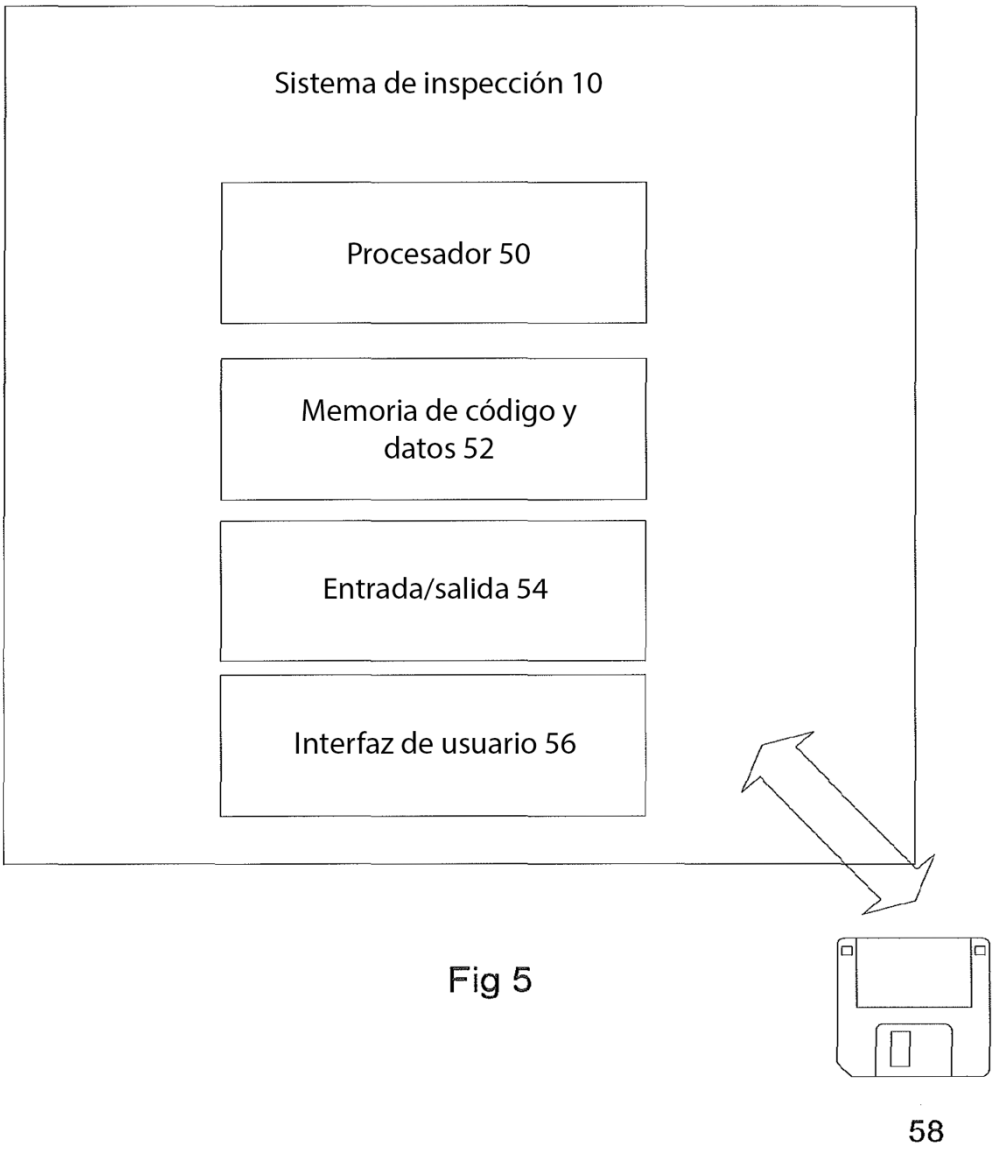
Sistema de inspección 10
Procesador 50
Memoria de código y datos 52
Entrada/salida 54
Interfaz de usuario 56
58

Fig 5

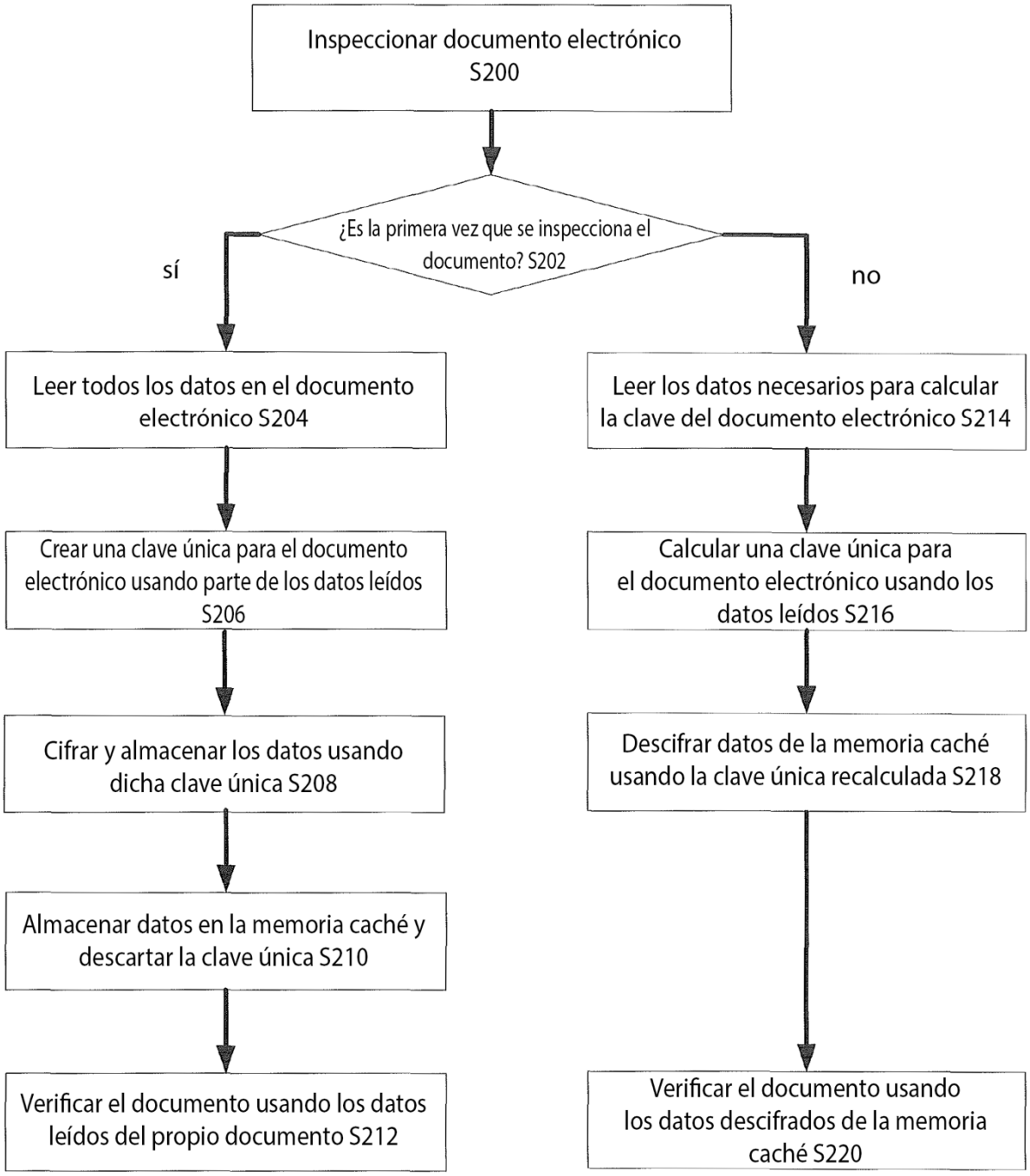
Inspeccionar documento electrónico S200
¿Es la primera vez que se inspecciona el documento? S202
sí
no
Leer todos los datos en el documento electrónico S204
Crear una clave única para el documento electrónico usando parte de los datos leídos S206
Cifrar y almacenar los datos usando dicha clave única S208
Almacenar datos en la memoria caché y descartar la clave única S210
Verificar el documento usando los datos leídos del propio documento S212
Leer los datos necesarios para calcular la clave del documento electrónico S214
Calcular una clave única para el documento electrónico usando los datos leídos S216
Descifrar datos de la memoria caché usando la clave única recalculada S218
Verificar el documento usando los datos descifrados de la memoria caché S220

Fig 6