(19) OFICINA ESPAÑOLA DE PATENTES Y MARCAS

ESPAÑA

(11) Número de publicación: **2 440 826**

(51) Int. CI.:

G06F 21/00 (2013.01)

(12) TRADUCCIÓN DE PATENTE EUROPEA T3

(96) Fecha de presentación y número de la solicitud europea: **08.08.2003 E 11195693 (4)**

(97) Fecha y número de publicación de la concesión europea: **02.10.2013 EP 2442204**

(54) Título: **Sistema y procedimiento para delegación de privilegios y control**

(30) Prioridad:

15.08.2002 US 218642

(45) Fecha de publicación y mención en BOPI de la traducción de la patente:
30.01.2014

(73) Titular/es:

ACTIVIDENTITY, INC. (100.0%)
6623 Dumbarton Circle
Fremont, CA 94555, US

(72) Inventor/es:

LE SAINT, ERIC F.

(74) Agente/Representante:

CURELL AGUILÁ, Mireia

DESCRIPCIÓN

Sistema y procedimiento para delegación de privilegios y control.

Campo de la invención

La presente invención se refiere en general a un sistema y un procedimiento de procesamiento de datos y más particularmente a un sistema y un procedimiento para delegar privilegios de uno o más testigos de seguridad a una o más unidades de procesamiento de datos.

Antecedentes

La solicitud de patente de Estados Unidos US 2002/0099952 A1 da a conocer un sistema y un procedimiento que controla de forma automática, transparente y segura la ejecución del software mediante la identificación y la clasificación del software y la localización de una regla y nivel de seguridad asociado para ejecutar software ejecutable. El nivel de seguridad puede denegar la ejecución del software, restringir su ejecución en cierta medida o permitir su ejecución sin restricciones. Para restringir software, puede calcularse un testigo de dirección restringida que reduzca el acceso del software a los recursos y/o elimine privilegios, en relación con un testigo de acceso normal del usuario. En la página 4, párrafo [0038] de este documento, se explica que "cuando un usuario inicia una sesión en una máquina o red segura [...] y se autentica, se configura un entorno de ejecución (contexto) para el usuario, que comprende la creación de un testigo de acceso".

La patente US n.º 5.649.099 da a conocer un procedimiento en el que unos programas de control de acceso (ACP) permiten la delegación controlada de los derechos de acceso de los clientes a unos intermediarios no fiables. Los ACP son programas que codifican especificaciones arbitrarias de derechos de acceso delegados. En la col. 2, líneas 41 y ff., se explica que "los sistemas de capacidades se basan en los testigos de capacidades que los servidores entregan a los clientes".

Por lo tanto, ambos documentos dan a conocer testigos generados mediante software.

La delegación de privilegios ofrece la posibilidad de permitir que otro actúe como sustituto del delegante. Hay una serie de estrategias diferentes relevantes para la realización del procedimiento de delegación. Por ejemplo, la patente US nº 5.339.403 concedida a Parker, describe un certificado de atributos de privilegios expedido por un servidor de autenticación para permitir a un cliente acceder a recursos distribuidos. En un segundo ejemplo, la patente US nº 5.918.228 concedida a Rich *et al.* describe un certificado de atributos de privilegios utilizado para "suplantar" a un cliente en otros servidores basados en la web. Un primer servidor web genera y expide el certificado de atributos de privilegios y lo presenta a otros servidores como un medio para "suplantar" a un cliente con finalidades de acceso. Una forma muy común de delegación de privilegios diseñada para redes que emplean protocolos TCP/IP es la del protocolo denominado Kerberos.

El protocolo Kerberos autentica la identidad de los usuarios que tratan de iniciar una sesión en una red y comprende mensajería segura basada en procedimientos de criptografía simétrica. Kerberos concede "tickets" a los usuarios a título de credenciales, que luego estos utilizarán para identificarse ante otros proveedores de servicios de red. Cada ticket comprende información que permite a otro proveedor de servicios de red determinar que el usuario se ha autenticado correctamente, de manera análoga a un certificado de atributos de privilegios. El ticket adecuado se presenta automáticamente al proveedor de servicios de red como un medio para evitar tener que someterse a diversos procedimientos de autenticación cada vez que se desee acceder a un nuevo servicio de red.

En los ejemplos citados, los servidores que expiden los certificados o tickets de atributos de privilegios son los encargados de la generación y el control de estos, en lugar de la persona que utiliza el sistema. La persona que utiliza el sistema debe, por consiguiente, confiar en las estrategias de delegación empleadas en el sistema. En segundo lugar, los sistemas basados en servidor tal vez no aporten suficiente flexibilidad al procedimiento de delegación cuando los criterios de delegación necesarios se basan en una función o en una regla en lugar de una identidad. Por último, los certificados de atributos de privilegios empleados en la correspondiente técnica son vulnerables en cierta medida a los ataques por personas o entidades que tienen acceso a los servidores que generan el certificado.

Por las anteriores razones, es necesario incorporar un mecanismo de delegación de privilegios flexible en uno o más testigos de seguridad mediante el cual el titular del testigo de seguridad tenga un mayor control sobre la emisión y el uso de los privilegios delegables.

Sumario

Según la presente invención, se ofrece un sistema de delegación de privilegios según las reivindicaciones 1, 14, 21 o 28 y un procedimiento para delegar un privilegio según la reivindicación 16.

La presente invención va dirigida a un sistema y un procedimiento de delegación de privilegios que aportan flexibilidad y control sobre la emisión y el uso de los privilegios delegables. La presente invención comprende un testigo de seguridad dotado de la capacidad de transferir privilegios delegables y atributos asociados a otro testigo de seguridad o sistema informático, ambos de los cuales se describen genéricamente en la presente memoria como unidades de procesamiento de datos. Se dan a conocer diversas formas de realización que comprenden un privilegio dividido que permite el acceso a un recurso controlado cuando se combina con todos los componentes para formar un privilegio completo.

La unidad de procesamiento de datos receptora comprende la capacidad operativa de almacenar y utilizar el privilegio delegado y efectuar intercambios de datos con el testigo de seguridad y, opcionalmente, con por lo menos una segunda unidad de procesamiento de datos. Se llevan a cabo autenticaciones mutuas entre el testigo de seguridad delegante y la unidad de procesamiento de datos receptora antes de que se transfiera el privilegio delegado.

La información que se puede comunicar en el intercambio de datos comprende datos de autenticación, uno o más privilegios delegados y los atributos asociados. Se utiliza un protocolo de mensajería segura durante los intercambios de datos. Los privilegios delegables comprenden un certificado de atributos de privilegios, un componente de clave, una clave criptográfica, un ticket digital, unas credenciales digitales, una contraseña, una plantilla biométrica, unos derechos digitales, una licencia o un crédito de fidelización.

Los usos comunes para los privilegios delegados comprenden autenticar, activar un terminal, personalizar un dispositivo inteligente, acceder a los recursos contenidos en la segunda unidad de procesamiento de datos u otra unidad de procesamiento de datos o accesibles a través de estas, permitir que la segunda unidad de procesamiento de datos u otra unidad de procesamiento de datos actúen como sustitutos del testigo de seguridad delegante y gestionar el crédito de fidelización. Los atributos contenidos en el certificado de atributos de privilegios o en el archivo separado definen el alcance de uso y los aspectos de seguridad necesarios para utilizar el privilegio delegado. Cuando los atributos están contenidos en el archivo separado, se añade una referencia cruzada comprobable al privilegio asociado.

Los atributos asociados al privilegio delegado facilitan suficiente información a la unidad de procesamiento de datos receptora para configurar el privilegio y aplicar los aspectos del control indicados en los atributos, que comprenden las políticas de seguridad y el estado del privilegio delegado. Las políticas de seguridad comprenden detalles relacionados con el período de validez, el número de usos restantes, los límites de tiempo y las medidas criptográficas que deben aplicarse. El estado de privilegio delegado comprende los requisitos de almacenamiento (transitorio o permanente) y el estado del sistema principal (inactivo, en arranque, modo seguro, modo inseguro, suspendido.) Los aspectos de control determinan cuándo debe activarse o destruirse el privilegio. Otro tipo de información contenida en los atributos comprende información operativa, tal como nombre de usuario, ID de usuario, nombre de dominio, nombre de cliente o nombre de sistema principal.

A continuación, se ilustran algunas ventajas de la presente invención a título de ejemplo. La delegación y control de privilegios pueden aplicarse al mantenimiento de la privacidad del historial médico de una persona. El historial médico de un paciente debería ser accesible solo para las personas autorizadas o "con privilegio" de acceso al historial. A fin de acceder al historial médico de un paciente, un terminal se activa transfiriendo de forma segura un privilegio tras las autenticaciones mutuas entre el testigo de seguridad de un médico y el testigo de seguridad asociado con el terminal. El privilegio completo puede transferirse desde el testigo de seguridad del médico o crearse combinando la información transferida con la información preexistente contenida en el testigo de seguridad del terminal. El privilegio delegado del médico permite la activación del terminal para leer el historial médico de un paciente almacenado en el testigo de seguridad del paciente o accesible de alguna manera mediante la información almacenada en el mismo.

Los atributos asociados al privilegio delegado pueden limitar la activación del terminal a las horas de consulta normales del médico y/o especificar que el privilegio delegado permanece en memoria transitoria únicamente. Los atributos pueden proporcionar también la capacidad de delegar privilegios a otro médico mientras el primer médico está de vacaciones. Para acceder al historial médico de un paciente, el paciente presenta su testigo de seguridad al terminal. Entonces, se inicia una sesión de autenticación en la que se verifica, para el testigo de seguridad del paciente, la presencia de los privilegios necesarios en el testigo de seguridad del terminal para permitir al terminal acceder al historial médico del paciente. El gerente de la misma consulta podría tener un privilegio delegable necesario para activar el mismo terminal a fin de examinar los saldos asociados al paciente, pero carecer del privilegio delegable necesario para examinar el historial médico del paciente. En una primera alternativa al uso del sistema de clave maestra dividida, se utiliza una clave maestra simétrica completa que se instala en todos los testigos de seguridad de autorización basados en función equivalentes al ejemplo de nivel de médico descrito anteriormente. En esta alternativa, se transfiere la clave maestra completa al testigo de seguridad asociado con el terminal, en lugar de un componente de la clave. Los demás aspectos de la segunda forma de realización de la presente invención son iguales. Las claves simétricas de cualquiera de los dos sistemas pueden basarse en algoritmos compatibles con la norma de encriptación de datos (DES), norma de encriptación de datos triple (3DES), norma de encriptación avanzada (AES), etc.

Una segunda alternativa al uso del sistema de clave dividida conlleva el uso de claves de infraestructura de clave pública (PKI). En esta alternativa, la autoridad expedidora genera una clave privada de grupo que representa un privilegio particular y la instala en todos los testigos de seguridad de autorización basados en función equivalentes al ejemplo de nivel de médico descrito anteriormente. La clave pública equivalente a la clave privada de grupo se instala asimismo en todos los testigos de seguridad de nivel de paciente equivalentes al testigo de seguridad de paciente descrito anteriormente. Las claves PKI pueden basarse en algoritmos que utilizan curvas elípticas, RSA, Diffie-Hellman, Pretty Good Privacy (PGP), El Gamal, etc. En todas las formas de realización que conllevan transferencias de claves criptográficas, deberían realizarse autenticaciones mutuas entre la los testigos de seguridad delegantes y delegados para evitar la divulgación no autorizada de las claves criptográficas. La autenticación del terminal por la unidad de procesamiento de datos del paciente es suficiente para utilizar los privilegios transferidos.

Breve descripción de los dibujos

La descripción detallada considerada conjuntamente con las figuras siguientes permitirá alcanzar una comprensión más completa de la presente invención.

La figura 1 es un diagrama de bloques del sistema generalizado para implementar la forma de realización principal de la presente invención.

La figura 1A es un diagrama de bloques detallado que representa un ciclo de autenticación mutua entre un testigo de seguridad y una primera unidad de procesamiento de datos.

La figura 1B es un diagrama de bloques detallado que representa la delegación de privilegios que comprende atributos asociados de un testigo de seguridad a una primera unidad de procesamiento de datos.

La figura 1C es un diagrama de bloques detallado que representa la verificación de privilegios por parte de una segunda unidad de procesamiento de datos.

La figura 1D es un diagrama de bloques detallado que representa el uso de privilegios por la primera unidad de procesamiento de datos, por medio del cual se accede a un ejemplo de recurso de una segunda unidad de procesamiento de datos mediante el privilegio delegado.

La figura 1E es un diagrama de bloques detallado que representa un privilegio existente contenido en una primera unidad de procesamiento de datos que presenta un atributo caducado.

La figura 1F es un diagrama de bloques detallado que representa la sustitución del atributo caducado asociado con el privilegio existente.

La figura 1G es un diagrama de bloques detallado que representa una variante de la primera forma de realización inventiva.

La figura 1H es un diagrama de bloques detallado que representa una transferencia de un privilegio parcial desde el testigo de seguridad hasta la primera unidad de procesamiento de datos.

La figura 1I es un diagrama de bloques detallado que representa la transferencia del privilegio parcial desde la primera unidad de procesamiento de datos hasta la segunda unidad de procesamiento de datos.

La figura 1J es un diagrama de bloques detallado que representa los privilegios parciales combinados dentro de la segunda unidad de procesamiento de datos y el acceso a un recurso controlado.

La figura 1K es un diagrama de bloques detallado que representa una variante de la primera forma de realización inventiva, en la que el segundo privilegio parcial es transferido desde la segunda unidad de procesamiento de datos hasta la primera unidad de procesamiento de datos.

La figura 1L es un diagrama de bloques detallado que representa los privilegios parciales combinados dentro de la primera unidad de procesamiento de datos y el acceso a un recurso controlado.

La figura 2 es un diagrama de bloques generalizado que representa una forma de realización alternativa de la presente invención, en la que se utilizan componentes de clave simétrica como forma de privilegio delegable.

La figura 2A es un diagrama de bloques detallado que representa un ciclo de autenticación mutua entre una primera y una segunda unidad de procesamiento de datos.

La figura 2B es un diagrama de bloques detallado que representa la delegación de privilegios desde la primera unidad de procesamiento de datos hasta la segunda unidad de procesamiento de datos, mediante un protocolo de

mensajería segura y la regeneración de la clave maestra simétrica.

La figura 2C es un diagrama de bloques detallado que representa un identificador exclusivo enviado desde una tercera unidad de procesamiento de datos a la unidad de procesamiento de datos como parte de una prueba de autenticación.

La figura 2D es un diagrama de bloques detallado que ilustra la diversificación de clave maestra mediante el identificador exclusivo para generar una clave específica para la unidad de procesamiento de datos necesaria para acceder a los recursos controlados por la tercera unidad de procesamiento de datos.

La figura 2E es un diagrama de bloques detallado que representa la respuesta a la prueba de autenticación que comprende el uso de la clave específica para la unidad de procesamiento de datos.

La figura 2F es un diagrama de bloques detallado que representa el acceso a los recursos controlados por la tercera unidad de procesamiento de datos tras la autentificación de la segunda unidad de procesamiento de datos por la tercera unidad de procesamiento de datos.

La figura 3 es un diagrama de bloques generalizado que representa una forma de realización alternativa de la presente invención, en la que se utiliza una clave simétrica completa como forma de privilegio delegable.

La figura 3A es un diagrama de bloques detallado que representa un ciclo de autenticación mutua entre una primera unidad de procesamiento de datos y una segunda unidad de procesamiento de datos.

La figura 3B es un diagrama de bloques detallado que representa la delegación de privilegios desde la primera unidad de procesamiento de datos hasta la segunda unidad de procesamiento de datos, mediante un protocolo de mensajería segura.

La figura 4 es un diagrama de bloques generalizado que representa una forma de realización alternativa de la presente invención, en la que se utiliza una clave privada de grupo asimétrica como forma de privilegio delegable.

La figura 4A es un diagrama de bloques detallado que representa un ciclo de autenticación mutua entre una primera unidad de procesamiento de datos y una segunda unidad de procesamiento de datos.

La figura 4B es un diagrama de bloques detallado que representa la delegación de privilegios y sus atributos asociados desde la primera unidad de procesamiento de datos hasta la segunda unidad de procesamiento de datos, mediante un protocolo de mensajería segura.

La figura 4C es un diagrama de bloques detallado que representa una prueba de autenticación enviada desde una tercera unidad de procesamiento de datos a la segunda unidad de procesamiento de datos, mediante una clave pública equivalente a la clave de grupo privada.

La figura 4D es un diagrama de bloques detallado que representa la respuesta a la prueba de autenticación que comprende el uso de la clave privada de grupo.

La figura 4E es un diagrama de bloques detallado que representa el acceso a los recursos controlados por la tercera unidad de procesamiento de datos tras la autentificación de la segunda unidad de procesamiento de datos por la tercera unidad de procesamiento de datos.

La figura 5 es un diagrama de flujo simplificado que ilustra las etapas implicadas en la implementación de la forma de realización principal de la presente invención.

La figura 6 es una tabla que ofrece un sumario de los tipos de privilegios delegables y la información contenida en los atributos asociados.

Descripción detallada

La presente invención ofrece nuevas implementaciones en la delegación de privilegios y los atributos asociados desde un testigo de seguridad hasta una o más unidades de procesamiento de datos. Para los propósitos de la presente invención, se presupone que el testigo de seguridad y las unidades de procesamiento de datos comprenden módulos, algoritmos y servicios de criptografía normalizados.

El término "unidad de procesamiento de datos" se refiere a un testigo de seguridad, un dispositivo inteligente o un sistema informático, según el caso. El término testigo de seguridad se refiere a los dispositivos de seguridad basados en hardware, tales como las tarjetas inteligentes, las tarjetas de circuitos integrados, los módulos de identificación de abonado (SIM), los módulos de identificación inalámbrica (WIM), los testigos de identificación, los módulos de aplicación segura (SAM), los módulos de seguridad de hardware (HSM), las tarjetas multimedia seguras

(SMMC) y dispositivos similares. Los términos unidad de procesamiento de datos y testigo de seguridad se utilizan indistintamente en la memoria y no implican ninguna limitación de uso.

Con referencia a la figura 1, se representan los componentes y las interrelaciones más importantes para implementar la forma de realización principal de la presente invención. Se representa un testigo de seguridad 10 conectado funcionalmente 12 al ordenador de un cliente 15. El ordenador del cliente 15 establece comunicaciones de proceso 65 con una primera unidad de procesamiento de datos DPU1 40. El ordenador del cliente 15 ofrece las interfaces de hardware y software necesarias para permitir al testigo de seguridad 10 comunicarse con la primera unidad de procesamiento de datos DPU1 40, pero por lo demás no afecta a las diversas formas de realización de la presente invención descritas en la presente memoria. El testigo de seguridad 10 comprende por lo menos un privilegio delegable P 20 y sus atributos asociados A 30.

El privilegio delegable P 20 puede utilizarse para autenticar, activar un terminal, personalizar un dispositivo inteligente, acceder a los recursos 60 contenidos en la segunda unidad de procesamiento de datos DPU2 50 u otra unidad de procesamiento de datos o accesibles a través de estas, permitir que la segunda unidad de procesamiento de datos DPU2 50 u otra unidad de procesamiento de datos actúe como sustituto del testigo de seguridad delegante 10 o gestionar los créditos de fidelización.

Los atributos A 30 asociados con el privilegio delegado P 20 facilitan suficiente información a una unidad de procesamiento de datos receptora para configurar el privilegio P 20 y aplicar aspectos de control indicados en los atributos A 30 que comprenden las políticas de seguridad y el estado del privilegio delegado. Las políticas de seguridad comprenden detalles relacionados con el período de validez, el número de usos restantes, los límites de tiempo y las medidas criptográficas que deben emplearse.

El estado del privilegio delegado comprende los requisitos de almacenamiento (transitorio o permanente) y el estado del sistema principal (inactivo, en arranque, modo seguro, modo inseguro, suspendido.) Los aspectos de control determinan cuándo debe activarse o destruirse el privilegio. Otro tipo de información contenida en los atributos A 30 comprende información operativa, tal como nombre de usuario, ID de usuario, nombre de dominio, nombre de cliente o nombre de sistema principal. La tabla de la figura 6 ofrece un sumario de los tipos de privilegios delegables y la información contenida en los atributos asociados.

Los atributos A 30 se asocian con el privilegio P 20 mediante una firma exclusiva, un código hash o de autenticación de mensaje o una autenticación de mensaje generado por hash que enlaza de manera inequívoca los atributos 30 con el privilegio 20. Los atributos A 30 normalmente se almacenan por separado de los privilegios 20, excepto cuando se incluyen en forma de certificado (por ejemplo, tickets digitales, derechos digitales o certificados de licencia o de atributos de privilegio).

La primera unidad de procesamiento de datos DPU1 40 establece comunicaciones de proceso 65 con la segunda unidad de procesamiento de datos DPU2 50. La segunda unidad de procesamiento de datos DPU2 50 60 comprende el recurso 60 que solo es accesible mediante el privilegio válido P 20. El recurso 60 se define genéricamente de tal forma que comprenda los datos o las funciones contenidas en la segunda unidad de procesamiento de datos DPU2 50 o accesibles desde otra unidad de procesamiento de datos mediante el recurso 60. Los enlaces de comunicación 65 y 85 pueden ser conexiones locales, conexiones de red remota o cualquier combinación de estas.

Con referencia a la figura 1A, se inicia un ciclo de autenticación mutua de prerrequisitos 70 antes de la transferencia de privilegios. La autenticación mutua 70 se prefiere como medio para asegurar que tanto la unidad de procesamiento de datos emisora como la unidad de procesamiento de datos receptora estén autorizadas para realizar transacciones de transferencia de privilegios. En la figura 1B, una vez que el ciclo de autenticación mutua se ha realizado con éxito, se establece un canal seguro entre el testigo de seguridad 10 y la primera unidad de procesamiento de datos DPU1 40.

El canal seguro 75 puede implementarse mediante protocolos de mensajería segura, tales como los de encriptación de capa de conexión segura (SSL), seguridad de capa de transporte (TLS) o IPsec. El privilegio P 20 y sus atributos asociados A 30 se envían de forma segura 65 a través del canal seguro 75 y se almacenan dentro de la primera unidad de procesamiento de datos DPU1 conforme a los aspectos de control especificados por los atributos A' 30'. (El privilegio P' 20' y el atributo asociado A' 30' aparecen con apóstrofos para indicar una copia duplicada de los originales.)

En la figura 1C, la primera unidad de procesamiento de datos DPU1 40 se autentifica a sí misma ante la segunda unidad de procesamiento de datos DPU2 50, y se establece un canal seguro 80. El privilegio P" 20" se envía de forma segura 85 a la segunda unidad de procesamiento de datos DPU2 50 donde se valida 90. El acceso y el uso 95 del recurso 60 se representa en la figura 1D.

En la figura 1E, se representa un privilegio P' 20' y sus atributos asociados A'x 30'. Los atributos A'x 30' comprenden un parámetro que ha expirado (por ejemplo, período de validez). A fin de utilizar el privilegio, se requiere una

actualización. Los atributos actualizados A" 30" se envían de forma segura desde el testigo de seguridad 10 a la primera unidad de procesamiento de datos DPU1 40, donde los atributos expirados A'x 30' se sustituyen por los atributos actualizados A"x 30" tal como se representa en la figura 1F.

Con referencia a la figura 1G, se representa un privilegio parcial p/ln 22 y sus atributos asociados A 30 almacenados inicialmente dentro del testigo de seguridad 10. Se representan una parte restante del privilegio p2/n 22' y sus atributos asociados A 30' almacenados dentro de un segundo testigo de seguridad 50. En esta forma de realización de la presente invención, es necesario combinar los privilegios parciales p1/n 22 y p2/n 22' a fin de obtener acceso a un recurso 60. El inventor prevé que el testigo de seguridad 10 o la segunda unidad de procesamiento de datos 50 puedan delegar los atributos A 30 y A' 30' o combinarlos para formar un conjunto completo de atributos. El inventor prevé también la posibilidad de combinar más de dos privilegios parciales para formar un privilegio utilizable.

Con referencia a la figura 1H, se representa cómo el privilegio parcial p1/n 22 y sus atributos asociados A' 30 se delegan 12 desde el testigo de seguridad 10 a 65 una primera unidad de procesamiento de datos DPU1 40 a través de un cliente 15. La delegación comprende un canal seguro 75 para impedir el seguimiento indebido de la transacción.

En la figura 1I, se representa cómo se delegan 85 nuevamente el privilegio parcial p1/n 22 y sus atributos asociados A 30 desde la primera unidad de procesamiento de datos DPU1 40 hasta la segunda unidad de procesamiento de datos DPU2 50 mediante un canal seguro 95. Continuando con la figura 1J, los privilegios parciales combinados p1/n 22 y p2/n 22' forman un privilegio completo P 24 que comprende un conjunto completo de atributos asociados A 32 y permite a la segunda unidad de procesamiento de datos DPU2 50 acceder al recurso controlado 60.

En la figura 1K, se representa una forma de realización equivalente, en la que se muestra cómo se delegan 85 el privilegio parcial p2/n 22' y sus atributos asociados A' 30' desde la segunda unidad de procesamiento de datos DPU2 50 hasta la primera unidad de procesamiento de datos DPU1 40 mediante un canal seguro 95. Continuando con la figura 1L, los privilegios parciales combinados p1/n 22 y p2/n 22' forman un privilegio completo P 24 que comprende un conjunto completo de atributos asociados A 32, que permite a la primera unidad de procesamiento de datos DPU1 40 acceder al recurso controlado 60'. Se representa cómo el recurso controlado 60' es transferido desde la segunda unidad de procesamiento de datos DPU2 50, con el único propósito de mantener la coherencia con los dibujos anteriores. El recurso controlado 60 podría permanecer en la segunda unidad de procesamiento de datos DPU2 50 y ser accesible mediante el enlace de comunicaciones 85.

Con referencia a la figura 2, se representan los componentes e interrelaciones más importantes para implementar otra forma de realización de la presente invención. En esta forma de realización de la presente invención, la delegación de privilegios se realiza por medio de claves criptográficas simétricas. Se representa un sistema informático 202 conectado funcionalmente a un primer testigo de seguridad 204 y un segundo testigo de seguridad 206. Un programa de intermediación (middleware), no representado e instalado en el sistema informático 202, admite el uso de dos o más unidades de procesamiento de datos. Se describe un ejemplo del anterior programa en el documento "Government Smart Card Interoperability Specification Contract Modification", número de contrato GS00T00ALD0208 PS02, 29 de agosto de 2000.

Los procedimientos de criptografía simétrica empleados en la presente forma de realización de la presente invención pueden basarse en algoritmos compatibles con la norma de encriptación de datos (DES), norma de encriptación de datos triple (3DES) o la norma de encriptación avanzada (AES).

Para llevar a la práctica la presente forma de realización de la presente invención, una autoridad de expedición genera inicialmente una clave maestra asociada con un privilegio particular. Pueden utilizarse claves maestras separadas para definir un determinado privilegio de un grupo seleccionado de entre unidades de procesamiento de datos. A continuación, la clave maestra se diversifica de forma secuencial con identificadores exclusivos asociados a un grupo predefinido de testigos de seguridad, para formar claves de privilegio exclusivas. Las claves de privilegio se utilizarán para verificar que otro testigo de seguridad, generalmente asociado con un terminal, tenga los privilegios necesarios antes de permitir el acceso a un recurso controlado 220. La autoridad de expedición incluye entonces la clave o las claves de privilegio resultantes en el testigo o los testigos de seguridad. La clave o claves maestras se diversifican, a continuación, mediante un mecanismo de división de claves y se instalan en las unidades de procesamiento de datos designadas, tal como se representa en la figura 2, como TOKEN 1 204 y TOKEN 2 206.

El primer testigo de seguridad TOKEN1 204 comprende el componente de clave MK1 205. El segundo testigo de seguridad TOKEN2 206 comprende el componente de clave equivalente MK2 210 y los medios para combinar los dos elementos de clave y formar la clave maestra completa. La clave maestra reconstruida está dispuesta para permanecer en la memoria transitoria del segundo testigo de seguridad 206 a fin de evitar la divulgación no autorizada conforme a lo prescrito por los atributos A 203 asociados con el privilegio de componente de clave MK1 205. Cualquier manipulación del testigo de seguridad que contiene la clave maestra provoca la destrucción de la clave maestra. Los recursos controlados 220 asociados con el sistema informático 202 se representan como una base de datos a título de ejemplo solo y únicamente son accesibles tras la verificación de privilegios mediante una tercera unidad de procesamiento de datos.

En la figura 2A, el ciclo de autenticación mutua 280 se lleva a cabo tal como se ha descrito anteriormente antes de la transferencia de privilegios. La autenticación mutua 280 se prefiere como medio para asegurar que tanto la unidad de procesamiento de datos emisora como la unidad de procesamiento de datos receptora estén autorizadas para realizar transacciones de transferencia de privilegios.

En la forma de realización preferida de la presente invención, las autenticaciones mutuas seguras se realizan mediante el mecanismo descrito en la solicitud de patente US n.º 10/058.734, "A System And Method For Performing Mutual Authentication Between Security Tokens", presentada el 30 de enero de 2002. Pueden utilizarse también mecanismos de autenticación de prueba/respuesta estándar.

En la figura 2B, se representa la transferencia del componente de clave MK1 205 y sus atributos asociados A 203 desde el primer testigo de seguridad TOKEN1 204 hasta el segundo testigo de seguridad 206. El segundo testigo de seguridad TOKEN2 206 reúne el par de componentes de clave MK1, MK2 205', 210, reconstruyendo de ese modo la clave maestra MK12 240. La clave maestra operativa MK12 240 se almacena en la memoria volátil del segundo testigo de seguridad TOKEN2 206 conforme a lo prescrito por los atributos asociados A' 203'. Se emplea un canal seguro 282 durante el procedimiento de transferencia del componente de clave.

En la figura 2C, el primer testigo de seguridad TOKEN1 204 se sustituye por un tercer testigo de seguridad TOKEN3 250. El tercer testigo de seguridad TOKEN3 250 comprende una clave de privilegio KT3 255 que se obtuvo de la clave maestra MK12 240 diversificando la clave maestra MK12 240 mediante un identificador exclusivo ID 260 asociado con el tercer testigo de seguridad 250. La clave de privilegio KT3 255 se generó e incluyó en el tercer testigo de seguridad TOKEN3 250 en el momento de su expedición por la autoridad de expedición. Cada testigo de seguridad incluido en el grupo de privilegios definido presenta una clave de privilegio instalada funcionalmente que se obtuvo e instaló de la misma manera. Para regenerar la clave de privilegio, el identificador exclusivo ID 280 se envía 260 desde el tercer testigo de seguridad 250 al segundo testigo de seguridad 206 como parte de la prueba de autenticación.

En la figura 2D, el segundo testigo de seguridad TOKEN2 206 diversifica la clave maestra MK12 240 con el identificador exclusivo recibido ID' 260' y reconstruye la clave de privilegio KT3' 255'. La clave de privilegio reconstruida KT3' 255' se mantiene asimismo en memoria volátil conforme a lo prescrito por los atributos asociados A' 203'. La clave de privilegio reconstruida KT3' 255' se utiliza para generar una respuesta a la prueba presentada por el tercer testigo de seguridad TOKEN3 250, tal como se representa en la figura 2E.

En la figura 2F, la autenticación satisfactoria demuestra al tercer testigo de seguridad que existe un privilegio válido en el segundo testigo de seguridad TOKEN2 206, lo cual permite el acceso a los recursos controlados 220, ya sea facilitando la información necesaria para acceder a un registro específico 295 (por ejemplo, número de seguridad social), o bien permitiendo el acceso y la transferencia de una clave criptográfica necesaria para desbloquear el recurso controlado, representado por un objeto' 270'. Se emplea un canal seguro 290 durante el procedimiento de transferencia de cualquier objeto' 270'.

Con referencia a la figura 3, se representa otra forma de realización de la presente invención, en la que se muestra una clave maestra completa MK 305 que representa un privilegio delegable y los atributos asociados A 302. La clave maestra MK 305 y sus atributos asociados A 302 se almacenan de forma segura dentro de un primer testigo de seguridad TOKEN1 304 y se conectan funcionalmente 380 al sistema informático de un cliente 303. Un segundo testigo de seguridad TOKEN2 306 está, asimismo, conectado funcionalmente 380 al sistema informático de un cliente 303 y establece comunicaciones de procesamiento con el primer testigo de seguridad TOKEN1 304. Unos recursos controlados 330 asociados al sistema informático 303 se representan como una base de datos (a título de ejemplo solo), siendo estos accesibles únicamente tras la verificación de los privilegios mediante un tercer testigo de seguridad.

Con referencia a la figura 3A, el ciclo de autenticación mutua de prerrequisitos 380 descrito anteriormente se inicia antes de la transferencia de privilegios. La transferencia de la clave maestra MK 305 y sus atributos asociados A 302 desde el primer testigo de seguridad 304 hasta el segundo testigo de seguridad 306 se representa en la figura 3B. El segundo testigo de seguridad 306 almacena funcionalmente la clave maestra recibida MK 305 en memoria volátil conforme a lo prescrito por los atributos asociados A' 302'. Se emplea un canal seguro 390 durante el procedimiento de transferencia de la clave maestra. Los aspectos adicionales para el uso de la clave maestra simétrica son idénticos a los descritos anteriormente para la parte de los componentes de clave.

Con referencia a la figura 4, se representa otra forma de realización de la presente invención, en la que una autoridad de expedición genera una clave privada de grupo Kpri 405 que representa un privilegio particular y los atributos asociados A 402 y la instala en el primer testigo de seguridad TOKEN1 403. El primer testigo de seguridad se conecta funcionalmente 480 con el sistema informático de un cliente 404.

Asimismo, un segundo testigo de seguridad TOKEN2 406 se conecta funcionalmente 480 con el sistema informático del cliente 404 y establece comunicaciones de procesamiento con el primer testigo de seguridad TOKEN1 403. Unos

recursos controlados 440 asociados al sistema informático 404 se representan como una base de datos (a título de ejemplo solo), siendo estos accesibles únicamente tras la verificación de los privilegios mediante un tercer testigo de seguridad. La clave pública equivalente a la clave privada de grupo se instala asimismo en todos los testigos de seguridad de nivel de usuario. Las claves PKI pueden basarse en algoritmos que utilizan curvas elípticas, RSA, Diffie-Hellman , Pretty Good Privacy (PGP), El Gamal, etc.

Con referencia a la figura 4A, el ciclo de autenticación mutua 480 descrito anteriormente se inicia antes de la transferencia de privilegios. La transferencia de la clave privada Kpri 405 y sus atributos asociados A 402 desde el primer testigo de seguridad TOKEN1 403 hasta el segundo testigo de seguridad TOKEN2 406 se representa en la figura 4B. El segundo testigo de seguridad 406 almacena funcionalmente la clave privada recibida Kpri 405 en memoria volátil conforme a lo prescrito por los atributos asociados A' 402'. Se emplea un canal seguro 490 durante el procedimiento de transferencia de la clave privada.

En la figura 4C, el primer testigo de seguridad TOKEN1 403 se sustituye por un tercer testigo de seguridad TOKEN3 450. El tercer testigo de seguridad TOKEN3 450 comprende una clave pública Kpub 455 que es la equivalente a la clave privada Kpri' 405'. La clave pública Kpub 455 se generó e incluyó en el tercer testigo de seguridad TOKEN3 450 en el momento de su expedición por la autoridad de expedición. Cada testigo de seguridad incluido en el grupo de privilegios definido presenta una clave pública instalada funcionalmente que se instaló de la misma manera. El tercer testigo de seguridad TOKEN3 450 genera la prueba de autenticación que comprende el uso de la clave pública Kpub 455. La prueba se envía 480 al segundo testigo de seguridad TOKEN2 406.

En la figura 4D, el segundo testigo de seguridad TOKEN2 406 recibe la prueba de autenticación y genera una respuesta que comprende el uso de la clave privada de grupo Kpri' 405'. La respuesta se envía 480 al tercer testigo de seguridad TOKEN3 450 para la autenticación.

En la figura 4E, la autenticación satisfactoria demuestra al tercer testigo de seguridad TOKEN3 450 que existe un privilegio válido en el segundo testigo de seguridad TOKEN2 406 que permite el acceso a los recursos controlados 440, ya sea facilitando la información necesaria para acceder a un registro específico 495 (por ejemplo, el número de seguridad social), o bien permitiendo el acceso y la transferencia de una clave criptográfica necesaria para desbloquear el recurso controlado representado por un objeto' 470'. Se emplea un canal seguro 490 durante el procedimiento de transferencia de cualquier objeto' 270'.

Con referencia a la figura 5, se presenta un diagrama de flujo simplificado que indica las etapas necesarias para implementar la presente invención. El procedimiento se inicia 500 mediante la realización de autenticaciones mutuas 502 entre un testigo de seguridad delegante y una primera unidad de procesamiento de datos 502.

Si cualquiera de las partes del ciclo de autenticación mutua resulta infructuosa 504, el procedimiento de delegación de privilegios termina 526. Si el procedimiento de autenticación se realiza con éxito 504, se establece un canal seguro 506, y los privilegios delegables y atributos asociados son transferidos desde el testigo de seguridad hasta la unidad de procesamiento de datos receptora 508. Para utilizar el privilegio, una segunda unidad de procesamiento de datos autentica 510 la unidad de procesamiento de datos receptora. Si el procedimiento de autenticación se realiza con éxito 512, se establece un canal seguro 514, y la segunda unidad de procesamiento de datos 516 verifica el privilegio delegable. Si el procedimiento de autenticación resulta infructuoso 512, el procedimiento de delegación de privilegios termina 526.

Si el procedimiento de verificación se realiza con éxito 518, se concede el acceso y el uso del privilegio delegable 524. Si el procedimiento de verificación resulta infructuoso 518, los atributos asociados con el privilegio se actualizan 520 y el procedimiento de verificación se intenta de nuevo 516. Si el procedimiento de verificación se realiza con éxito 518, se concede el acceso y el uso del privilegio delegable 524, conforme a lo prescrito por los atributos asociados. Si el procedimiento de verificación resulta infructuoso por segunda vez, el procedimiento de delegación de privilegios termina 526.

Las formas de realización de la presente invención descritas anteriormente se facilitan a título ilustrativo y descriptivo. Dichas formas de realización no pretenden limitar la presente invención a la forma específica descrita. En particular, se prevé que la implementación funcional de la presente invención descrita en la presente memoria pueda implementarse igualmente en hardware, software, firmware y/u otros componentes funcionales o elementos básicos disponibles. Tomando en consideración la información facilitada en la presente memoria, es posible realizar otras variantes y formas de realización, no siendo el propósito de la presente descripción detallada limitar el alcance de la presente invención.

Esta descripción se refiere, entre otros, a un primer sistema para delegar un privilegio (20) y los atributos asociados (30) desde un testigo de seguridad (10) hasta por lo menos una primera unidad de procesamiento de datos (40), permitiendo dicho privilegio (20) a la por lo menos una primera unidad de procesamiento de datos (40) acceder por lo menos a uno de los recursos, conforme a los requisitos prescritos en dichos atributos asociados (30), que comprende:

i. dicho testigo de seguridad (10) que comprende dicho privilegio (20) y dichos atributos asociados (30) y unos medios de delegación para delegar dicho privilegio (20) a dicha por lo menos una primera unidad de procesamiento de datos (40),

ii. dicha por lo menos una primera unidad de procesamiento de datos (40) que comprende unos medios de procesamiento de privilegios para implementar dicho privilegio (20) conforme a dichos requisitos prescritos en dichos atributos asociados (30),

iii. unos medios de comunicación para realizar intercambios de datos entre dicho testigo de seguridad (10) y dicha por lo menos una primera unidad de procesamiento de datos (40).

En dicho primer sistema, puede realizarse una autenticación mutua entre dicho testigo de seguridad (10) y dicha por lo menos una primera unidad de procesamiento de datos (40) antes de delegar dicho privilegio (20). Además, dichos medios de comunicación pueden comprender un protocolo de mensajería segura. Además, dichos intercambios de datos pueden comprender datos de autenticación, dicho privilegio (20) o dichos atributos asociados (30).

En dicho primer sistema, dicho privilegio (20) puede ser actualizable mediante sustitución de por lo menos una parte de dicho atributos asociados (30) por uno o más nuevos atributos asociados.

En dicho primer sistema, dicha por lo menos una primera unidad de procesamiento de datos (40) puede ser un dispositivo inteligente.

En dicho primer sistema, dicha por lo menos una primera unidad de procesamiento de datos (40) puede ser otro testigo de seguridad.

En dicho primer sistema, dichos atributos asociados (30) pueden comprender aspectos de control.

En dicho primer sistema, dichos aspectos de control pueden comprender políticas de seguridad. Además, dichos aspectos de control pueden comprender por lo menos un estado de privilegio.

En dicho primer sistema, dicho privilegio (20) puede comprender un componente de clave, una clave criptográfica, un certificado de atributos de privilegios, un ticket digital, una licencia, un derecho digital, unas credenciales digitales, una contraseña, una plantilla biométrica, una muestra biométrica o un crédito de fidelización.

En dicho primer sistema, dicho por lo menos un recurso puede ser accesible para dicha primera unidad de procesamiento de datos (40) solo si dicho privilegio (20) está presente en dicha primera unidad de procesamiento de datos y es verificado por lo menos por una segunda unidad de procesamiento de datos (50). Además, dicho privilegio (20) puede facilitar a dicha por lo menos una primera unidad de procesamiento de datos (40) la realización de una función seleccionada del grupo que consiste en operaciones de sustitución para dicho testigo de seguridad (10), activación de terminales, personalización de un dispositivo inteligente, acceso a dicho por lo menos un recurso o gestión de créditos de fidelización.

La presente descripción se refiere, entre otros, a un segundo sistema para delegar un privilegio (20) desde un testigo de seguridad (10) hasta por lo menos una primera unidad de procesamiento de datos (40), en el que dicho privilegio (20) permite a dicha por lo menos una primera unidad de procesamiento de datos (40) realizar una función seleccionada del grupo que consiste en operaciones de sustitución para dicho testigo de seguridad (10), activación de terminales, personalización de un dispositivo inteligente, acceso a un recurso incluido en por lo menos una segunda unidad de procesamiento (50) o accesible a través de esta o gestión de créditos de fidelización.

Dicho segundo sistema puede comprender además atributos asociados con dicho privilegio (20), en el que dichos tributos facilitan suficiente información a dicha primera unidad de procesamiento de datos (40) para utilizar dicho privilegio (20) y aplicar uno o más aspectos de control indicados en dicho atributos asociados (30), que comprenden políticas de seguridad y, por lo menos, un estado de privilegio.

Esta descripción se refiere, entre otros, a un primer procedimiento para delegar un privilegio (20) que presenta unos atributos asociados (30) desde un testigo de seguridad (10) hasta por lo menos una primera unidad de procesamiento de datos (40), permitiendo dicho privilegio (20) a dicha por lo menos una primera unidad de procesamiento de datos (40) utilizar dicho privilegio (20) conforme a los requisitos prescritos en dichos atributos asociados (30), comprendiendo dicho procedimiento las etapas siguientes:

i. realización (502) de una transacción de autenticación mutua entre dicho testigo de seguridad (10) y dicha por lo menos una primera unidad de procesamiento de datos (40),

ii. transferencia segura (508) de dicho privilegio (20) que comprende dichos atributos asociados (30) a dicha por lo menos una primera unidad de procesamiento de datos (40),

iii. utilización (524) de dicho privilegio (20) conforme a lo prescrito por dichos atributos asociados (30).

En dicho primer procedimiento, dicha por lo menos una primera unidad de procesamiento de datos (40) puede ser un sistema informático. Además, dicha por lo menos una primera unidad de procesamiento de datos (40) puede ser otro testigo de seguridad.

En dicho primer procedimiento, dicho privilegio (20) puede ser actualizable mediante sustitución de dichos atributos asociados (30) por un nuevo atributo asociado por lo menos. Además, dicho privilegio (20) puede transferirse desde dicho testigo de seguridad (10) hasta dicho por lo menos una primera unidad de procesamiento de datos (40) mediante un protocolo de mensajería segura.

La presente descripción se refiere, entre otros, a un primer sistema de delegación de privilegios que comprende:

i. un testigo de seguridad (10) que comprende por lo menos un privilegio delegable (20) y unos atributos asociados con dicho privilegio delegable (20),

ii. por lo menos una primera unidad de procesamiento de datos (40) que comprende unos medios para utilizar dicho privilegio (20) conforme a los requisitos prescritos en dichos atributos asociados (30).

En dicho primer sistema de delegación de privilegios, dicha por lo menos una primera unidad de procesamiento de datos (40) puede ser un sistema informático.

En dicho primer sistema de delegación de privilegios, dicha por lo menos una primera unidad de procesamiento de datos (40) puede ser otro testigo de seguridad.

En dicho primer sistema de delegación de privilegios, dicho privilegio (20) puede ser actualizable mediante sustitución de dichos atributos asociados (30) por un nuevo atributo asociado por lo menos.

En dicho primer sistema de delegación de privilegios, dicho privilegio (20) es transferido desde dicho testigo de seguridad (10) hasta dicha por lo menos una primera unidad de procesamiento de datos (40) mediante un protocolo de mensajería segura. Además, dicho testigo de seguridad (10) y dicha por lo menos una primera unidad de procesamiento de datos (40) pueden autenticarse mutuamente antes de que dicho privilegio (20) se transfiera.

En dicho primer sistema de delegación de privilegios, dicho privilegio (20) puede permitir a dicha por lo menos una primera unidad de procesamiento de datos (40) realizar una función seleccionada del grupo que consiste en operaciones de sustitución para dicho testigo de seguridad (10), activación de terminales, personalización de un dispositivo inteligente, acceso a un recurso incluido en una segunda unidad de procesamiento de datos (50) o accesible a través de esta o gestión de créditos de fidelización.

REIVINDICACIONES

1. Sistema de delegación de privilegios, que comprende:

   i. un testigo de seguridad basado en hardware (10) que incluye por lo menos una primera parte de un privilegio delegable (20) y unos atributos asociados con dicha primera parte de dicho privilegio delegable (20) y unos medios de transferencia para transferir dicha primera parte de dicho privilegio delegable (20) y dichos atributos por lo menos a una primera unidad de procesamiento de datos (40),

   ii. incluyendo dicha primera unidad de procesamiento de datos (40) una segunda parte de dicho privilegio delegable (20), unos primeros medios de combinación para combinar dicha primera parte de dicho privilegio delegable (20) con dicha segunda parte de dicho privilegio delegable (20) para formar un privilegio utilizable.

2. Sistema según la reivindicación 1, en el que dicha segunda parte de dicho privilegio delegable (20) está contenida en una segunda unidad de procesamiento de datos (50).

3. Sistema según la reivindicación 2 en el que dicha primera parte de dicho privilegio delegable (20) y dichos atributos asociados (30) son transferidos desde dicha primera unidad de procesamiento de datos (40) hasta dicha segunda unidad de procesamiento de datos (50).

4. Sistema según la reivindicación 3, en el que dicha segunda unidad de procesamiento de datos (50) incluye unos segundos medios de combinación para combinar dicha primera parte de dicho privilegio delegable (20) con dicha segunda parte de dicho privilegio delegable (20).

5. Sistema según una de las reivindicaciones 2 a 4, en el que dicha primera unidad de procesamiento de datos (40) o dicha segunda unidad de procesamiento de datos (50) es un sistema informático.

6. Sistema según una de las reivindicaciones 2 a 5, en el que dicha primera unidad de procesamiento de datos (40) o dicha segunda unidad de procesamiento de datos (50) es otro testigo de seguridad.

7. Sistema según una de las reivindicaciones anteriores, en el que dicho privilegio (20) es transferido desde dicho testigo de seguridad (10) hasta dicha primera unidad de procesamiento de datos (40) utilizando un protocolo de mensajería segura.

8. Sistema según una de las reivindicaciones anteriores, en el que el acceso a un recurso es habilitado combinando dicha primera parte de dicho privilegio delegable (20) con dicha segunda parte de dicho privilegio delegable (20).

9. Sistema según una de las reivindicaciones 3 a 8, en el que dicho privilegio (20) es transferido desde dicha primera unidad de procesamiento de datos (40) hasta dicha segunda unidad de procesamiento de datos (50) utilizando un protocolo de mensajería segura.

10. Sistema según una de las reivindicaciones 4 a 9, en el que dicha segunda parte de dicho privilegio delegable (20) es transferida desde dicha segunda unidad de procesamiento de datos (50) hasta dicha primera unidad de procesamiento de datos (40).

11. Sistema según la reivindicación 10, en el que dicho recurso está contenido en dicha primera unidad de procesamiento de datos (40).

12. Sistema según la reivindicación 10, en el que dicho recurso está contenido en dicha segunda unidad de procesamiento de datos (50).

13. Sistema según la reivindicación 12, en el que dicho recurso es transferido desde dicha segunda unidad de procesamiento de datos (50) hasta dicha primera unidad de procesamiento de datos (40).

14. Sistema según la reivindicación 11, en el que dicho recurso es transferido desde dicha primera unidad de procesamiento de datos (40) hasta dicha segunda unidad de procesamiento de datos (50).

15. Sistema según una de las reivindicaciones anteriores, en el que dicho privilegio delegable (20) es generado combinando una pluralidad de privilegios parciales en una sola unidad de procesamiento de datos.

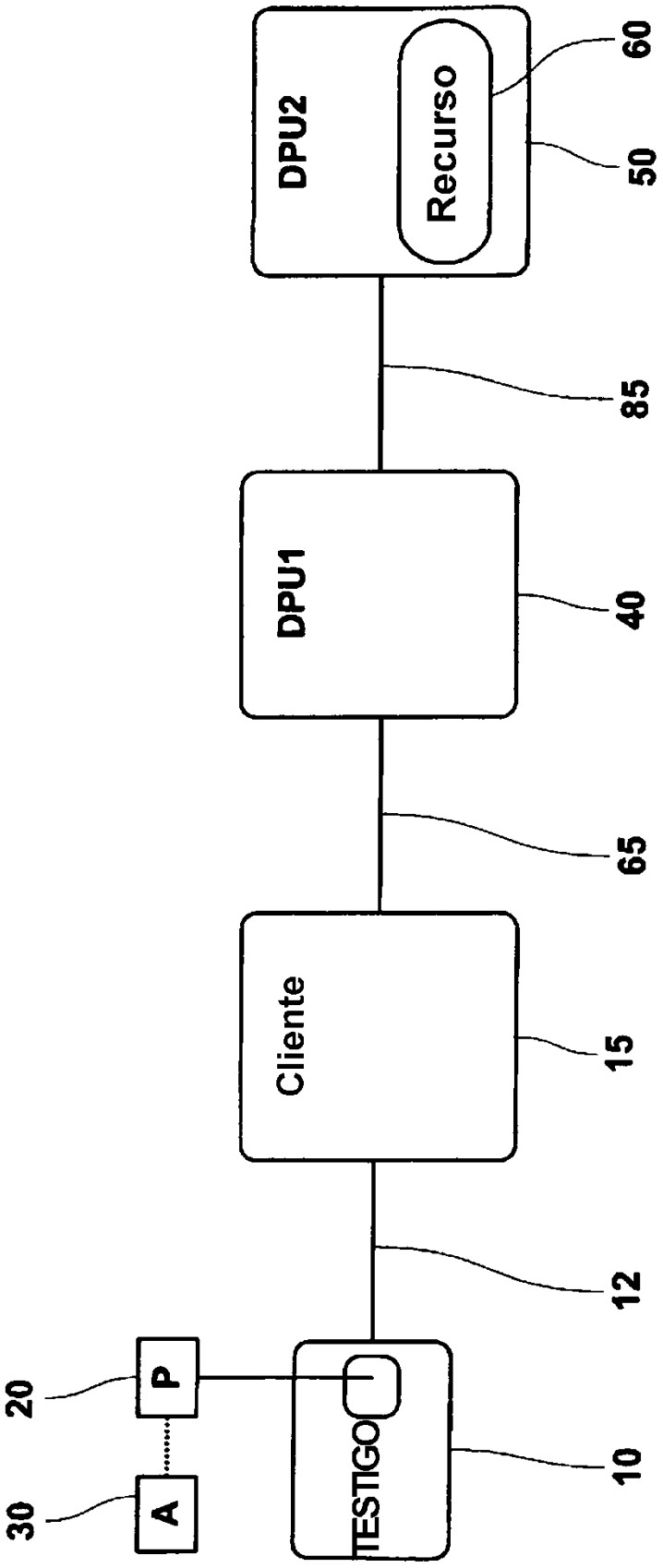
DPU2
Recurso
60
50
85
DPU1
40
65
Cliente
15
12
P
20
A
30
TESTIGO
10

FIG. 1

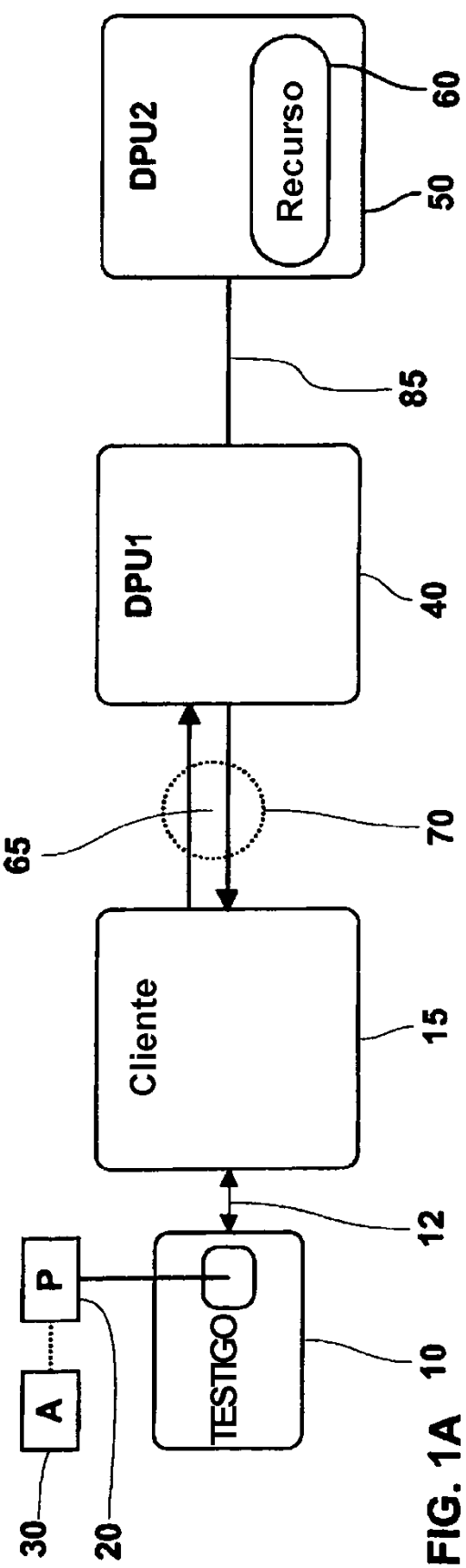
DPU2
Recurso
60
50
85
DPU1
40
65
70
Cliente
15
12
P
A
TESTIGO
10
30
20

FIG. 1A

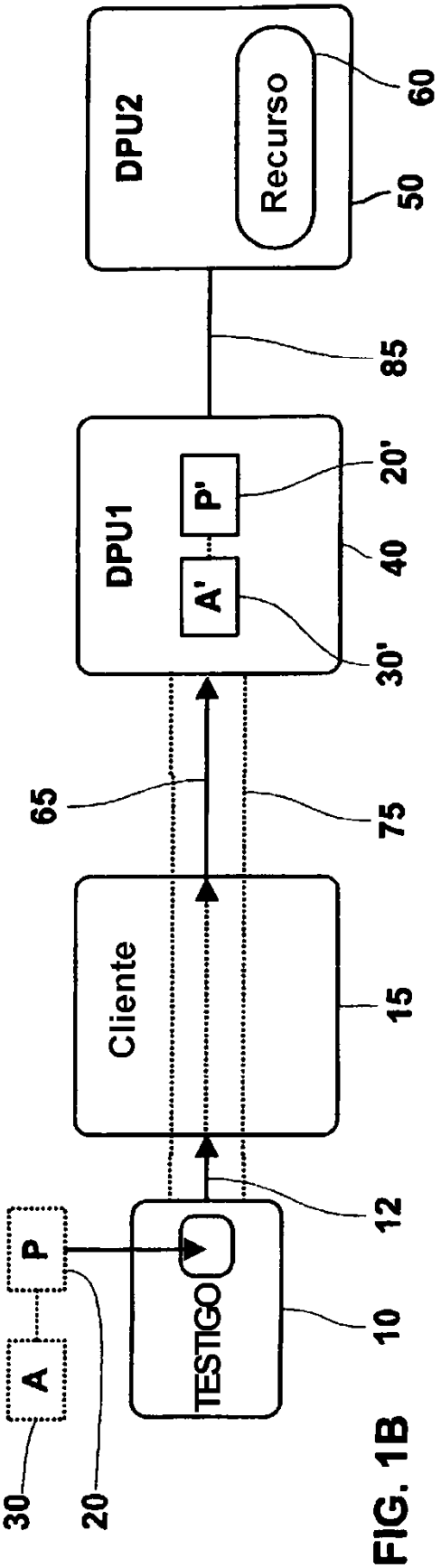
DPU2
Recurso
60
50
85
DPU1
P'
A'
20'
40
30'
65
75
Cliente
15
12
P
A
TESTIGO
10
30
20

FIG. 1B

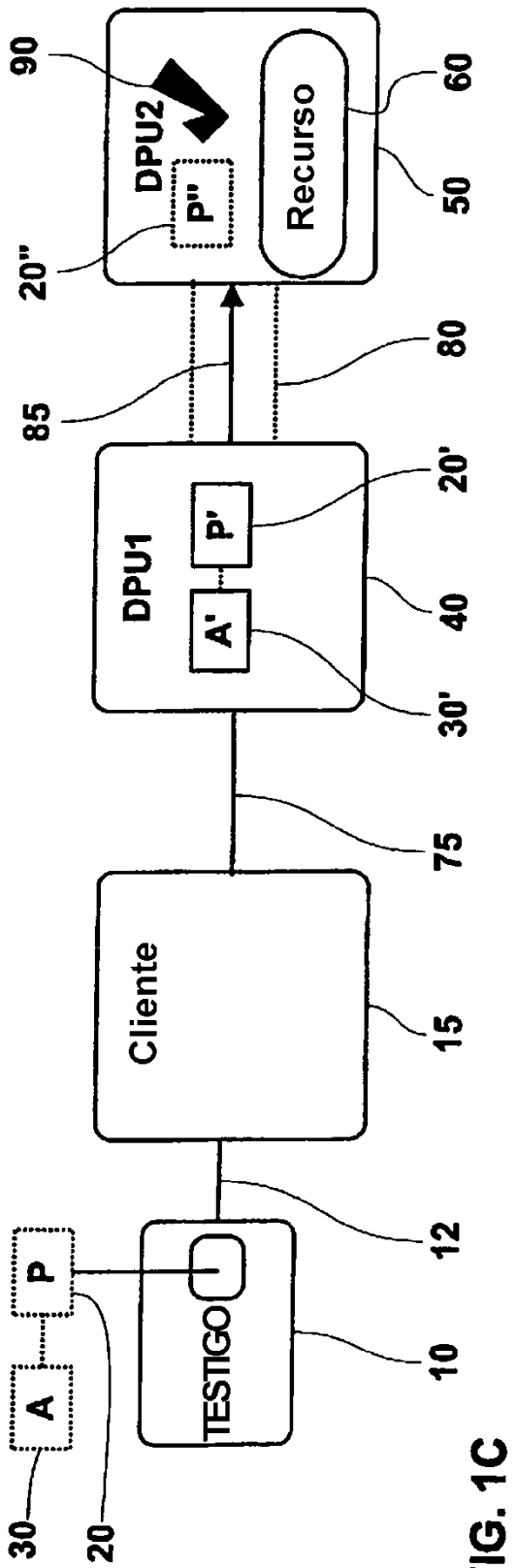
90
DPU2
P''
20''
Recurso
60
50
85
80
DPU1
P'
A'
20'
40
30'
75
Cliente
15
12
TESTIGO
10
P
A
30
20

FIG. 1C

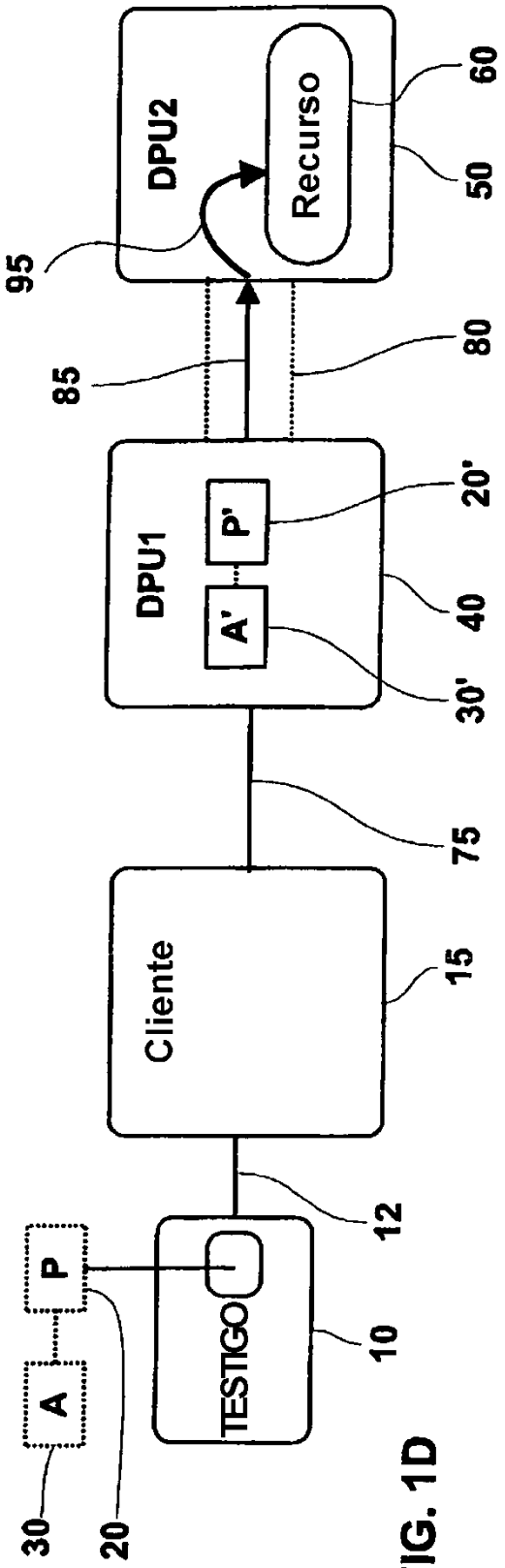
95
DPU2
Recurso
60
50
85
80
DPU1
P'
A'
20'
40
30'
75
Cliente
15
12
TESTIGO
10
P
A
30
20

FIG. 1D

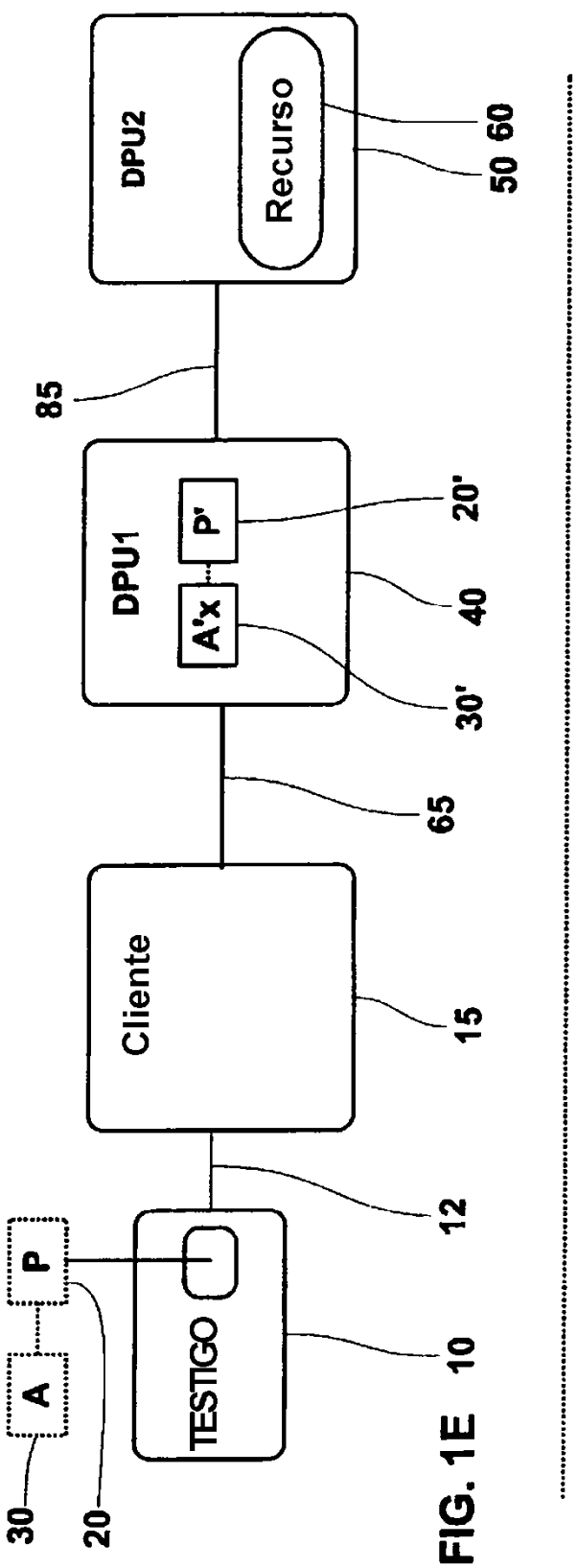
DPU2
Recurso
50 60
85
DPU1
P'
A'x
20'
40
30'
65
Cliente
15
12
TESTIGO
10
P
A
30
20

FIG. 1E

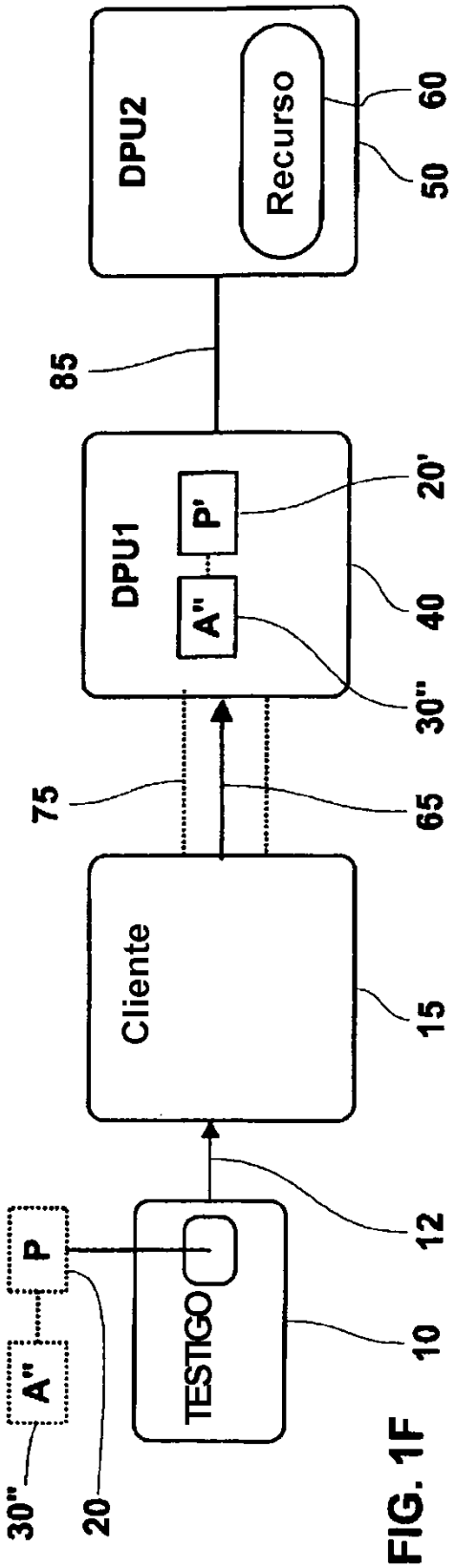
DPU2
Recurso
50 60
85
DPU1
P'
A"
20'
40
30"
75
65
Cliente
15
12
TESTIGO
10
P
A"
30"
20

FIG. 1F

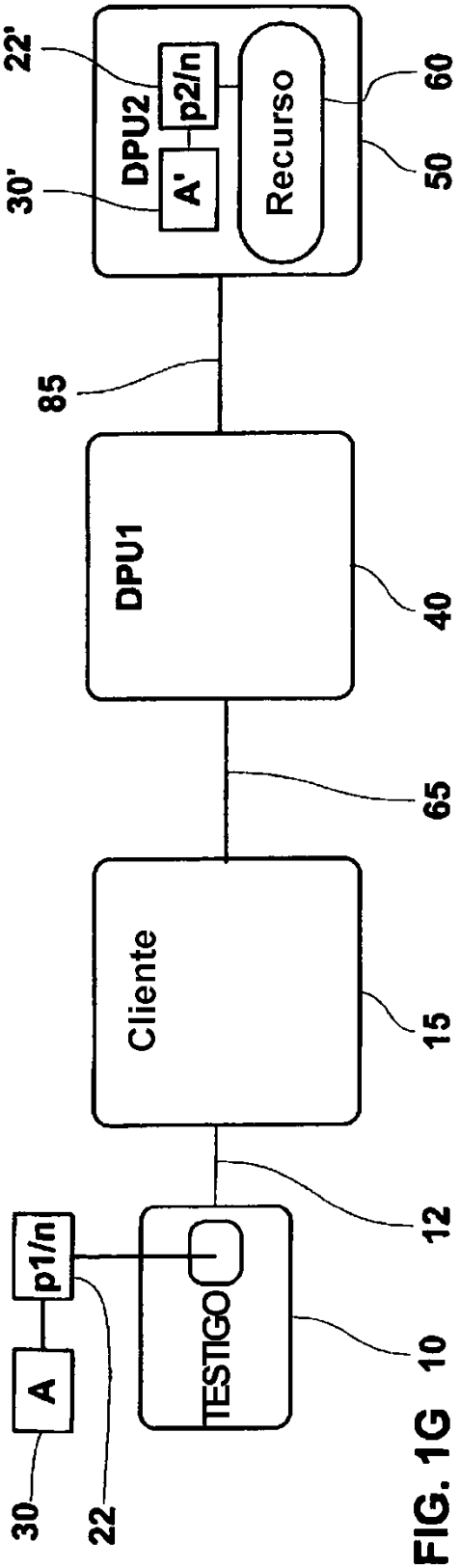
22'
30'
DPU2
p2/n
A'
Recurso
60
50
85
DPU1
40
65
Cliente
15
12
p1/n
A
TESTIGO
10
30
22

FIG. 1G

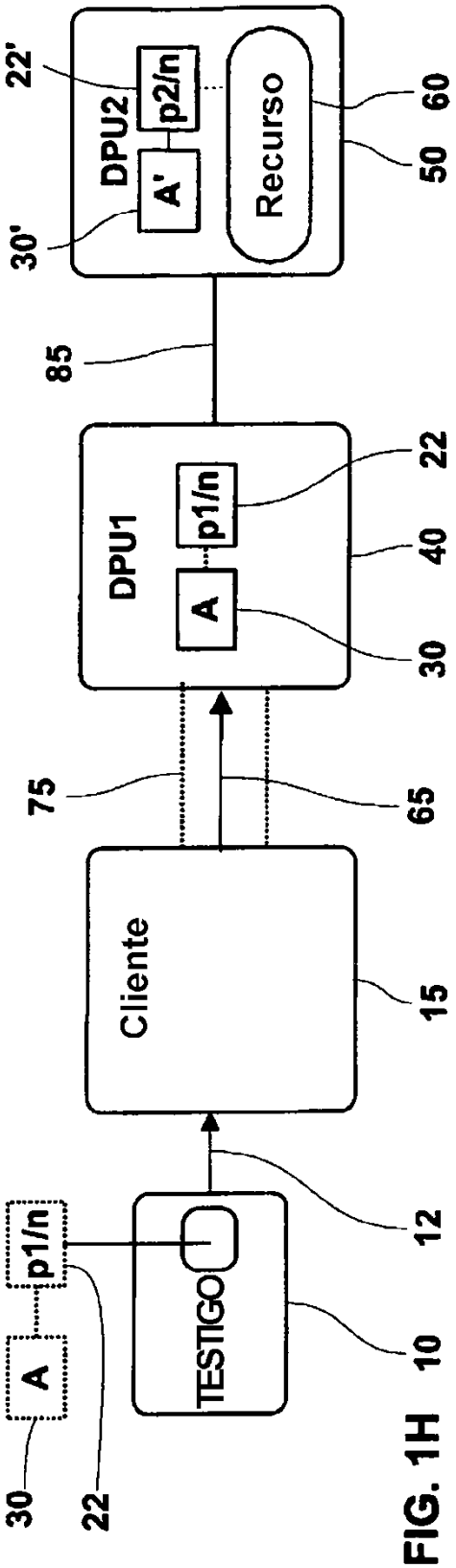
22'
30'
DPU2
p2/n
A'
Recurso
60
50
85
DPU1
p1/n
A
22
40
30
75
65
Cliente
15
12
p1/n
A
TESTIGO
10
30
22

FIG. 1H

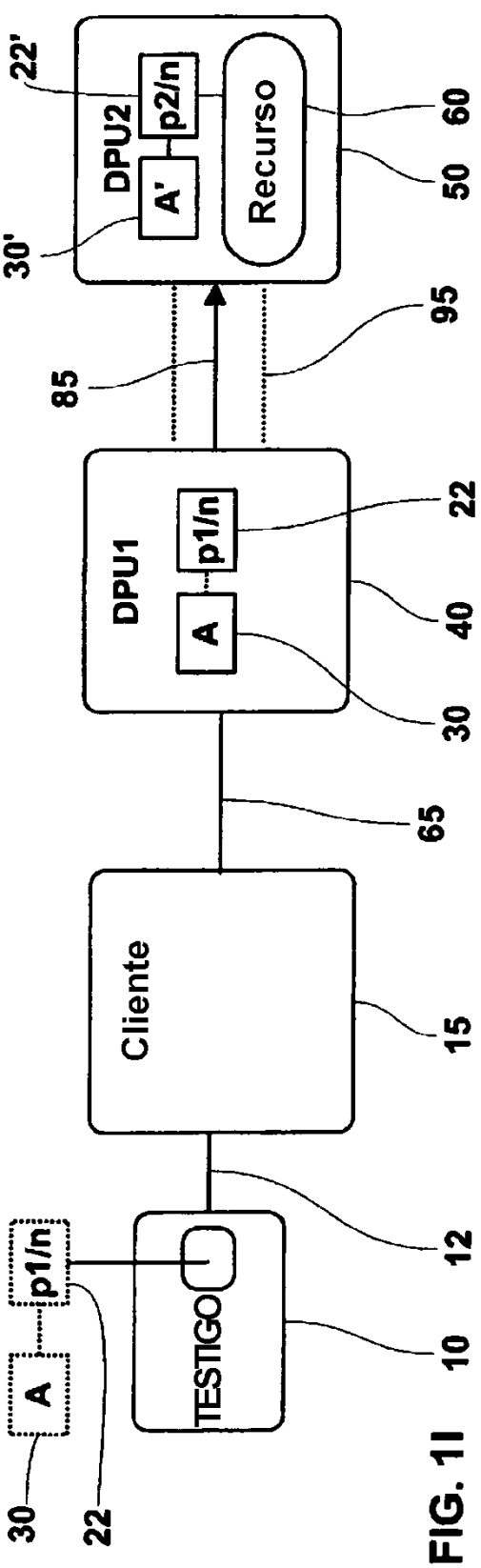
22'
DPU2
p2/n
A'
Recurso
30'
60
50
85
95
DPU1
p1/n
A
22
40
30
65
Cliente
15
p1/n
A
TESTIGO
12
10
30
22

FIG. 1I

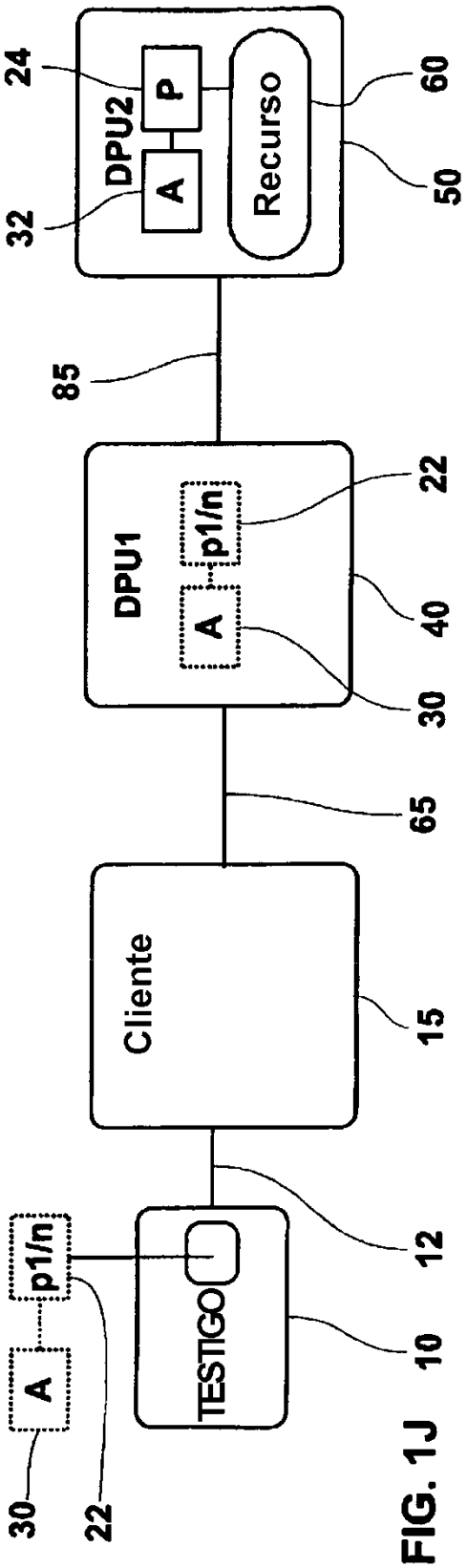
24
DPU2
P
A
Recurso
32
60
50
85
DPU1
p1/n
A
22
40
30
65
Cliente
15
p1/n
A
TESTIGO
12
10
30
22

FIG. 1J

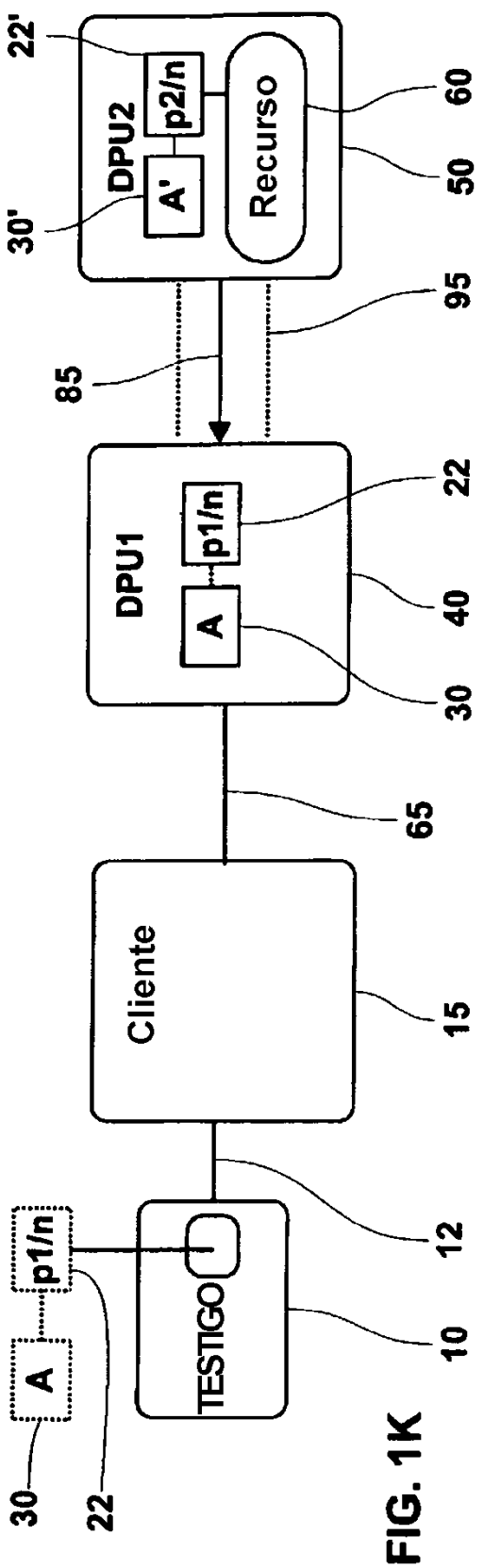
22'
DPU2
p2/n
A'
Recurso
30'
60
50
95
85
DPU1
p1/n
A
22
40
30
65
Cliente
15
p1/n
A
TESTIGO
12
10
30
22

FIG. 1K

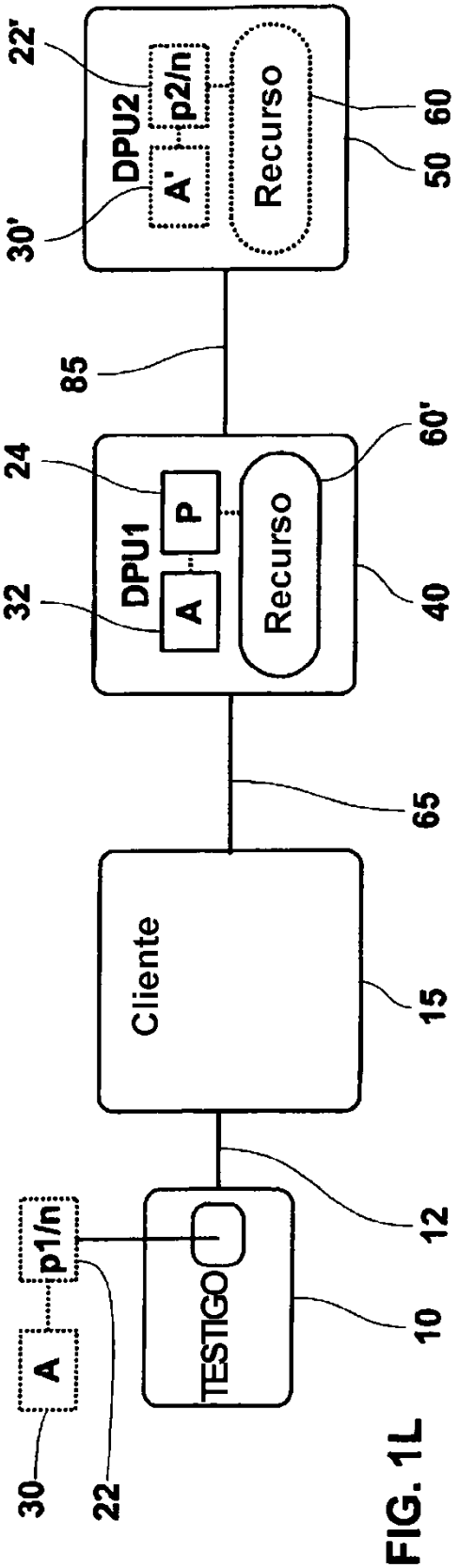
22'
DPU2
p2/n
A'
Recurso
30'
60
50
85
24
DPU1
P
A
32
Recurso
60'
40
65
Cliente
15
p1/n
A
TESTIGO
12
10
30
22

FIG. 1L

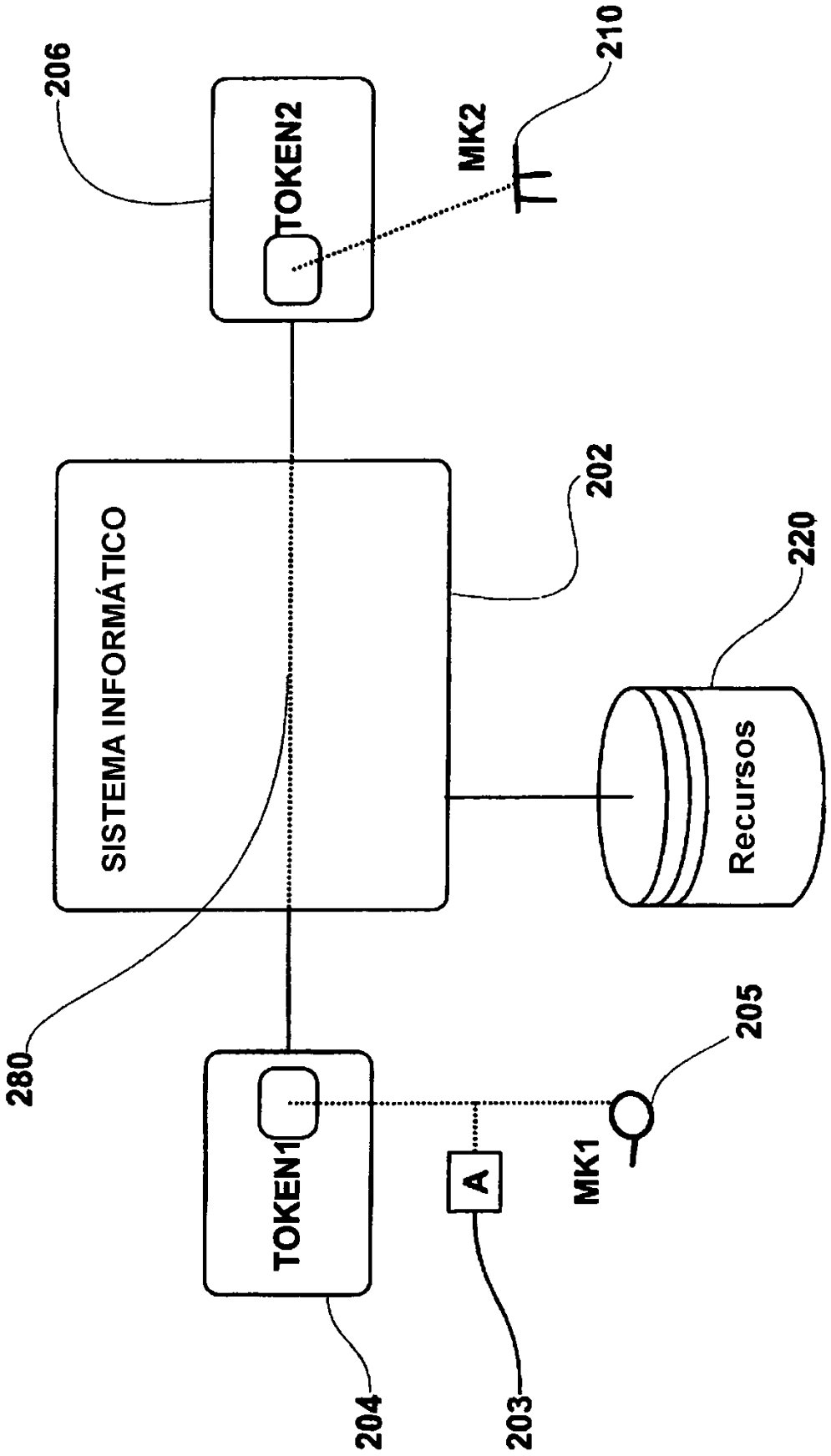
206
TOKEN2
210
MK2
SISTEMA INFORMÁTICO
202
220
Recursos
280
205
TOKEN1
MK1
A
204
203

FIG. 2

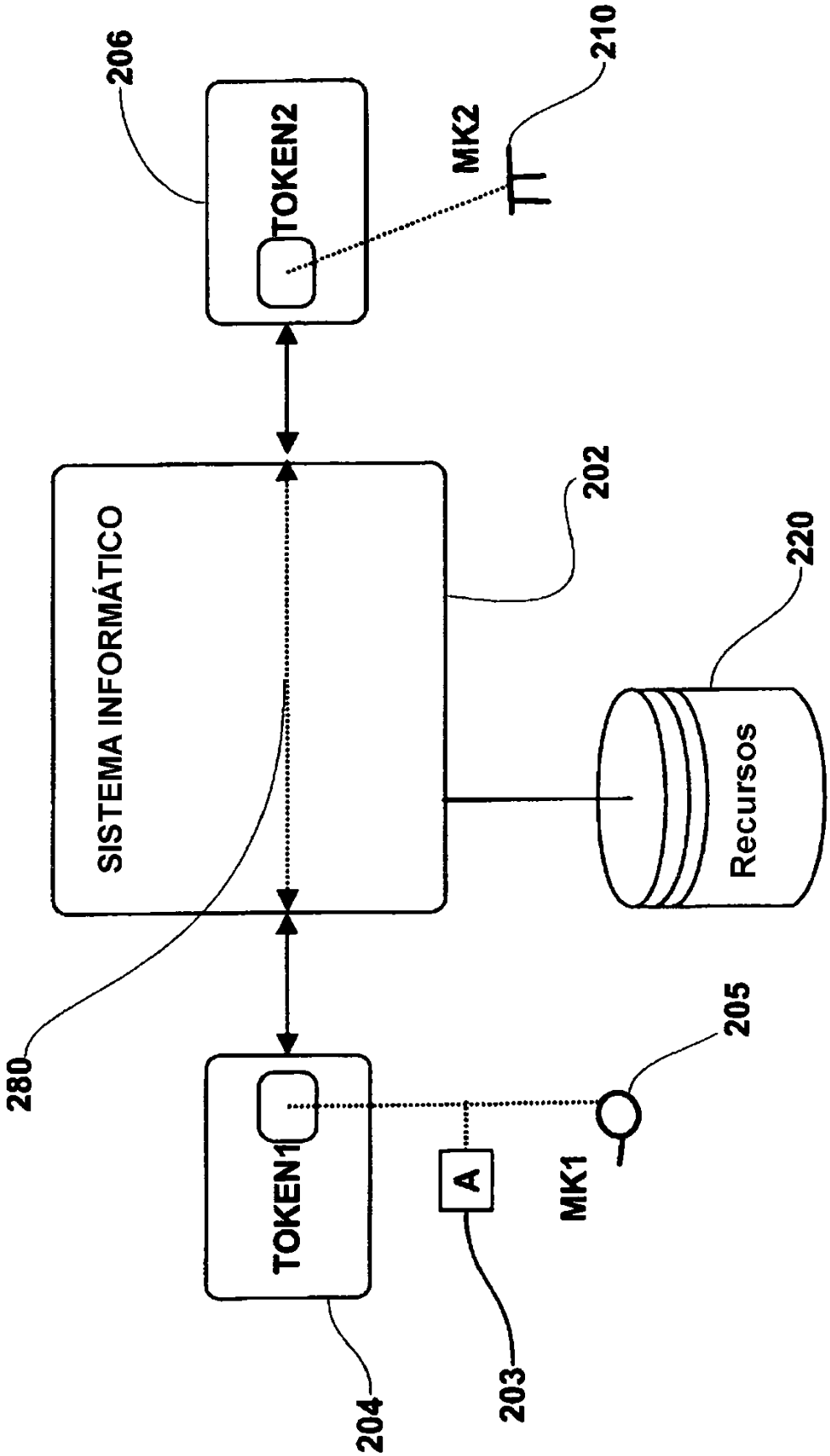
206
TOKEN2
210
MK2
SISTEMA INFORMÁTICO
202
220
Recursos
280
205
TOKEN1
A
MK1
204
203

FIG. 2A

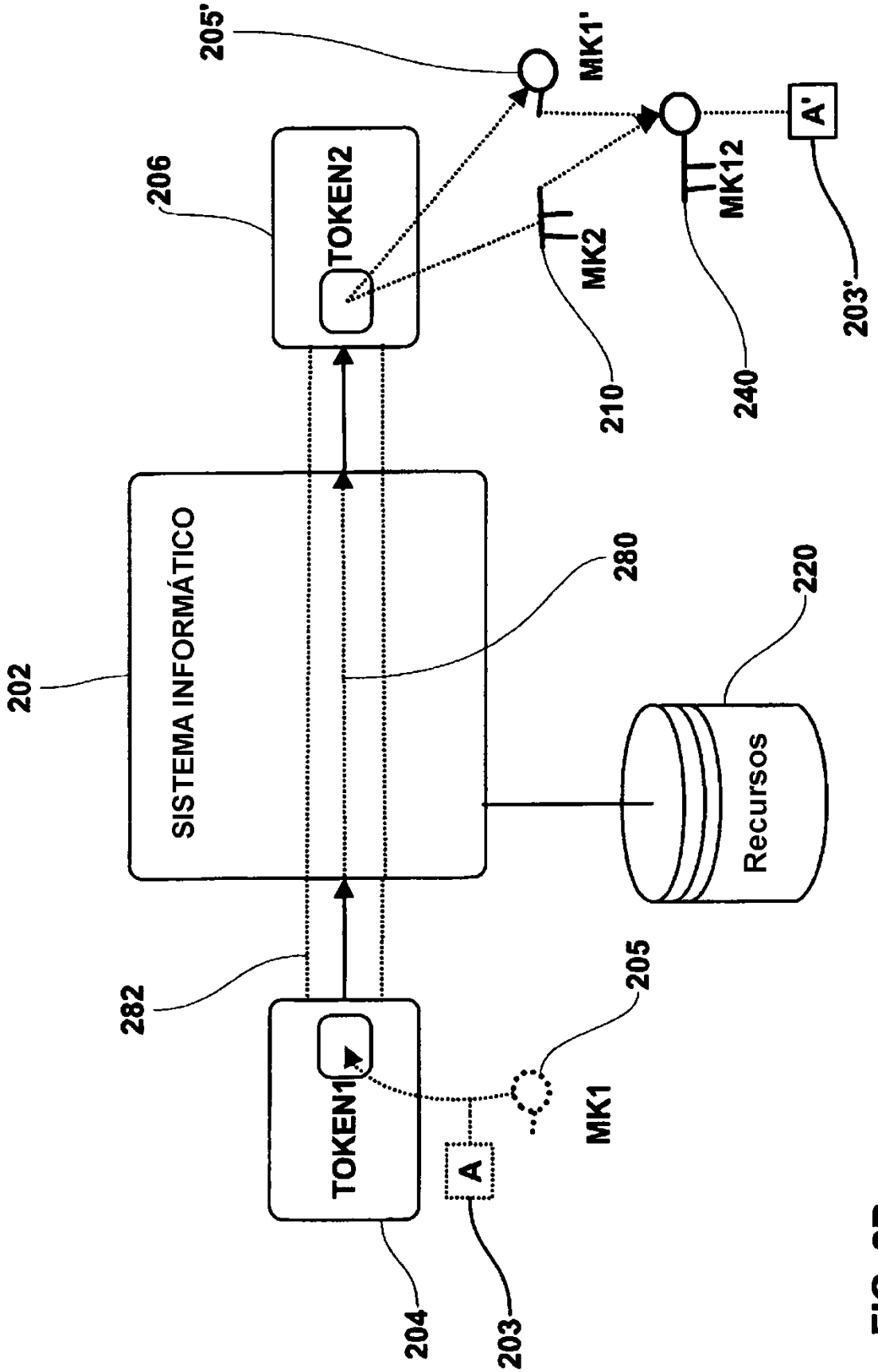
205'
MK1'
206
TOKEN2
MK2
MK12
A'
203'
210
240
SISTEMA INFORMÁTICO
202
280
220
Recursos
282
205
TOKEN1
MK1
A
204
203

FIG. 2B

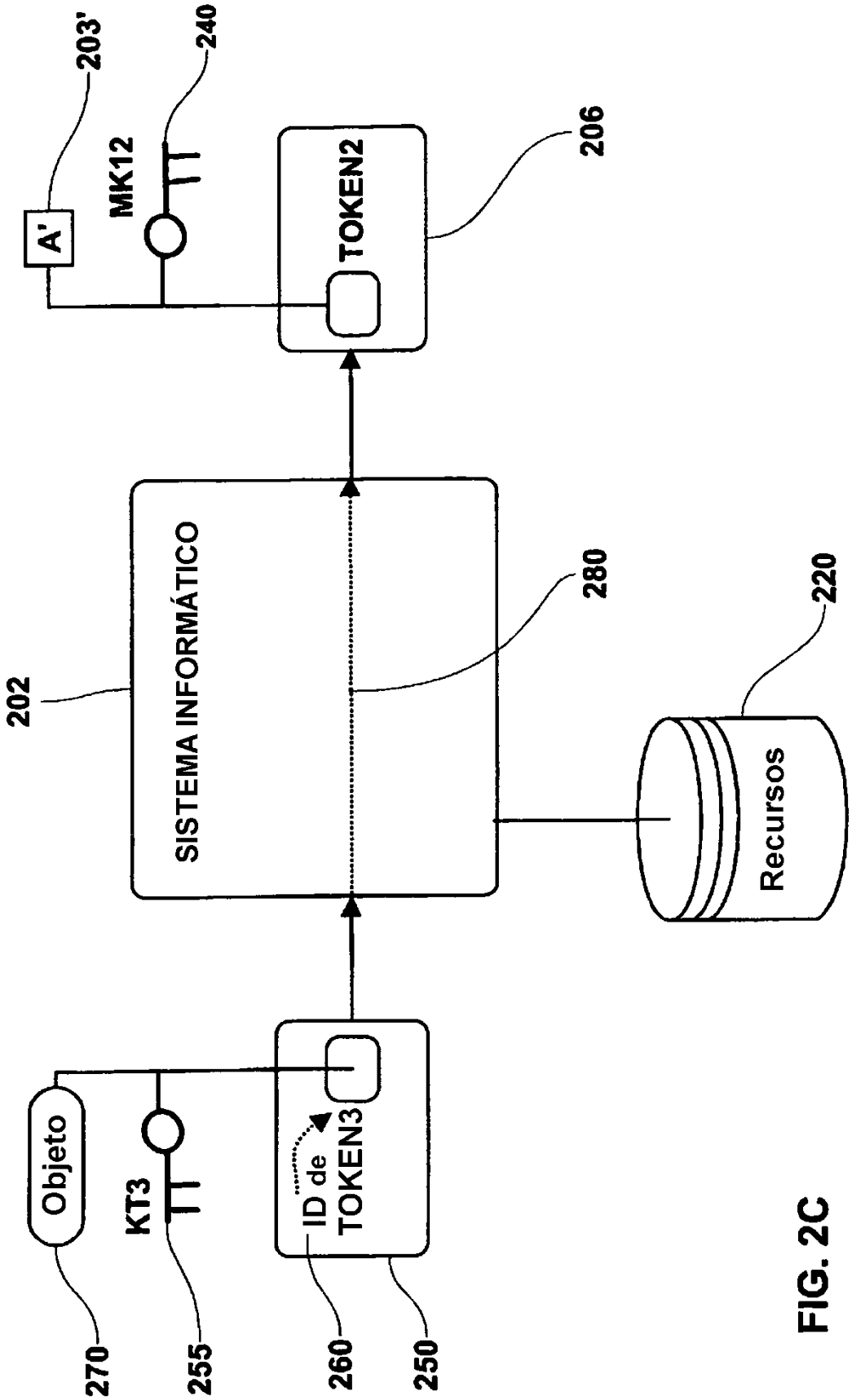
203'
240
MK12
A'
TOKEN2
206
SISTEMA INFORMÁTICO
202
280
220
Recursos
Objeto
KT3
ID de
TOKEN3
270
255
260
250

FIG. 2C

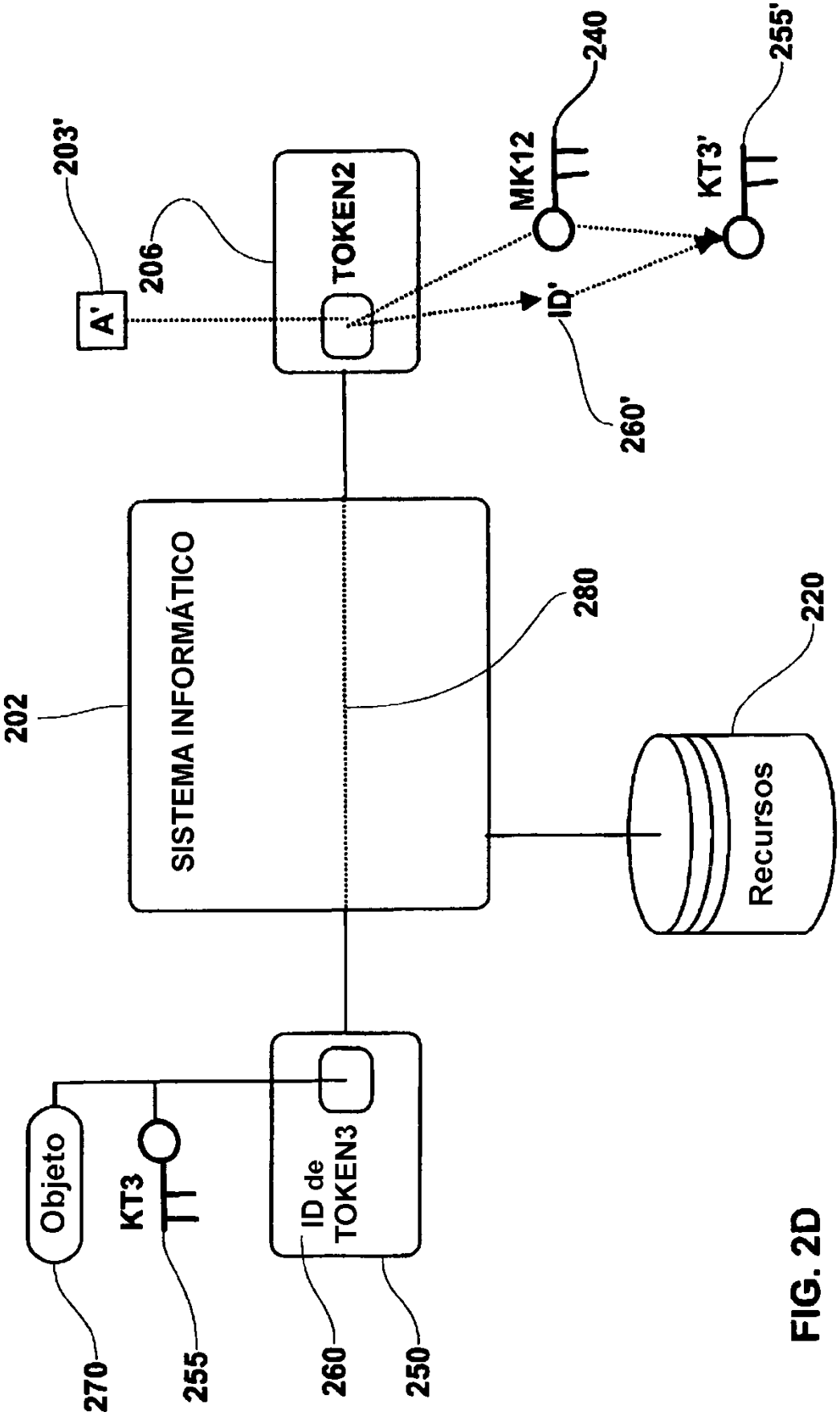
203'
206
A'
TOKEN2
MK12
240
KT3'
255'
ID'
260'
202
SISTEMA INFORMÁTICO
280
220
Recursos
Objeto
KT3
ID de TOKEN3
270
255
260
250

FIG. 2D

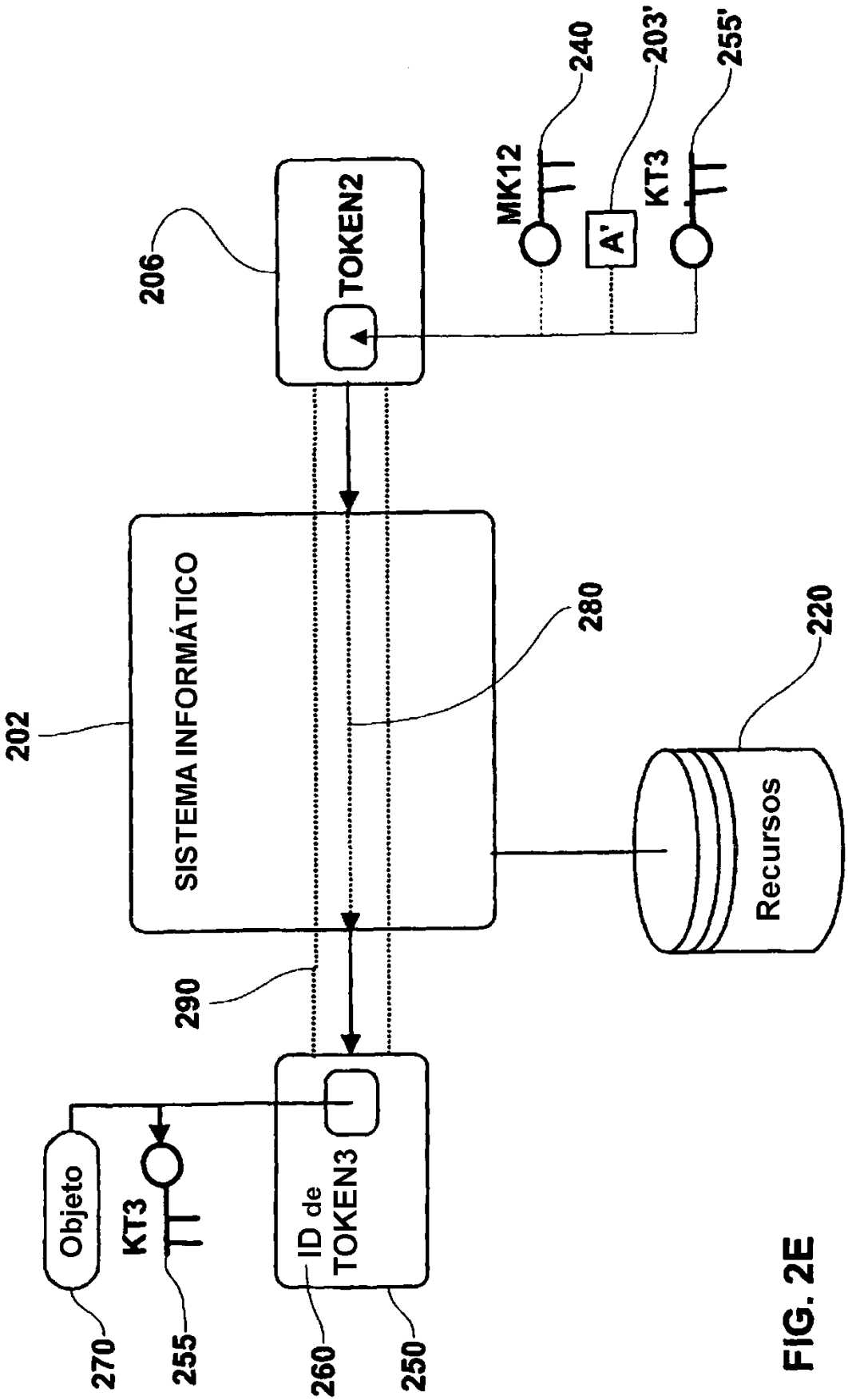
206
TOKEN2
MK12
240
A'
203'
KT3
255'
202
SISTEMA INFORMÁTICO
280
220
Recursos
290
Objeto
KT3
ID de
TOKEN3
270
255
260
250

FIG. 2E

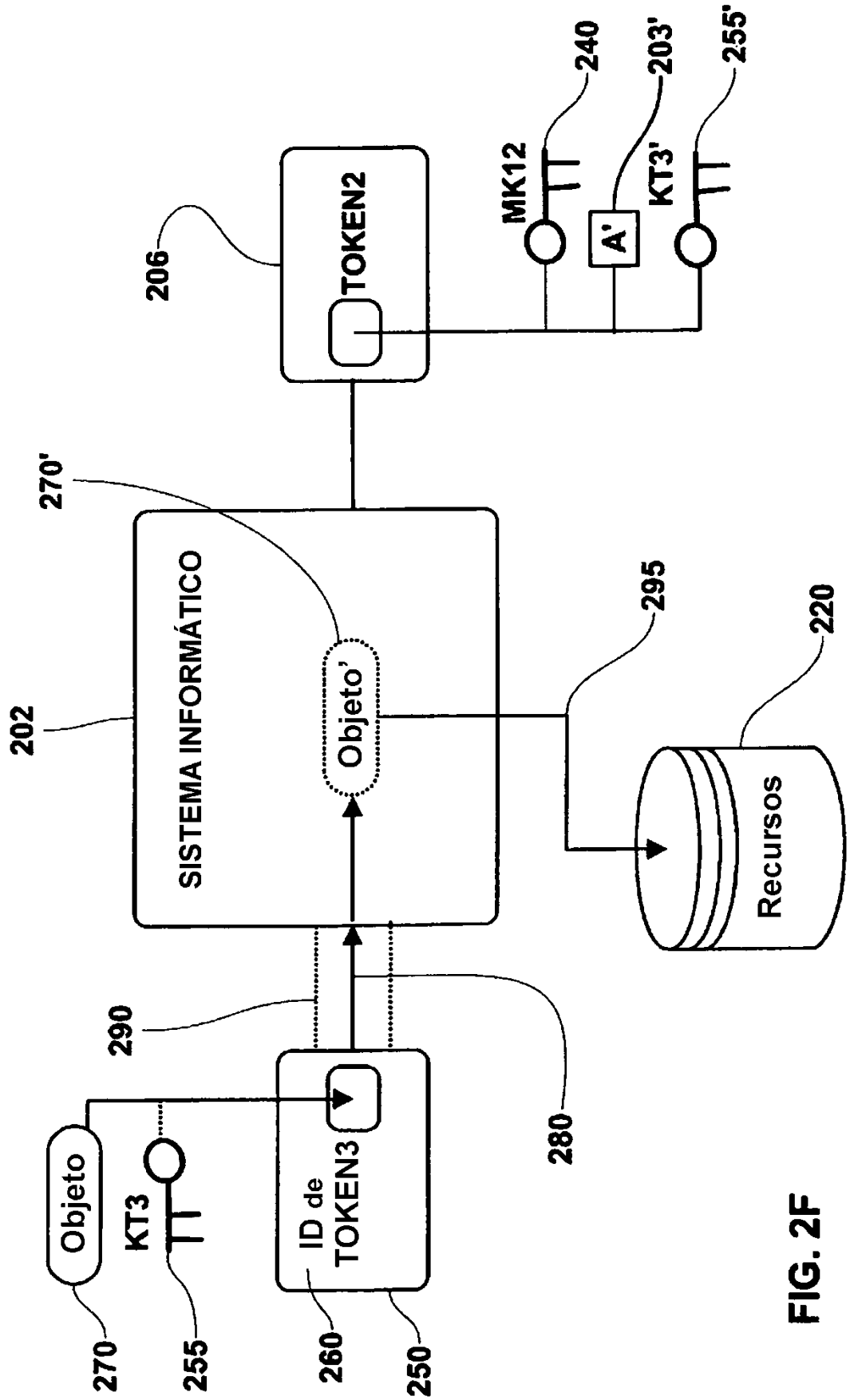
206
TOKEN2
240
MK12
A'
203'
KT3'
255'
270'
202
SISTEMA INFORMÁTICO
Objeto'
295
220
Recursos
290
280
Objeto
KT3
ID de TOKEN3
270
255
260
250

FIG. 2F

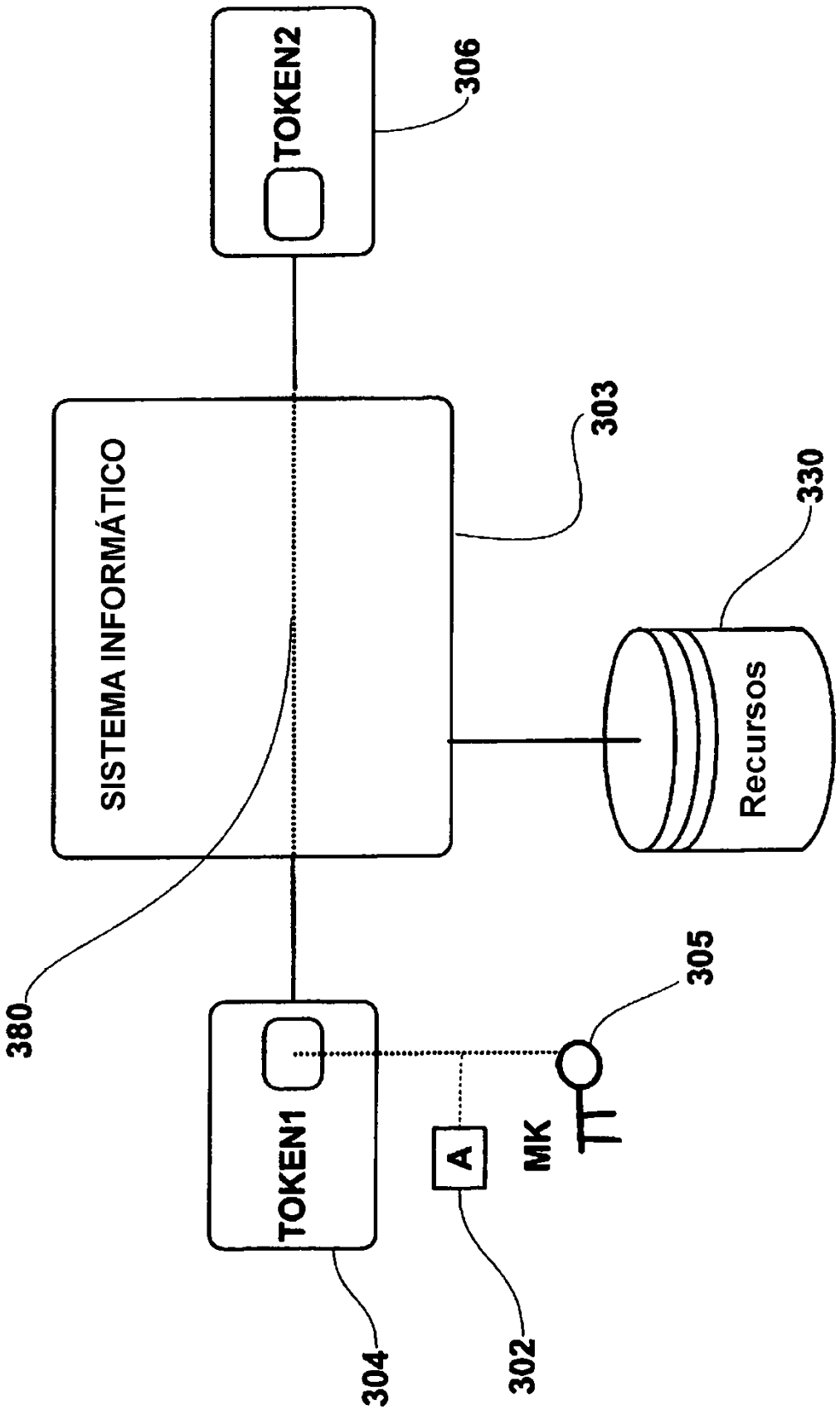
TOKEN2
306
SISTEMA INFORMÁTICO
303
330
Recursos
380
TOKEN1
A
MK
305
304
302

FIG. 3

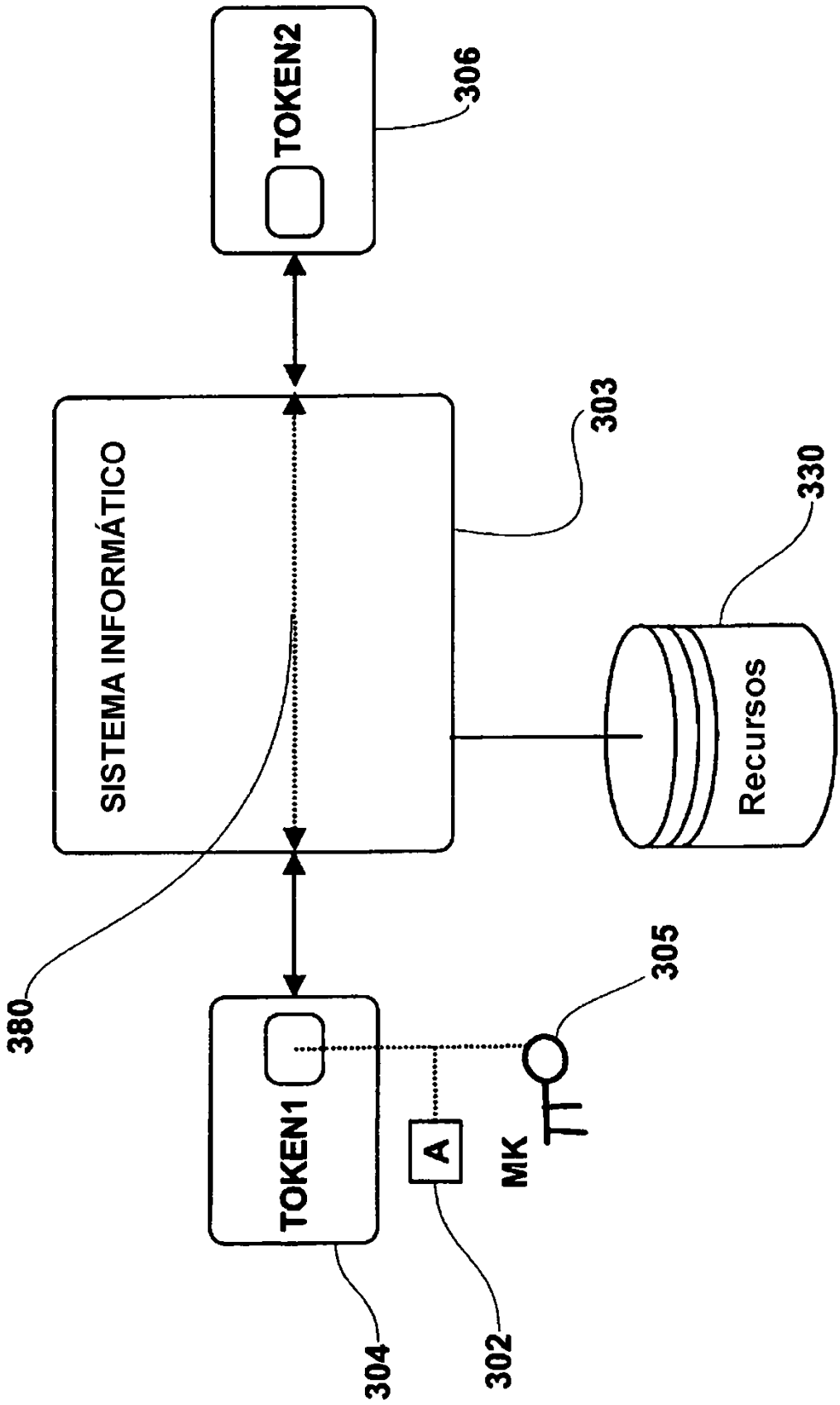
TOKEN2
306
SISTEMA INFORMÁTICO
303
330
Recursos
380
305
TOKEN1
A
MK
304
302

FIG. 3A

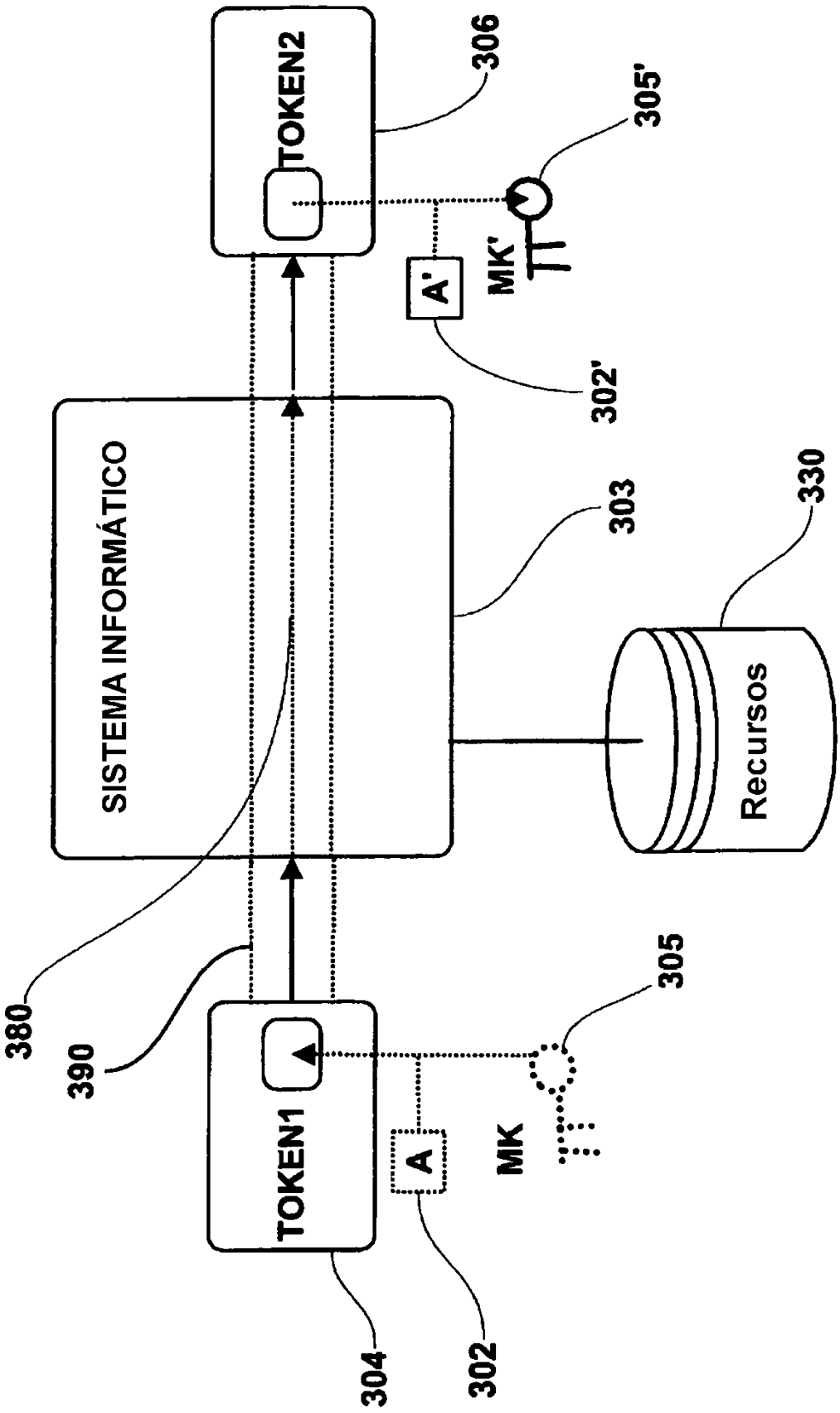
TOKEN2
306
305'
MK'
A'
302'
SISTEMA INFORMÁTICO
303
330
Recursos
380
390
TOKEN1
A
MK
305
304
302

FIG. 3B

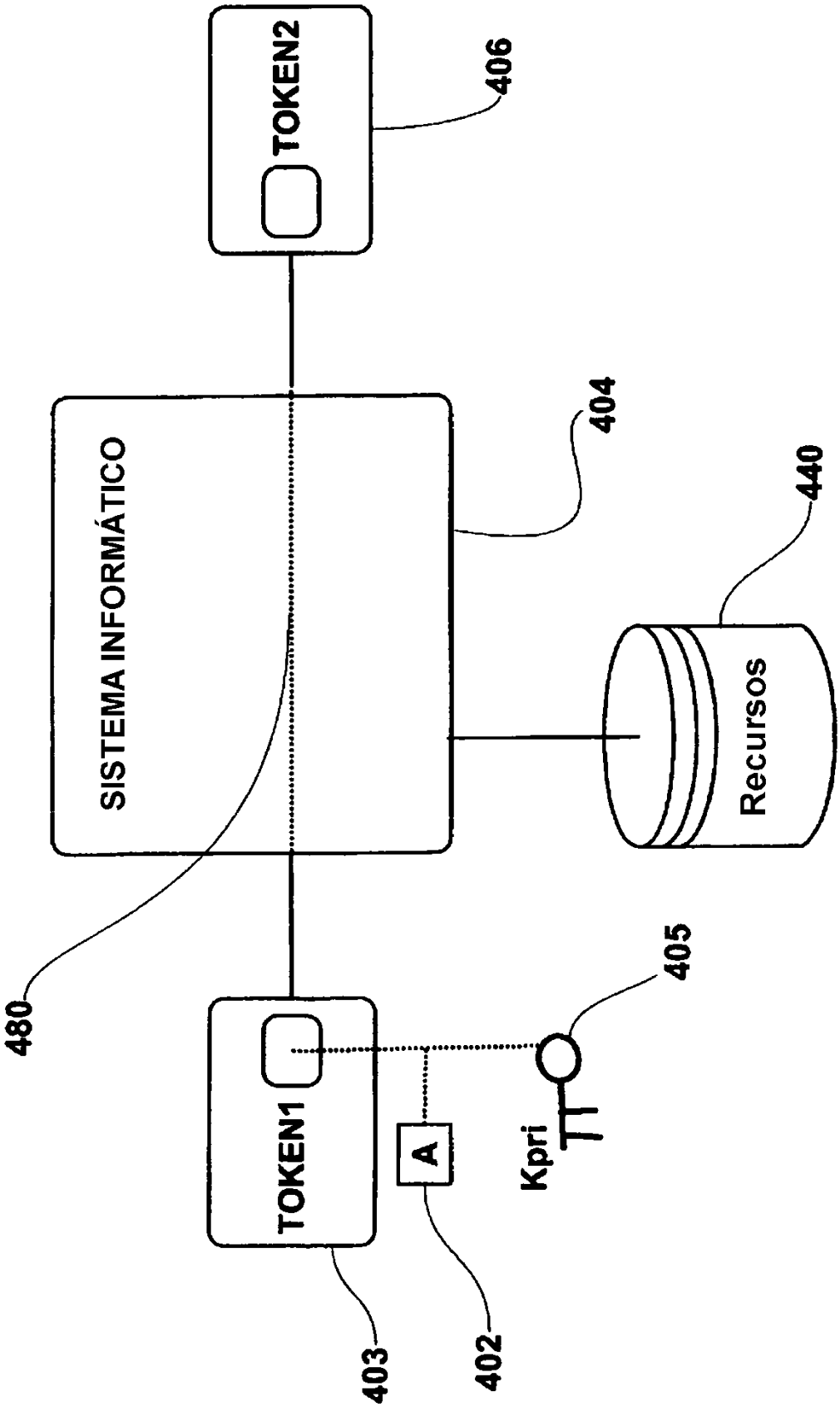
TOKEN2
406
SISTEMA INFORMÁTICO
404
440
Recursos
480
405
TOKEN1
A
Kpri
403
402

FIG. 4

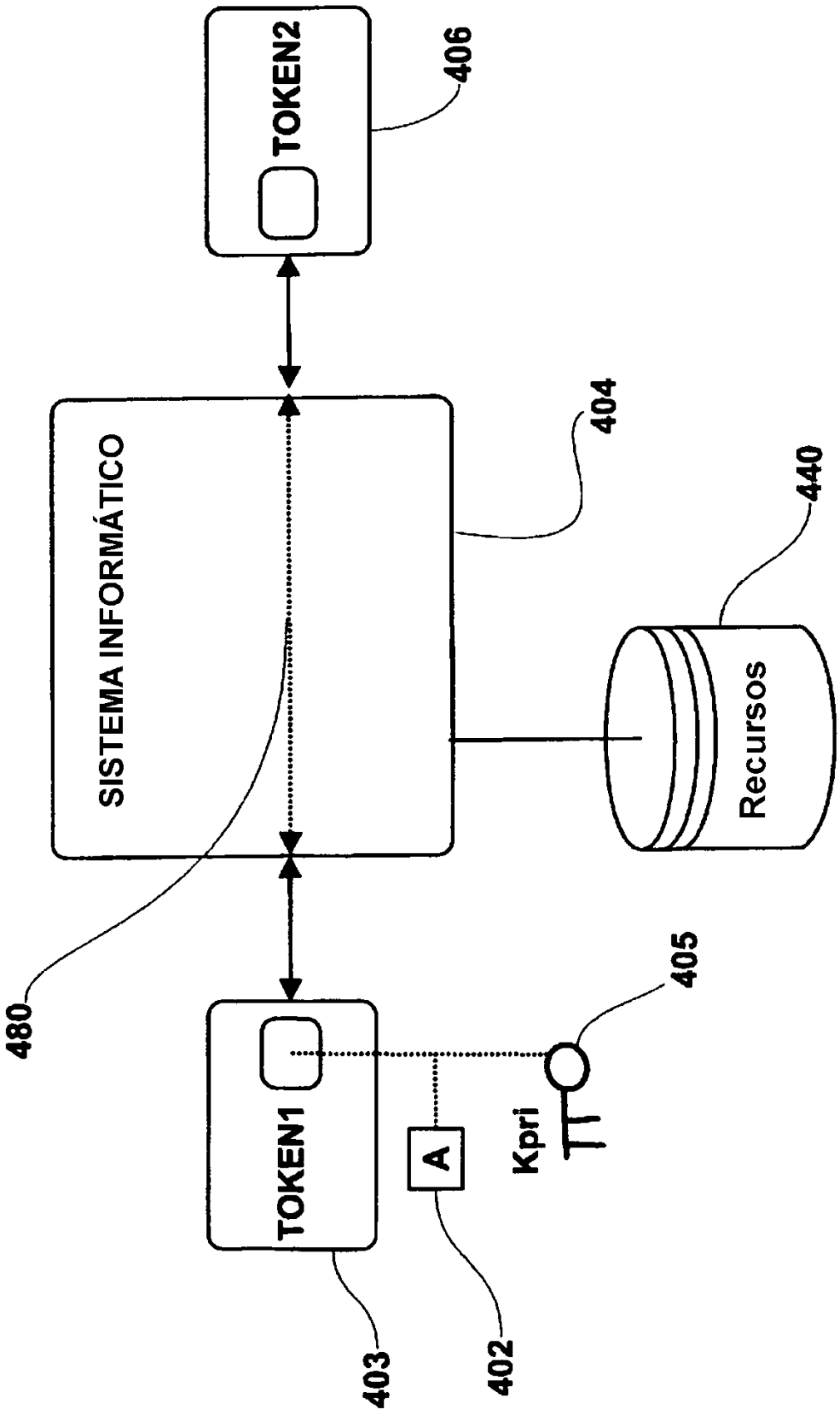
TOKEN2
406
SISTEMA INFORMÁTICO
404
440
Recursos
480
405
TOKEN1
A
Kpri
403
402

FIG. 4A

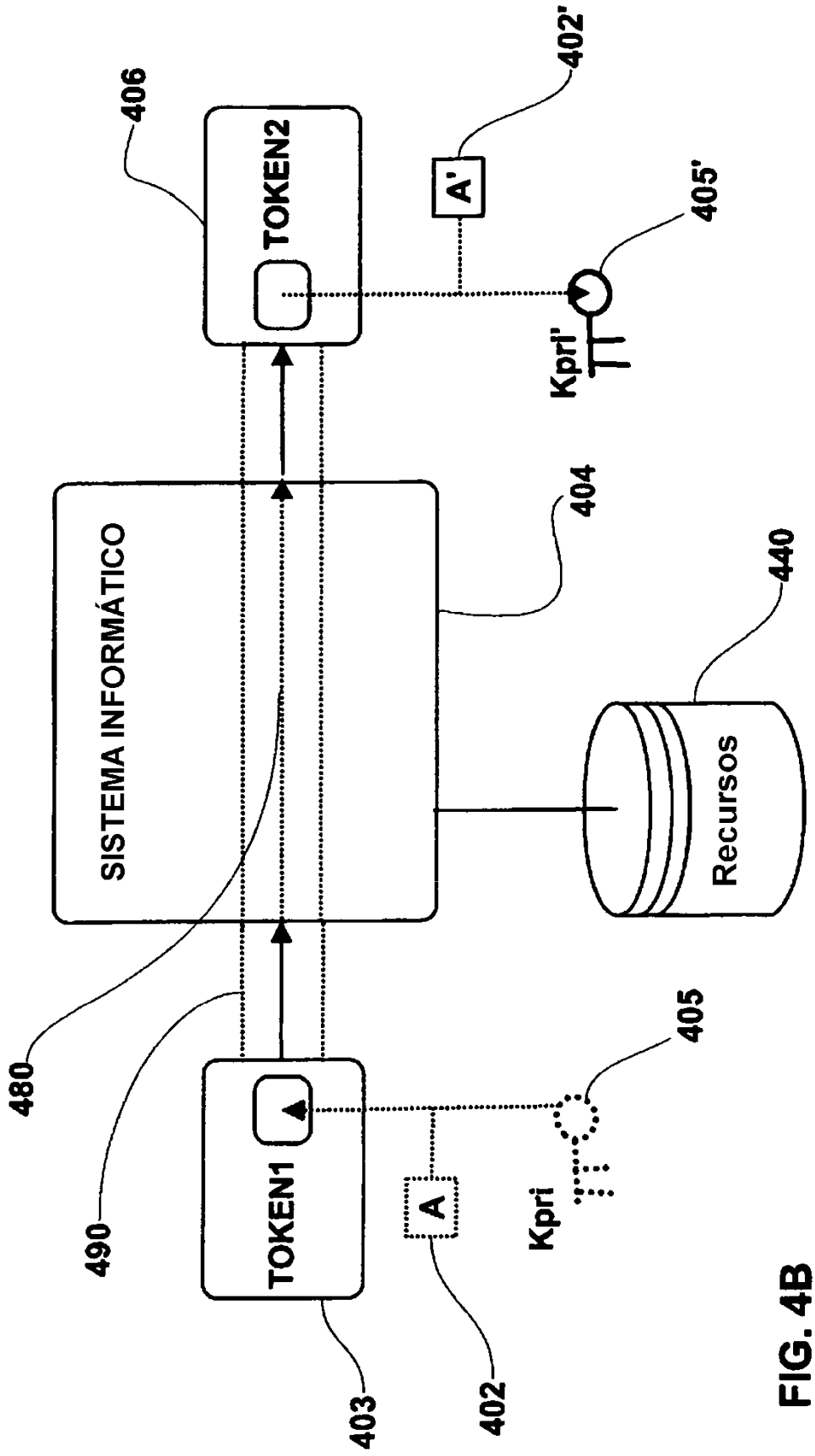
406
TOKEN2
402'
A'
405'
Kpri'
SISTEMA INFORMÁTICO
404
440
Recursos
480
490
TOKEN1
A
Kpri
405
403
402

FIG. 4B

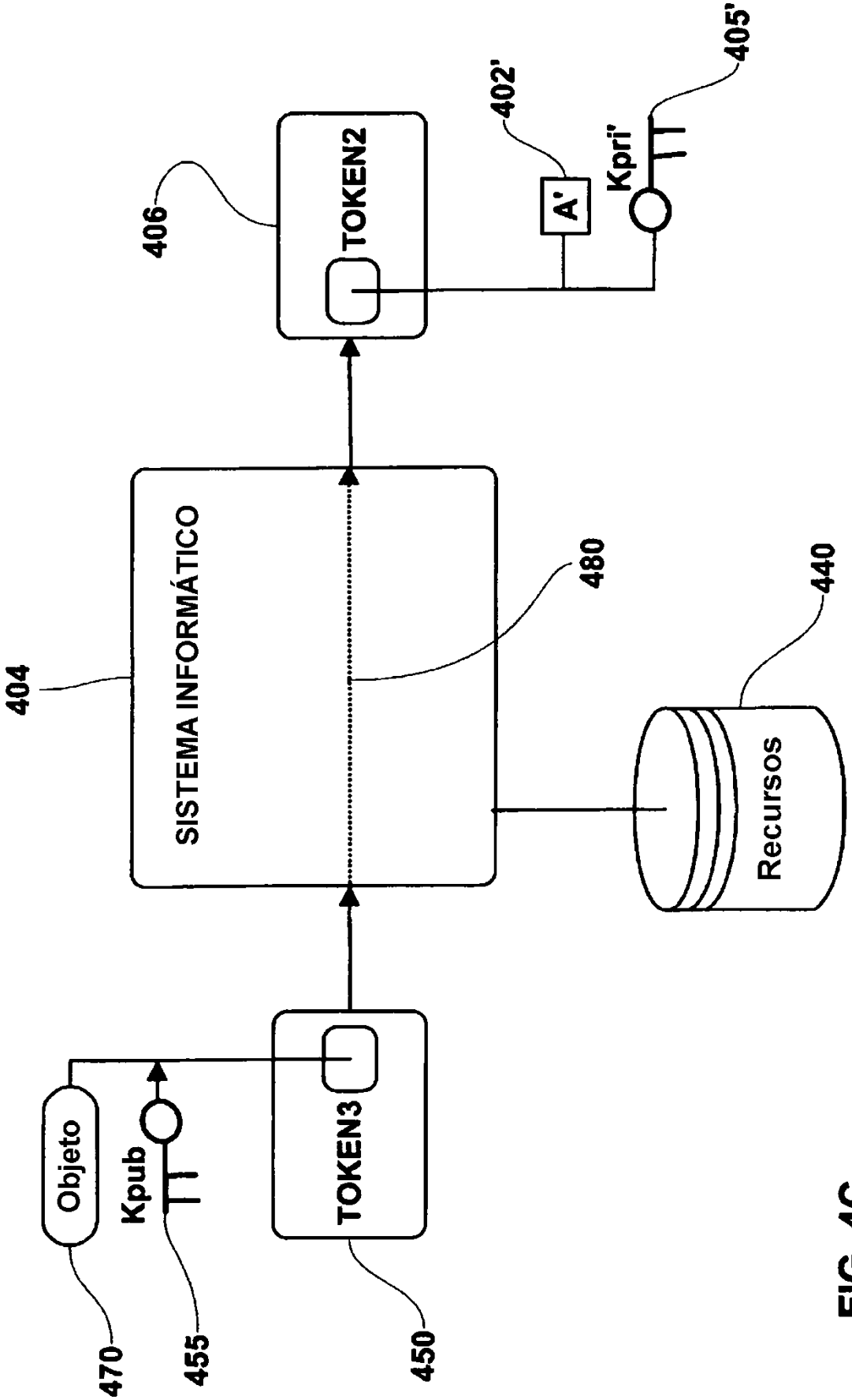
Objeto
Kpub
TOKEN3
SISTEMA INFORMÁTICO
Recursos
TOKEN2
A'
Kpri'
470
455
450
404
480
440
406
402'
405'

FIG. 4C

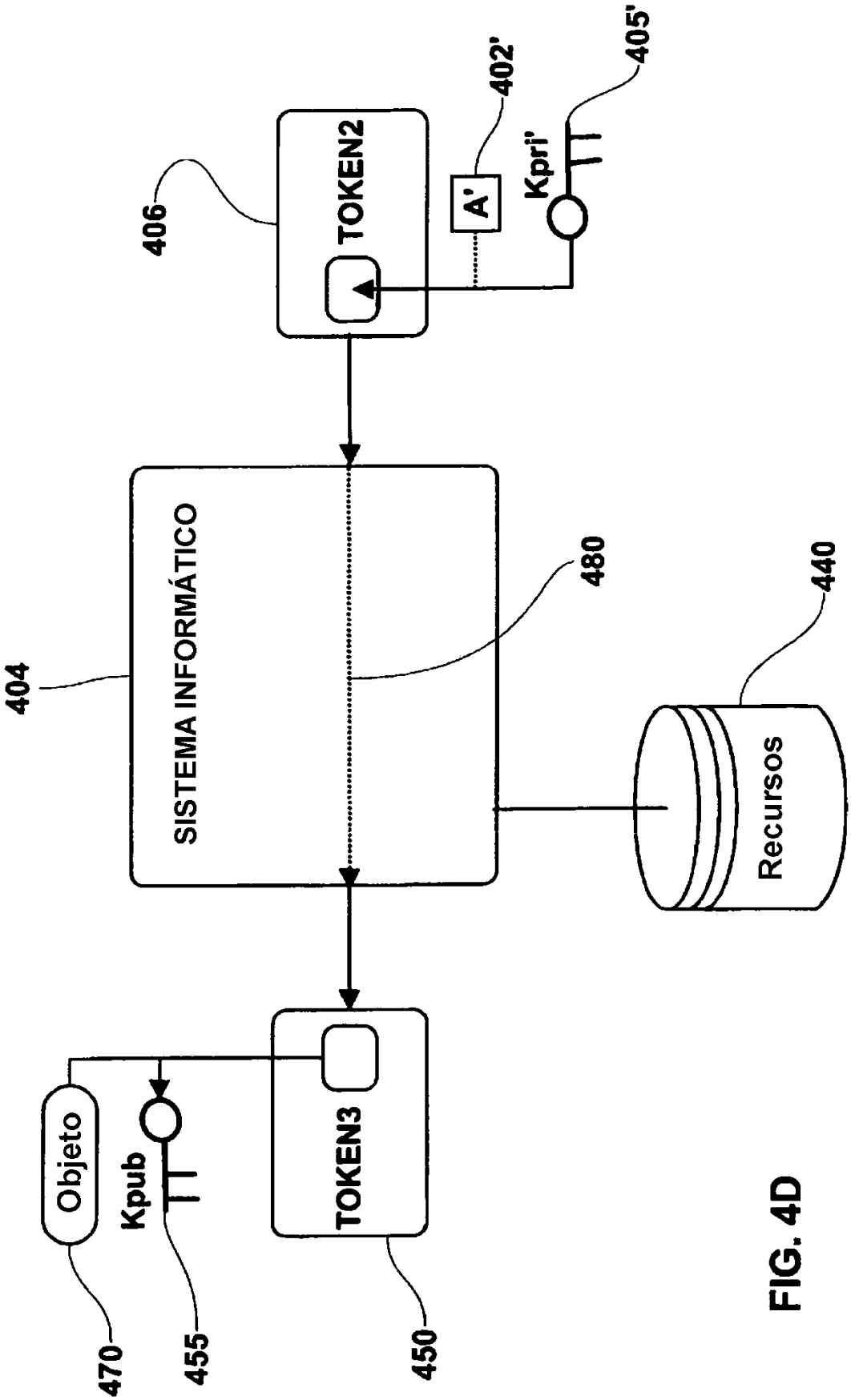
406
TOKEN2
402'
A'
Kpri'
405'
404
SISTEMA INFORMÁTICO
480
440
Recursos
Objeto
Kpub
TOKEN3
470
455
450

FIG. 4D

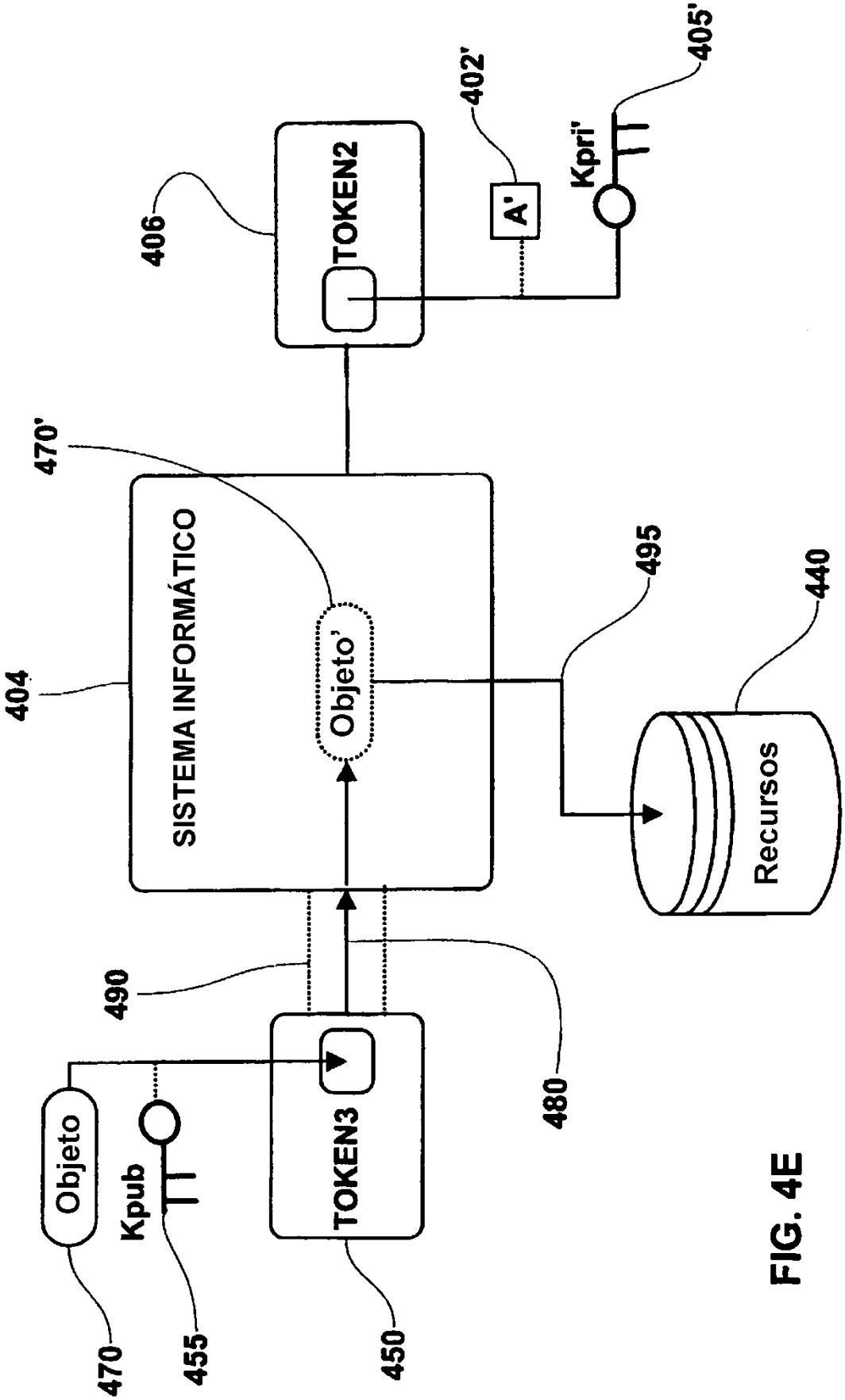
405'
402'
406
TOKEN2
A'
Kpri'
470'
SISTEMA INFORMÁTICO
Objeto'
404
495
440
Recursos
490
480
Objeto
Kpub
TOKEN3
470
455
450

FIG. 4E

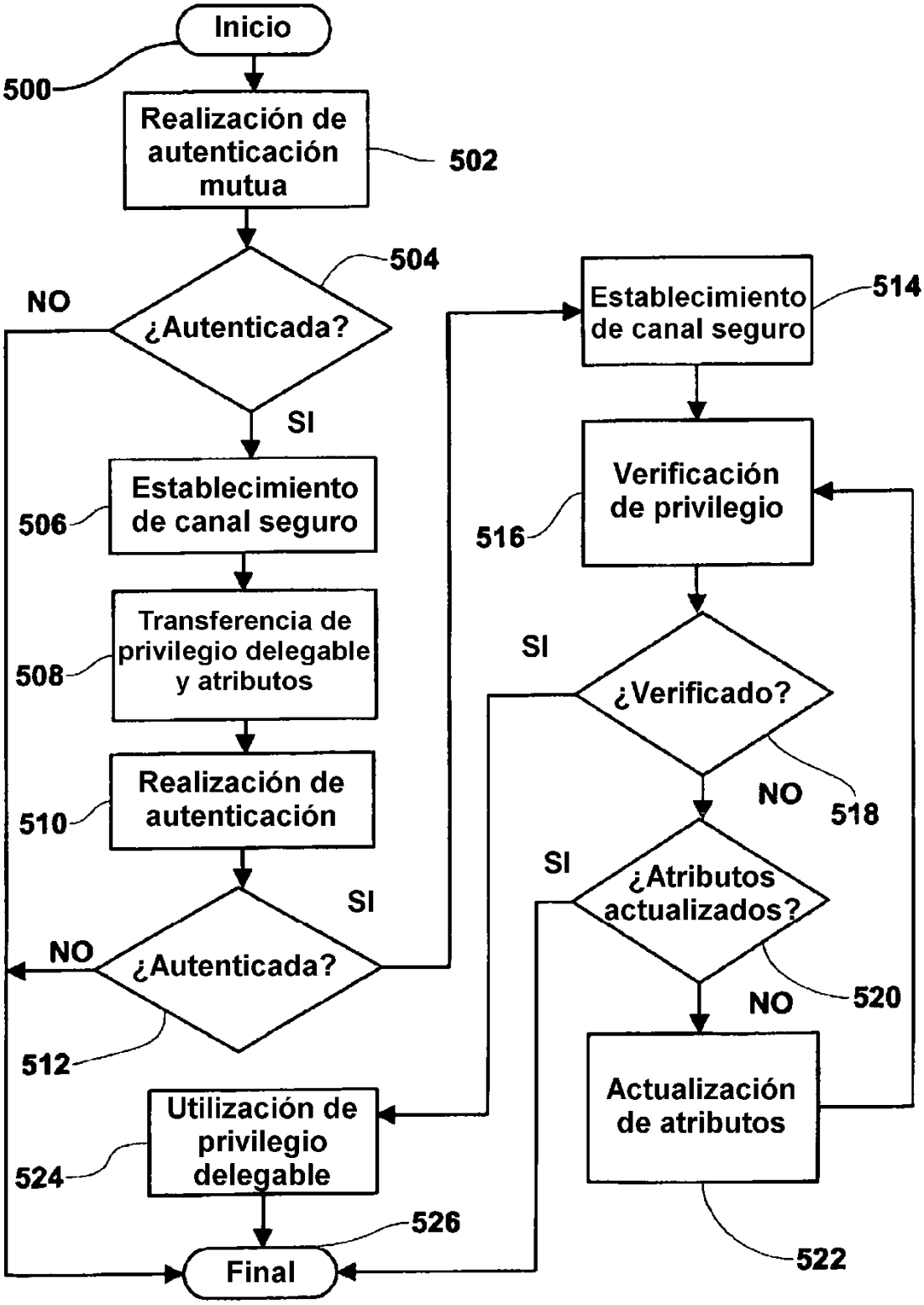
Inicio
500
Realización de autenticación mutua
502
504
NO
¿Autenticada?
SI
Establecimiento de canal seguro
506
Transferencia de privilegio delegable y atributos
508
Realización de autenticación
510
SI
NO
¿Autenticada?
512
Establecimiento de canal seguro
514
Verificación de privilegio
516
SI
¿Verificado?
NO
518
SI
¿Atributos actualizados?
NO
520
Actualización de atributos
522
Utilización de privilegio delegable
524
526
Final

FIG. 5

PRIVILEGIOS

Componente de clave

Clave criptográfica

Certificado de atributos de privilegios

Ticket digital

Credenciales digitales

Contraseña

Plantilla biométrica

Crédito de fidelización

FUNCIONES DE PRIVILEGIO

Operaciones de sustitución

Activación de terminales

Personalización de dispositivo inteligente

Acceso a recursos

Gestión de créditos de fidelización

ATRIBUTOS

ASPECTOS DE CONTROL

Activar/destruir

Políticas de seguridad

Período de validez

N.º de usos restantes

Límites de tiempo

Medidas criptográficas

Almacenamiento (permanente o transitorio)

ESTADOS DE PRIVILEGIO

Inactivo

En arranque

Modo seguro

Modo inseguro

Suspendido

INFORMATIVOS

Nombre de usuario

ID de usuario

Nombre de dominio

Nombre de cliente

Nombre de sistema principal

ID de testigo

FIG.6