(19) OFICINA ESPAÑOLA DE PATENTES Y MARCAS

ESPAÑA

(11) Número de publicación: **2 388 215**

(51) Int. CI.:
H04L 29/06 (2006.01)
G07C 9/00 (2006.01)

(12) TRADUCCIÓN DE PATENTE EUROPEA T3

(96) Número de solicitud europea: **04293091 .7**
(96) Fecha de presentación: **22.12.2004**
(97) Número de publicación de la solicitud: **1549020**
(97) Fecha de publicación de la solicitud: **29.06.2005**

(54) Título: **Sistema de control de entrada**

(30) Prioridad:
22.12.2003 US 740518

(45) Fecha de publicación de la mención BOPI:
10.10.2012

(45) Fecha de la publicación del folleto de la patente:
10.10.2012

(73) Titular/es:
ACTIVCARD INC.
6623 DUMBARTON CIRCLE
FREMONT, CA 94555, US

(72) Inventor/es:
Fedronic, Dominique Louis Joseph y
Wen, Wu

(74) Agente/Representante:
Curell Aguilá, Mireia

DESCRIPCIÓN

Sistema de control de entrada.

Campo de la invención

La presente invención se refiere en general a un procedimiento y un sistema de procesamiento de datos y, más particularmente, a un sistema de control de acceso físico de comunicaciones inalámbricas que combina controles de acceso físicos y lógicos que utilizan las características de seguridad proporcionadas por la implementación de testigos de seguridad con protocolos de autenticación normalizados.

Antecedentes

Los últimos acontecimientos mundiales y la creciente competencia internacional han acelerado los esfuerzos por fusionar sistemas de seguridad físicos y lógicos, particularmente para grandes empresas comerciales, industriales y gubernamentales. No obstante, estos esfuerzos de fusión se han visto notablemente obstaculizados por la gran infraestructura de sistemas físicos de seguridad instalados sujetos a derechos de propiedad. Estos sistemas físicos de seguridad prioritarios a menudo utilizan arquitecturas de red, protocolos de comunicaciones, bases de datos y sistemas de archivos con derechos de propiedad que son difíciles de integrar en los sistemas modernos de seguridad de red. Se describe un ejemplo de sistema de seguridad con derecho de propiedad en la patente US nº 5.682.142 de Loosmore *et al*. El documento de referencia de Loosmore da a conocer un sistema de seguridad integrado que está dispuesto para funcionar como un sistema de seguridad autónomo separado.

Las incompatibilidades entre los sistemas de seguridad físicos y lógicos provocan a menudo deficiencias graves en los sistemas de seguridad físicos, lógicos o en ambos tipos. En un ejemplo reciente de una base de datos de recursos humanos, se indicaba el despido de un empleado, aunque en el acceso al correo electrónico y la red el exempleado todavía constaba como activo, hecho que podría haber permitido el acceso lógico del exempleado a los recursos de la empresa. D.Smith describe este ejemplo en la revista *esecure*, de septiembre de 2002 (22) que puede consultarse. Aunque este ejemplo ilustra mejor las incompatibilidades lógicas entre las diferentes bases de datos institucionales, no es difícil imaginar una situación similar en la que una tarjeta de acceso físico se mantiene en estado activo, debido a incompatibilidades entre los sistemas físicos y lógicos de seguridad. Esta cuestión es particularmente importante en instalaciones susceptibles de ser afectadas, tales como los aeropuertos, en las que una tarjeta de acceso físico perdida, robada o indebidamente gestionada podría conducir al secuestro de un avión.

Otro impedimento para la fusión de los sistemas físicos y lógicos de seguridad es la falta de normas oficiales especialmente elaboradas para los sistemas físicos de seguridad.

Los profesionales de TI, partidarios del uso de arquitecturas abiertas de sistemas informáticos, protocolos de red normalizados y sistemas de bases de datos normalizados, tales como el ODBC, están promulgando normas de facto. Se describe un ejemplo de sistema de seguridad físico y lógico integrado en la patente US nº 6.233.588 de Marchoili *et al*. Aunque el documento de referencia de Marchoili trata sobre la falta de normalización de las capacidades informáticas de los sistemas de seguridad físicos y lógicos centralizados, no trata sobre la falta de normalización de los controladores de seguridad que deben interactuar con los sistemas de seguridad.

La falta de normalización de los controladores de seguridad todavía constituye un impedimento importante para la fusión de los sistemas físicos y lógicos de seguridad, en la medida en que muchos clientes de seguridad todavía carecen de capacidades de interfaz de red normalizadas. Por ejemplo, la empresa HID Corporation ofrece un controlador de puertas avanzado que se acciona mediante una tarjeta inteligente sin contacto y se denomina MIFARE ® (6055B). La implementación avanzada de una tarjeta inteligente sin contacto proporciona unos medios prácticos y seguros para usar con los sistemas de seguridad tanto físicos como lógicos. Sin embargo, uno de los principales inconvenientes de este controlador de seguridad es la falta de una interfaz de red normalizada. En su lugar, el controlador está provisto de una interfaz RS-232C para la conexión local con un sistema de ordenador personal normalizado#. (Véase la hoja de referencia de HID MIFARE ® (6055B), MRG-EN-US, rev. 10-02, que puede consultarse.)

La interfaz RS-232C se utiliza para cargar o actualizar localmente una memoria caché asociada al controlador de seguridad con los códigos de tarjeta inteligente autorizados, mediante software y protocolos de comunicación de propiedad que se ejecutan en un ordenador personal. Esta disposición limita la escalabilidad, requiere la gestión individual de los controles remotos de seguridad e impide la aplicación de cambios dinámicos y centralizados a los códigos de tarjeta inteligente autorizados.

Otros proveedores de controladores de seguridad sí que ofrecen capacidades de interfaz de red normalizadas, pero generalmente comprenden contraseñas estáticas vulnerables y/o codificación de autenticación de propiedad que están lejos de ser ideales, especialmente en implementaciones inalámbricas del controlador de seguridad en desarrollo en las que las comunicaciones con un sistema de seguridad centralizado pueden interceptarse con más facilidad. En muchos casos, los controladores de seguridad son dirigidos habitualmente hacia un panel de control

centralizado mediante un enlace en serie, que a continuación se conecta con una red normalizada.

El documento EP 0 913 979 describe un sistema que comprende un centro de control, un teléfono de móvil y un objeto en el cual se halla un dispositivo que se puede activar a distancia. Los datos se transmiten desde un transmisor situado en el teléfono móvil hasta un receptor del objeto remoto que se desea controlar. Los datos (por ejemplo, pulsaciones o patrones de voz) se introducen en el teléfono móvil, a fin de que el centro de control los utilice para la autenticación. Tras la autenticación de los datos, el centro de control envía al teléfono móvil una señal específica que indica que la autenticación ha resultado positiva, y el teléfono móvil convierte la señal específica en una señal de habilitación. Entonces, la señal de habilitación se envía al objeto controlado a distancia, donde se activa un circuito electromecánico conectado al objeto controlado a distancia.

El documento FR 2 695 364 da a conocer un sistema antirrobo que se utiliza con automóviles provistos de un sistema de apertura y cierre remoto por infrarrojos instalado en las puertas. El sistema presenta un transmisor de infrarrojos portátil y un receptor de infrarrojos fijado al vehículo, que están conectados con el microordenador de control de encendido e inyección del vehículo. El receptor de infrarrojos transmite una trama codificada al ordenador de control del motor para permitir a este continuar con la transmisión de operaciones de encendido e inyección. El funcionamiento del emisor portátil se pasa por alto fuera de los tiempos de utilización predefinidos.

El documento WO 02091316 da a conocer un procedimiento para activar y/o gestionar por lo menos un dispositivo de seguridad personal (PSD) con por lo menos un primer sistema informático remoto a través de una primera red, utilizando por lo menos un cliente como anfitrión para dicho por lo menos un PSD, comprendiendo dicho procedimiento las etapas siguientes: a) establecimiento de por lo menos una canalización de comunicaciones a través de dicha primera red entre dicho por lo menos un PSD y dicho por lo menos primer sistema informático remoto, b) recuperación de información de propiedad (I) por dicho por lo menos primer sistema informático remoto desde un lugar de almacenamiento remoto, c) transmisión de dicha información de propiedad (I) desde dicho primer sistema informático remoto hasta dicho por lo menos un PSD a través de dicha por lo menos una canalización de comunicaciones y d) almacenamiento y/o procesamiento de dicha información de propiedad (I) en dicho por lo menos un PSD.

Con el mencionado propósito, la presente invención es un procedimiento para controlar físicamente el acceso a un lugar protegido según la reivindicación 1 y un sistema y un controlador de seguridad para controlar físicamente el acceso a un lugar protegido según las reivindicaciones 10 y 18 respectivamente.

Otras características de la presente invención se describen en las reivindicaciones subordinadas.

Así pues, un controlador de seguridad ideal comprendería capacidades de interfaz de red normalizadas, permitiría comunicaciones seguras con un sistema de seguridad integrado incluso a través de enlaces de telecomunicaciones inalámbricas, aprovecharía las ventajas y la seguridad ofrecidas por las tarjetas inteligentes y se integraría perfectamente con los sistemas lógicos de seguridad de generación actual.

Sumario

La presente invención trata sobre muchas de las limitaciones descritas anteriormente y ofrece un sistema de seguridad integrado que se asimila perfectamente a los sistemas lógicos de seguridad de generación actual. El sistema de seguridad integra un controlador de seguridad que presenta capacidades de interfaz de red normalizadas y aprovecha las ventajas y la seguridad ofrecidas por las tarjetas inteligentes y los dispositivos relacionados para finalidades de seguridad tanto físicas como lógicas.

La expresión "parámetro crítico de seguridad" empleado en la presente memoria integra la definición del Instituto nacional de normas y tecnología de EE.UU. (NIST) especificada en la publicación FIPS PUB 140-2, "Security Requirements For Security tokens" y comprende los datos y atributos de autenticación, las contraseñas, los PIN, las muestras biométricas y las claves de encriptación asimétricas y simétricas.

La expresión "testigo de seguridad" empleado en la presente memoria comprende dispositivos de seguridad basados en hardware, tales como módulos criptográficos, tarjetas inteligentes, tarjetas con chip de circuito integrado, soportes de datos portátiles (PDC), dispositivos de seguridad personales (PSD), módulos de identificación del abonado (SIM), módulos de identidad inalámbrica (WIM), mochilas de testigos USB, testigos de identificación, módulos de aplicación segura (SAM), módulos de seguridad de hardware (HSM), símbolos de multimedia segura (SMMC), chips de Trusted Platform Computing Alliance (TPCA) y dispositivos similares.

La parte del procedimiento de la presente invención comprende el establecimiento de una conexión de comunicación segura a través de una red entre un controlador de seguridad y por lo menos un servidor de autenticación, el acoplamiento operativo de un testigo de seguridad con el controlador de seguridad, el envío de un parámetro crítico de seguridad desde el testigo de seguridad hasta el controlador de seguridad para la autenticación, el envío del parámetro crítico de seguridad al servidor de la autenticación por medio de la conexión de comunicación segura, la realización por el servidor de autenticación de una transacción de autenticación para el parámetro crítico de

seguridad y el envío del resultado de la transacción de autenticación desde el servidor de autenticación hasta el controlador de seguridad por medio de la conexión de comunicación segura.

La última acción de la parte del procedimiento de la presente invención activa un circuito electromecánico controlado por el controlador de seguridad si el resultado es afirmativo y confirma que la transacción de autenticación se ha realizado con éxito. El circuito electromecánico está asociado a una puerta de acceso físico que se abre al activarse dicho circuito electromecánico. El circuito electromecánico permanece activado durante un tiempo preestablecido y específico para el testigo de seguridad. Esto permite controlar la apertura de un acceso, tal como una puerta para la entrada de suministros o para facilitar el paso a las personas con discapacidades físicas.

La conexión de comunicaciones segura comprende un secreto compartido establecido entre el controlador de seguridad y el servidor de autenticación, que es mantenido de forma segura por un módulo de acceso seguro acoplado funcionalmente al controlador de seguridad.

El controlador de seguridad es uno de los controladores de seguridad de una pluralidad, la totalidad de los cuales son clientes del servidor de autenticación conectados en red. En una forma de realización de la presente invención, por lo menos una parte de la conexión de comunicaciones segura se establece a través de un enlace de telecomunicaciones inalámbricas que integra un protocolo de seguridad que comprende uno de los protocolos SSL, IPsec, PCT, TLS o RADIUS.

En una forma de realización de la presente invención, el controlador de seguridad se comunica asimismo de forma segura a través de la red con un servidor de administración de ciclo de vida. El servidor de administración de ciclo de vida está adaptado para realizar funciones de administración del ciclo de vida relacionadas con las aplicaciones, los parámetros críticos de seguridad o los datos de usuario instalados en el testigo de seguridad o el módulo de acceso seguro.

Breve descripción de los dibujos

Las características y las ventajas de la presente invención se pondrán de manifiesto a partir de la siguiente descripción detallada considerada conjuntamente con los dibujos adjuntos. En la medida de lo posible, se utilizan los mismos números y caracteres de referencia para denotar características, elementos, componentes o partes similares de la presente invención. Se prevé la posibilidad de aplicar cambios y modificaciones a la forma de realización descrita sin abandonar el alcance verdadero de la presente invención definido en las reivindicaciones adjuntas.

La figura 1 es un diagrama de bloques general de un servidor de autenticación activado por testigo de seguridad.

La figura 1A es un diagrama de bloques general de un controlador de seguridad.

La figura 1B es un diagrama de bloques general de un testigo de seguridad.

La figura 2 es un diagrama de bloques detallado de una forma de realización de la presente invención, en la que un servidor de autenticación activado por testigo establece comunicaciones de procesamiento con un controlador de seguridad a través de un enlace de telecomunicaciones inalámbricas.

La figura 2A es un diagrama de bloques detallado de la presente invención, en la que se establece un secreto compartido entre el servidor de autenticación y el controlador de seguridad como parte del protocolo de autenticación RADIUS.

La figura 2B es un diagrama de bloques detallado de la presente invención, en la que se envía de forma segura un parámetro crítico de seguridad al servidor de autenticación para la autenticación.

La figura 2C es un diagrama de bloques detallado de la presente invención, en la que el servidor de autenticación realiza una transacción de autenticación utilizando el parámetro crítico de seguridad recibido.

La figura 2D es un diagrama de bloques detallado de la presente invención, en la que se genera un resultado afirmativo de la transacción de autenticación y este se envía de forma segura al controlador de seguridad.

La figura 2E es un diagrama de bloques detallado de la presente invención, en la que se realiza una transacción de administración de ciclo de vida entre el módulo de acceso seguro y el servidor de autenticación.

La figura 2Fes un diagrama de bloques detallado de otra forma de realización de la presente invención, en la que un módulo de acceso seguro asociado a un controlador de seguridad autentica localmente un parámetro crítico de seguridad.

La figura 2G es un diagrama de bloques detallado de otra forma de realización de la presente invención, en la que

se realiza una o más transacciones de administración de ciclo de vida entre un servidor de administración de ciclo de vida, el servidor de autenticación, el módulo de acceso seguro y el testigo de seguridad.

La figura 3 es un diagrama de flujo que ilustra las etapas principales asociadas al control físico del acceso a un lugar protegido mediante la presente invención.

La figura 3A es un diagrama de flujo que ilustra las etapas principales asociadas a la realización de una transacción de administración de parámetro crítico de seguridad entre el módulo de acceso seguro y el servidor de autenticación.

La figura 3B es un diagrama de flujo que ilustra las etapas principales asociadas a la realización local de una autenticación de parámetro crítico de seguridad y el envío de una lista de acceso al servidor de autenticación.

Descripción detallada

La presente invención ofrece un sistema de seguridad integrado que se asimila perfectamente a los sistemas lógicos de seguridad de generación actual. El sistema de seguridad integrado comprende un controlador de seguridad que presenta capacidades de interfaz de red normalizadas y aprovecha las ventajas y la seguridad ofrecidas por las tarjetas inteligentes y los dispositivos relacionados para finalidades de seguridad tanto físicas como lógicas. La presente invención se basa de forma no limitativa en las tecnologías de comunicaciones seguras normalizadas conocidas en el ámbito de la técnica correspondiente, que comprenden los protocolos de capa de conexión segura (SSL), seguridad de capa de transporte (TLS), tecnología de comunicaciones privadas (PCT), seguridad de protocolo de Internet (IPsec) o servicio de autenticación remota de llamadas de usuarios (RADIUS).

La utilización de las tecnologías de comunicaciones seguras está respaldada por la capa de enlace IEEE 802.1x, lo cual hace que estos protocolos sean muy adecuados para las comunicaciones seguras en redes de comunicaciones inalámbricas, tales como las 802.11a, 802.11b y 802.11g. También son compatibles por supuesto otras disposiciones que utilizan redes fijas u ópticas basadas en la norma IEEE 802.22.

Con referencia a la figura 1, se ilustra un diagrama de bloques de un servidor de autenticación 105. El servidor de autenticación 105 comprende un procesador 5, una memoria principal 10, una pantalla 20 acoplada eléctricamente a una interfaz de pantalla 15, un subsistema de memoria secundaria 25 conectado eléctricamente a una unidad de disco duro 30, una unidad de memoria extraíble 35 acoplada eléctricamente a un dispositivo de memoria extraíble 40 y una interfaz de memoria auxiliar extraíble 45 conectada eléctricamente a un dispositivo de memoria auxiliar extraíble 50.

El subsistema de interfaz de comunicaciones 55 está acoplado a un transceptor de red 60 y una red 65, un testigo de seguridad opcional 75, tal como un módulo de seguridad de hardware (HSM) que está asociado eléctricamente a una interfaz de testigo de seguridad 70 y una interfaz de entrada de usuario 80 que comprende un ratón y un teclado 85, y un escáner biométrico opcional 95 que está acoplado eléctricamente a una interfaz de escáner biométrico opcional 90.

El procesador 5, la memoria principal 10, la interfaz de pantalla 15, el subsistema de memoria secundaria 25 y el sistema de interfaz de comunicaciones 55 están acoplados eléctricamente a una infraestructura de comunicaciones 100. El servidor de autenticación 105 comprende un sistema operativo, software de autenticación, aplicaciones de comunicaciones seguras, software para otras aplicaciones, software de criptografía capaz de realizar funciones de criptografía simétricas y asimétricas, software de mensajería segura y software de interfaz de dispositivo.

Los expertos en la materia tendrán en cuenta que la expresión "servidor de autenticación" se utiliza para describir genéricamente un servidor de autenticación que facilita información de autorización y autenticación a una red IEEE 802.x, a la cual trata de conectarse o acceder el usuario, en lugar de estar restringido a los servicios de comunicaciones conmutadas o serie. La disposición básica del servidor de autenticación 105 también es aplicable al servidor de administración de ciclo de vida representado en la figura 2G.

Con referencia a la figura 1A, se ilustra un diagrama de bloques de un controlador de seguridad 110. El controlador de seguridad 110 comprende un procesador 5n, un testigo de seguridad 75n acoplado al procesador 5n y una infraestructura de comunicaciones 100n. El testigo de seguridad 75n generalmente se denomina "módulo de acceso seguro" (SAM). El controlador de seguridad comprende además una pantalla 20n, tal como una pantalla LCD y/o de LED, que está acoplada eléctricamente a una interfaz de pantalla 15n, una memoria volátil 10a, una memoria permanente10b que comprende una RAM flashable, una memoria de solo lectura programable y eléctricamente borrable (EEPROM) 10c y un subsistema de interfaz de comunicaciones 55n.

El subsistema de interfaz de comunicaciones 55n está acoplado a la interfaz de testigo de seguridad 70n y comprende conectabilidad con contacto y sin contacto 70I con un testigo de seguridad extraíble 75r. El subsistema de interfaz de comunicaciones 55n está acoplado además con un transceptor de red 60n, una interfaz de entrada de usuario 80n que comprende un teclado opcional 85n opcional, un escáner biométrico opcional 95n acoplado eléctricamente a una interfaz de escáner biométrico opcional 90n y un circuito de control electromecánico 130. Al

activarse, el circuito de control electromecánico 130 permite el acceso físico a un lugar protegido. Los ejemplos comprenden cerraduras para puertas controladas electromagnéticamente, cerraduras eléctricas para puertas, portones y torniquetes. El circuito electromagnético es operativo generalmente para activar de forma momentánea un solenoide eléctrico y permitir el acceso de una persona a un área controlada.

El procesador 5n, el testigo de seguridad 75n, la interfaz de pantalla 15n, la memoria volátil 10a, la memoria permanente 10b, la EEPROM 10c y el subsistema de interfaz de comunicaciones 55n están acoplados eléctricamente a una infraestructura de comunicaciones 100n. El controlador de seguridad comprende un entorno operativo integrado, aplicaciones de seguridad compatibles con las controladas por el servidor de autenticación 105, aplicaciones de comunicaciones seguras, software para otras aplicaciones, software de criptografía capaz de realizar funciones de criptografía simétricas y asimétricas, software de mensajería segura y software de interfaz de dispositivo. El módulo de acceso seguro 75n comprende además por lo menos un par de claves asimétricas y software de aplicaciones relacionadas para permitir intercambios de clave seguros con el servidor de autenticación. Las aplicaciones, las claves criptográficas y los datos de usuario almacenados dentro del testigo de seguridad 75r se pueden intercambiar, modificar, añadir o eliminar en una transacción de administración de ciclo de vida con el servidor de autenticación 105 o el servidor de administración de ciclo de vida 105L representado en la figura 2G.

Con referencia a la figura 1B, se ilustra un diagrama de bloques de un testigo de seguridad extraíble 75r. El testigo de seguridad 75r comprende una interfaz inalámbrica, óptica y/o eléctrica 60t, 60w compatible con la interfaz de testigo de seguridad 70n, un procesador 5t, un coprocesador criptográfico opcional 5tc acoplado al procesador 5t y una infraestructura de comunicaciones 100t, una memoria volátil 10vm, una memoria permanente 10nvm, una memoria de solo lectura programable y eléctricamente borrable (EEPROM) 10eeprom y una interfaz de comunicaciones 55t acoplada a la interfaz 60t, 60w.

El procesador 5t, el coprocesador criptográfico opcional 5tc, la memoria volátil 10vm, la memoria permanente 10nvm, la memoria de solo lectura programable y eléctricamente borrable (EEPROM) 10eeprom y la interfaz de comunicaciones 55t están acoplados eléctricamente a la infraestructura de comunicaciones 100t. La EEPROM 10eeprom comprende además un entorno operativo de tiempo de ejecución, extensiones criptográficas integradas en el sistema operativo capaces de realizar funciones criptográficas simétricas y asimétricas compatibles con el controlador de la seguridad y el software criptográfico activado por testigo de seguridad, por lo menos un recurso seguro protegido por un parámetro crítico de seguridad acoplado por lo menos a una aplicación de autenticación remota de testigo y un par de claves de infraestructura de clave pública asimétrica (PKI) acoplado funcionalmente a la por lo menos una aplicación de autenticación remota de testigo.

En la memoria no volátil 10nv, se almacenan funcionalmente uno o más parámetros críticos de seguridad de referencia que se cotejan con un parámetro crítico de seguridad facilitado por la por lo menos una aplicación de autenticación remota para permitir el acceso al único o a los diversos recursos seguros protegidos por parámetro crítico de seguridad.

Con referencia a la figura 2, se ilustra una disposición general de la presente invención. La presente invención comprende un controlador de seguridad SC 110 que establece comunicaciones de procesamiento a través de una red 65 con un servidor de autenticación AS 105. El testigo de seguridad extraíble ST 75r está acoplado funcionalmente al controlador de seguridad SC 110.

El controlador de seguridad SC 110 comprende un procesador 5n acoplado funcionalmente a un transceptor de red T/R2 60n, una memoria que comprende por lo menos una aplicación de transacción de autenticación NA 210, un circuito electromecánico que al activarse permite el acceso físico a un área protegida, un módulo de acceso seguro (SAM) 75n por lo menos para almacenar un secreto compartido necesario para un protocolo de comunicaciones seguras, una interfaz de usuario opcional UI 85n y una pantalla DI 20n. La interfaz de usuario U1 85n y la pantalla DI 20n se facilitan en situaciones de áreas que requieren altos requisitos de seguridad. Por ejemplo, dependiendo de los requisitos de seguridad para acceder físicamente a un área protegida, puede ser que se exija a la entidad autenticarse localmente ante el testigo de seguridad 75r aportando una muestra biométrica y/o un número de identificación personal (PIN) para poder realizar transacciones con el servidor de autenticación AS 105.

El testigo de seguridad extraíble ST 75r, tal como una tarjeta inteligente, está asociado con la entidad y acoplado funcionalmente al controlador de seguridad 110 a través de la interfaz 70n de contacto o no contacto representada en la figura 1A. El testigo de seguridad extraíble ST 75r comprende por lo menos un parámetro crítico de seguridad CSPr 235r que se almacena dentro del testigo de seguridad ST 75r y es recuperable.

El testigo de seguridad extraíble ST 75r comprende por lo menos una aplicación de acceso remoto por testigo instalada funcionalmente en la memoria del testigo (no representada). La por lo menos una aplicación de acceso remoto por testigo TRA 215 permite al testigo de seguridad ST 75r enviar el parámetro crítico de seguridad CSPr 235r al controlador de seguridad SC 110 para su autenticación por el servidor de autenticación AS 105.

El servidor de autenticación AS 105 comprende un procesador de servidor 5 acoplado a un transceptor de red T/R1 60c que es compatible con el transceptor de red T/R2 60n instalado en el controlador de seguridad SC 110, y a una

base de datos 30 que comprende una pluralidad de parámetros críticos de seguridad de referencia CSPs 235s necesarios para autenticar el parámetro crítico de seguridad recibido desde el controlador de seguridad SC 110. Por otra parte, los parámetros críticos de seguridad de referencia CSPs 235s pueden almacenarse funcionalmente dentro de un módulo de seguridad de hardware HSM 75s. El procesador de servidor 5 está acoplado a una memoria que comprende por lo menos una aplicación de transacción de autenticación SA 205. La por lo menos una aplicación de transacción de autenticación SA 205 permite al servidor de autenticación AS 105 autenticar el parámetro crítico de seguridad CSPr 235 facilitado por el testigo de seguridad ST 75r.

El protocolo de mensajería utilizado para comunicarse con el testigo de seguridad ST 75r y el módulo de acceso seguro 75n comprende un protocolo de comunicaciones que cumple la norma ISO 7816. La conversión de protocolos entre los protocolos de comunicaciones por paquete de alto nivel y el protocolo de comunicaciones ISO 7816 de nivel más bajo puede llevarse a cabo mediante la aplicación de acceso remoto SA 205 instalada en el servidor de autenticación AS 105 o mediante el software de aplicaciones NA 210 instalado en el controlador de seguridad SC 110.

Se describe una disposición segura para intercambiar mandatos y respuestas APDU entre el testigo de seguridad ST 75r, el módulo de aplicación de seguridad 75n y el servidor de autenticación AS 105 en la solicitud de patente US 2002-0162021 (de nº de serie 09/844.246) que puede consultarse.

Con referencia a la figura 2A, una entidad inicia el acceso físico acoplando funcionalmente su testigo de seguridad ST 75r con el controlador de seguridad SC 110. El controlador de seguridad SC 110 genera y envía una petición de acceso AR 265R al servidor de autenticación AS 105 conforme a un protocolo de autenticación establecido. Los atributos comprendidos en la petición de acceso AR 265R indican el testigo de seguridad de la entidad (habitualmente un número de serie) que puede cotejarse con las políticas de seguridad establecidas para la entidad incluso antes de que se inicie la autenticación (no representado). Por ejemplo, si la entidad no tiene permiso para entrar en el área protegida a la cual intenta acceder, la transacción termina sin más procesamiento.

Las políticas de seguridad se describen en la solicitud de patente US 2004-0123152 (de nº de serie 10/402.960) que puede consultarse y la solicitud de patente US 2004-0221174 (de nº de serie 10/425.028) que también puede consultarse.

Como parte del protocolo de autenticación establecido, si no está disponible ninguna de antemano, el servidor de autenticación AS 105 genera un secreto compartido KSr 240r, KSs 240s que se comparte de forma segura con el controlador de seguridad y es mantenida por el módulo de acceso seguro 75n. El intercambio seguro de clave secreta es posible gracias al protocolo de comunicaciones seguro implementado a través de la red 65. No obstante, en su lugar pueden utilizarse intercambios seguros de clave secreta más resistentes si es necesario para satisfacer un requisito particular de seguridad.

Con referencia a la figura 2B, una vez que se han establecido los secretos compartidos KSr 240r, KSs 240s para la conexión de comunicaciones segura entre el servidor de autenticación AS 105 y el controlador de seguridad SC 110, se recupera un parámetro crítico de seguridad CSPr 235r del testigo de seguridad de la entidad ST 75r y se envía de forma segura 65 al servidor de autenticación AS 105 para su autenticación.

Con referencia a la figura 2C, una vez que el servidor de autenticación AS 105 ha recibido el parámetro crítico de seguridad de la entidad CSPr 235r', este se compara con un parámetro crítico de seguridad de referencia CSPs 235s' recuperado de la base de datos 30 o el HSM 75s. Si el parámetro crítico de seguridad de la entidad CSPr 235r' no se autentica, se envía un mensaje de rechazo de autenticación al controlador de seguridad y no se permite el acceso de la entidad al área protegida. Si la autenticación del parámetro crítico de seguridad de la entidad CSPr 235r' se realiza con éxito, la aplicación del servidor de autenticación SA 205 genera un resultado de autenticación afirmativa 265, representado por una marca de verificación.

Con referencia a la figura 2D, el resultado de autenticación afirmativa 265 se envía entonces de forma segura al controlador de seguridad SC 110. La aplicación del controlador de seguridad NA 210 procesa el resultado de autenticación afirmativa 265, lo cual lleva a la activación del circuito de control electromecánico EMC 130. El tiempo durante el cual el circuito de control electromecánico EMC 130 está activado se ajusta de manera específica para un testigo de seguridad de entidad particular. Esto permite controlar la apertura de un acceso, tal como una puerta para la entrada de suministros o para facilitar el paso a las personas con discapacidades físicas.

Con referencia a la figura 2E, se representa otra forma de realización de la presente invención, en la que se realiza una transacción de administración de parámetro crítico de seguridad entre el servidor de autenticación AS 105 y el módulo de acceso seguro 75n.

En esta forma de realización de la presente invención, se establece una conexión de comunicaciones segura 65 entre por lo menos el controlador de seguridad SC 110 y el servidor de autenticación AS 105 mediante, por ejemplo, las claves simétricas compartidas KSr, KSs 240r, 240s.

En una forma de realización de la presente invención, la conexión de comunicaciones segura permite comunicaciones seguras de extremo a extremo entre el módulo de acceso seguro 75n y el servidor de autenticación AS 105. Como deducirán los expertos en la materia, es posible utilizar también otras disposiciones de canal de comunicaciones seguras.

En este ejemplo, se envía de forma segura un parámetro crítico de seguridad CSPs 235s para su almacenamiento dentro del módulo de acceso seguro 75n seguro. La transacción de parámetro crítico de seguridad puede ser un intercambio de parámetro crítico de seguridad, una sustitución de parámetro crítico de seguridad, una generación de parámetro crítico de seguridad, una supresión de parámetro crítico de seguridad o un cambio de un atributo a un parámetro criptográfico de seguridad. El parámetro crítico de seguridad puede obtenerse en un almacén de datos 30 o en un módulo de seguridad de hardware HSM 75s acoplados funcionalmente al servidor de autenticación.

Con referencia a la figura 2F, se representa una forma de realización alternativa de la presente invención, en la que el módulo de acceso seguro 75n acoplado al controlador de seguridad SC 110 integra uno o más parámetros críticos de seguridad CSPn 235n para autenticar localmente al usuario. Esta disposición permite conceder acceso a una lista de acceso local 280 de usuarios autenticados al área protegida sin tener que depender de las autenticaciones del servidor de autenticación AS 105, hecho que resulta particularmente ventajoso durante períodos de elevado tráfico, tales como en cambios de turno o períodos en los que el servidor de autenticación AS 105 y/o la red de comunicaciones 65 están temporalmente fuera de servicio. La lista de acceso local 280 de usuarios autenticados o indicaciones de usuarios autorizados (por ejemplo, identificadores exclusivos de testigo) se envían al servidor de autenticación AS 105 al llenarse la lista de acceso local 280, cuando el servidor de autenticación AS 105 lo solicita y/o las comunicaciones con el servidor de autenticación AS 105 se restauran.

La lista de acceso local 280 se envía al servidor de autenticación AS 105 por medio de los mecanismos de comunicaciones seguros descritos anteriormente. Esta disposición permite una completa administración de los CSP, incluidas las funciones de administración de claves y la actualización de listas de acceso autorizado a través de disposiciones de red que cumplen la norma IEEE 802.x. El servidor de autenticación AS 105 utiliza entonces la lista de acceso local para actualizar una lista de acceso maestra 285.

Con referencia a la figura 2G, se representa otra forma de realización de la presente invención en la que un servidor de administración de ciclo de vida LCS 105L está funcionalmente acoplado a la red 65. En esta forma de realización de la presente invención, el servidor de administración de ciclo de vida LCS 105L mantiene las aplicaciones de seguridad y la información criptográfica empleadas por el servidor de autenticación AS 105A, el controlador de seguridad SC 110, el módulo de acceso seguro 75n y, opcionalmente, el testigo de seguridad ST 75r. Esta disposición permite al servidor de administración de ciclo de vida LCS 105L distribuir, intercambiar, suprimir, añadir o modificar uno o más parámetros críticos de seguridad, aplicaciones o datos de usuario instalados en dichos dispositivos.

Con referencia a la figura 3, se ilustran las principales etapas de implementación de la presente invención. El proceso se inicia 300 estableciendo una conexión de comunicaciones segura que integra una clave simétrica compartida entre un controlador de seguridad y un servidor de autenticación 305. La clave simétrica se almacena y mantiene de forma segura en un módulo de acceso seguro asociado al controlador de seguridad 310. A continuación, se envía un parámetro crítico de seguridad desde un testigo de seguridad de la entidad hasta el controlador de seguridad 310. El controlador de seguridad envía el parámetro crítico de seguridad al servidor de autenticación por medio de la conexión de comunicaciones segura 320 para su autenticación.

El servidor de autenticación realiza una transacción de autenticación mediante el parámetro crítico de seguridad de la entidad 325 y genera un resultado de transacción de autenticación 330. El resultado de la transacción de autenticación se envía entonces al controlador de seguridad, por medio de la conexión de comunicaciones segura, para su evaluación 335. Si el parámetro crítico de seguridad de la entidad no se autentica con éxito 340, el procesamiento termina 350 y no se permite a la entidad el acceso al área protegida. Si el parámetro crítico de seguridad de la entidad se autentica con éxito 340, entonces se activa un circuito electromecánico 345, hecho que permite el acceso físico de la entidad al área protegida durante un tiempo preestablecido, tras el cual concluye el acceso y el procesamiento 350.

Con referencia a la figura 3A, se ilustran las etapas principales de la implementación de una forma de realización alternativa de la presente invención. El proceso se inicia 301 estableciendo un canal de comunicaciones seguro entre por lo menos un controlador seguro, pero preferentemente entre un módulo de acceso seguro acoplado al controlador de seguridad, y el servidor de autenticación 303.

A continuación, el servidor de autenticación realiza por lo menos una transacción de administración de ciclo de vida en conjunción con el módulo de acceso seguro 307. Una vez efectuada la transacción de administración de ciclo de vida, el procesamiento termina 309. Los expertos en la materia tendrán en cuenta que es posible realizar transacciones de administración de ciclo de vida adicionales con un testigo de seguridad acoplado funcionalmente también.

Por último, con referencia a la figura 3B, se ilustran las etapas principales de la implementación de otra forma de realización de la presente invención. En esta forma de realización de la presente invención, el proceso se inicia 302 enviando un parámetro crítico de seguridad (CSP) desde un testigo de seguridad asociado a una entidad hasta un controlador de seguridad provisto de un módulo de acceso seguro 304. El módulo de acceso seguro trata de autenticar localmente el CSP 306, y el resultado de la autenticación se registra en una lista de acceso local 308. A continuación, la lista de acceso local se envía, por medio de una conexión de comunicaciones segura 312, a un servidor de autenticación, donde la lista de acceso maestra se actualiza con la información contenida en la lista de acceso local 314. El proceso termina una vez que la lista de acceso maestro se ha actualizado 322.

Las formas de realización de la presente invención descritas anteriormente se proveen 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. No se pretende limitar el alcance a ningún entorno operativo de testigo de seguridad particular. Tomando en consideración la información facilitada en la presente memoria, se observará que es posible realizar otras variantes y formas de realización, no siendo el propósito de la descripción detallada anterior el de limitar el alcance de la presente invención, que está limitado por las reivindicaciones adjuntas.

REIVINDICACIONES

1. Procedimiento para controlar físicamente el acceso a un lugar protegido, que comprende las etapas siguientes:

- establecer una conexión de comunicaciones segura a través de una red entre un controlador de seguridad (110) y por lo menos un servidor de autenticación (105),

- acoplar funcionalmente un testigo de seguridad (75) a dicho controlador de seguridad,

- enviar un parámetro crítico de seguridad desde dicho testigo de seguridad hasta dicho controlador de seguridad para su autenticación,

- enviar dicho parámetro crítico de seguridad por lo menos a dicho servidor de autenticación por medio de dicha conexión de comunicaciones segura,

- realizar, mediante dicho servidor de autenticación, una transacción de autenticación para dicho parámetro crítico de seguridad,

- enviar un resultado de dicha transacción de autenticación desde dicho servidor de autenticación hasta dicho controlador de seguridad por medio de dicha conexión de comunicaciones segura, y

- activar un circuito electromecánico (130) controlado por dicho controlador de seguridad si dicho resultado confirma que dicha transacción de autenticación se ha realizado con éxito,

caracterizado porque dicha activación de dicho circuito electromecánico está limitada a una duración preestablecida específica para dicho testigo de seguridad.

2. Procedimiento según la reivindicación 1, en el que dicha conexión de comunicaciones segura incluye un secreto compartido establecido entre dicho servidor de autenticación y dicho controlador de seguridad, y que es mantenido de forma segura por un módulo de acceso seguro acoplado funcionalmente a dicho controlador de seguridad.

3. Procedimiento según la reivindicación 1 o 2, en el que dicho controlador de seguridad es uno de entre una pluralidad de controladores de seguridad, en el que dicha pluralidad de controladores de seguridad está constituida por clientes conectados en red de por lo menos dicho servidor de autenticación.

4. Procedimiento según cualquiera de las reivindicaciones 1 a 3, en el que dicho circuito electromecánico está asociado a una puerta de acceso físico y en el que la activación de dicho circuito electromecánico abre dicha puerta de acceso físico.

5. Procedimiento según cualquiera de las reivindicaciones 1 a 4, en el que por lo menos una parte de dicha conexión de comunicaciones segura se establece a través de un enlace de telecomunicaciones inalámbricas.

6. Procedimiento según cualquiera de las reivindicaciones 1 a 5, en el que dicha conexión de comunicaciones segura incorpora un protocolo de seguridad que incluye SSL, IPsec, PCT, TLS o RADIUS.

7. Procedimiento según la reivindicación 2, que comprende las etapas siguientes:

- establecer dicha conexión de comunicaciones segura, a través de dicha red, entre dicho servidor de autenticación y dicho módulo de acceso seguro que está acoplado funcionalmente a dicho controlador de seguridad,

- acoplar funcionalmente dicho testigo de seguridad con dicho módulo de acceso seguro por medio de una interfaz acoplada a dicho controlador de seguridad,

- enviar dicho parámetro crítico de seguridad desde dicho testigo de seguridad hasta dicho módulo de acceso seguro,

- enviar dicho parámetro crítico de seguridad a dicho servidor de autenticación por medio de dicha conexión de comunicaciones segura,

- realizar la transacción de autenticación mediante dicho servidor de autenticación por medio de un proceso que incorpora dicho parámetro crítico de seguridad,

- enviar dicho resultado de dicha transacción de autenticación desde dicho servidor de autenticación hasta dicho controlador de seguridad por medio de dicha conexión de comunicaciones segura, y

- activar dicho circuito electromecánico controlado por dicho controlador de seguridad si dicho resultado confirma que dicha transacción de autenticación se ha realizado con éxito.

8. Procedimiento según cualquiera de las reivindicaciones 1 a 7, en el que dicho controlador de seguridad establece además comunicaciones seguras a través de dicha red con un servidor de administración de ciclo de vida adaptado para realizar funciones de administración de ciclo de vida relacionadas con aplicaciones, parámetros críticos de seguridad o datos de usuario instalados en dicho testigo de seguridad o en dicho módulo de acceso seguro.

9. Procedimiento según las reivindicaciones 2 y 8, en el que dicha una o más transacciones de administración de ciclo de vida comprenden la distribución, el intercambio, la supresión, la adición o la modificación de uno o más parámetros críticos de seguridad, aplicaciones o datos de usuario instalados en dicho módulo de acceso seguro.

10. Sistema para controlar físicamente el acceso a un lugar protegido que comprende:

- un testigo de seguridad (110) acoplado funcionalmente a un controlador de seguridad (75) y que incluye unos medios para enviar un parámetro crítico de seguridad a dicho controlador de seguridad para su autenticación,

- un módulo de acceso seguro acoplado funcionalmente a dicho controlador de seguridad y que incluye unos medios para mantener de forma segura un secreto compartido establecido por un servidor de autenticación (105) e incorpora dicho secreto compartido en una conexión de comunicaciones segura establecida con por lo menos un servidor de autenticación;

- unos medios de control electromecánico (130) acoplados funcionalmente a dicho controlador de seguridad que incluye unos medios para abrir una puerta de acceso física una vez activados,

comprendiendo dicho controlador de seguridad unos medios para:

- establecer dicha conexión de comunicaciones segura con por lo menos dicho servidor de autenticación, enviar dicho parámetro crítico de seguridad a dicho servidor de autenticación por medio de dicha conexión de comunicaciones segura y activar dichos medios de control electromecánico como respuesta a un resultado de autenticación afirmativo recibido desde dicho servidor de autenticación,

comprendiendo dicho servidor de autenticación unos medios para:

- establecer dichas comunicaciones seguras con dicho controlador de seguridad, realizar una transacción de autenticación como respuesta a la recepción de dicho parámetro crítico de seguridad desde dicho controlador de seguridad, y

- suministrar dicho resultado de autenticación afirmativa a dicho controlador de seguridad por medio de dicha conexión de comunicaciones segura tras una autentificación correcta de dicho parámetro crítico de seguridad,

caracterizado porque el sistema comprende además unos medios para limitar la activación de dicho circuito electromecánico a una duración preestablecida específica para dicho testigo de seguridad.

11. Sistema según la reivindicación 10, en el que dicha por lo menos una parte de dicha conexión de comunicaciones segura se establece a través de un enlace de telecomunicaciones inalámbricas.

12. Sistema según la reivindicación 10 u 11, en el que dicha conexión de comunicaciones segura incorpora un protocolo de seguridad que incluye SSL, IPsec, PCT, TLS o RADIUS.

13. Sistema según cualquiera de las reivindicaciones 10 a 12, en el que dicho módulo de acceso seguro incluye además unos medios para realizar localmente dicha transacción de autenticación.

14. Sistema según la reivindicación 13, en el que dicho controlador de seguridad o dicho módulo de acceso seguro incluyen además unos medios para mantener por lo menos una lista de acceso de parámetros críticos de seguridad autenticados localmente.

15. Sistema según la reivindicación 15, en el que dicho servidor de autenticación incluye además unos medios para recibir dicha por lo menos una lista de acceso de parámetros críticos de seguridad autenticados localmente y actualizar un acceso maestro asociado a dicho servidor de autenticación.

16. Sistema según cualquiera de las reivindicaciones 10 a 15, que comprende además un servidor de administración de ciclo de vida que comprende unos medios para:

- establecer una conexión de comunicaciones segura con dicho módulo de acceso seguro o dicho controlador de

seguridad, y

- realizar una o más transacciones de administración de ciclo de vida con dicho módulo de acceso seguro.

17. Sistema según la reivindicación 16, en el que dicha una o más transacciones de administración de ciclo de vida comprenden la distribución, el intercambio, la supresión, la adición o la modificación de uno o más parámetros críticos de seguridad, aplicaciones o datos de usuario instalados en dicho módulo de acceso seguro.

18. Controlador de seguridad (110) para controlar físicamente el acceso a un lugar protegido (110) que comprende:

- un procesador,
- una memoria acoplada a dicho procesador,
- una interfaz de testigo de seguridad acoplada a dicho procesador,
- un transceptor de red acoplado a dicho procesador,
- un módulo de acceso seguro acoplado a dicho procesador,
- un circuito de control electromagnético acoplado a dicho procesador, y
- por lo menos una aplicación instalada por lo menos en una parte de dicha memoria que contiene instrucciones lógicas ejecutables por dicho procesador para:
- establecer una conexión de comunicaciones segura a través de una red con por lo menos un servidor de autenticación (105) por medio de dicho transceptor de red,
- realizar una transacción de autenticación en conjunción con dicho servidor de autenticación para un parámetro crítico de seguridad recibido por medio de dicha interfaz de testigo de seguridad,
- recibir y mantener un secreto compartido en dicho módulo de acceso seguro,
- incorporar dicho secreto compartido en dicha conexión de comunicaciones segura, y
- activar dicho circuito de control electromecánico tras la recepción de un resultado de autenticación afirmativo asociado a dicha transacción de autenticación,

caracterizado porque comprende además unos medios para limitar la activación de dicho circuito electromecánico a una duración preestablecida específica para dicho testigo de seguridad.

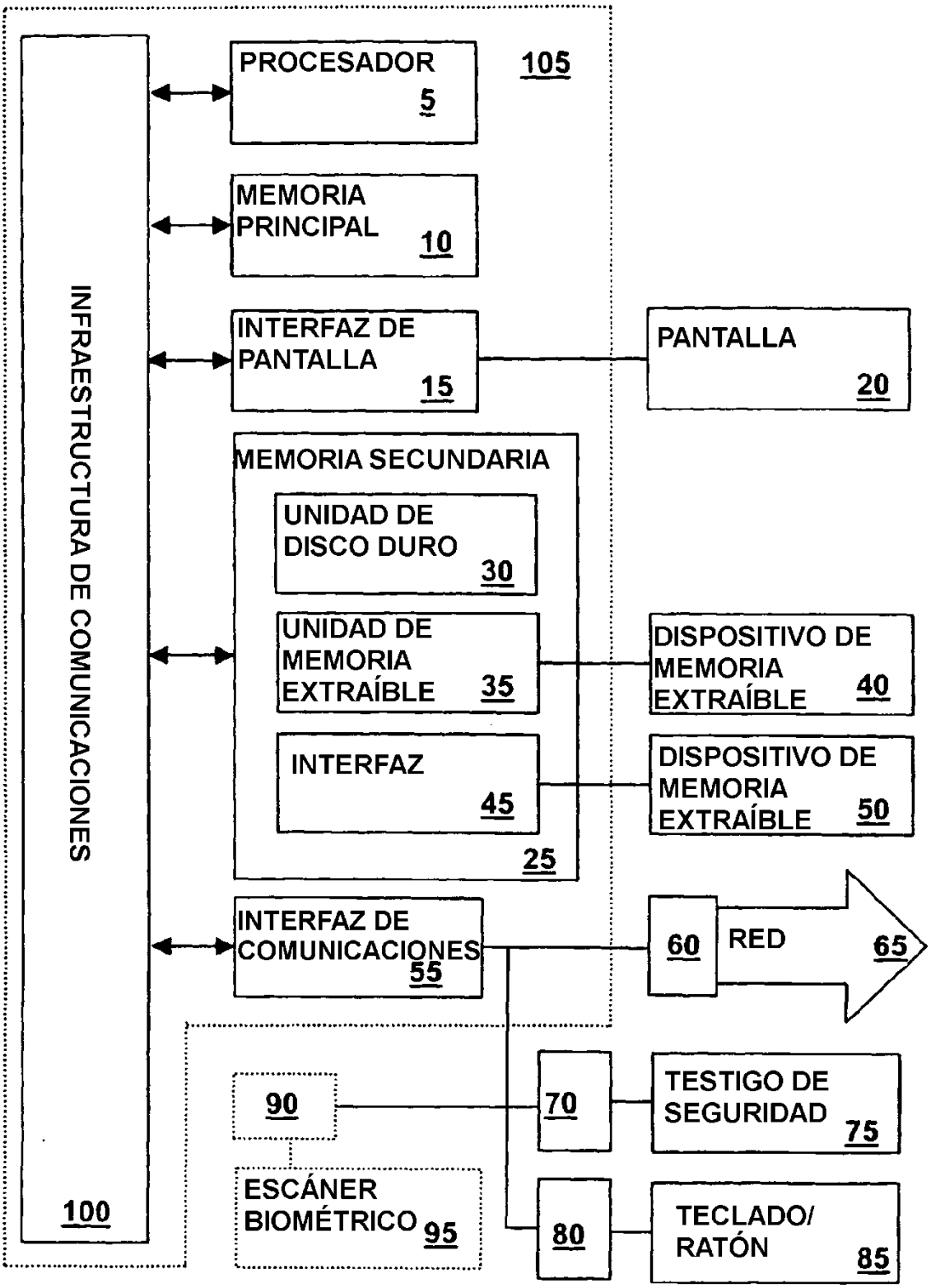
INFRAESTRUCTURA DE COMUNICACIONES
100
PROCESADOR
5
105
MEMORIA PRINCIPAL
10
INTERFAZ DE PANTALLA
15
PANTALLA
20
MEMORIA SECUNDARIA
UNIDAD DE DISCO DURO
30
UNIDAD DE MEMORIA EXTRAÍBLE
35
DISPOSITIVO DE MEMORIA EXTRAÍBLE
40
INTERFAZ
45
DISPOSITIVO DE MEMORIA EXTRAÍBLE
50
25
INTERFAZ DE COMUNICACIONES
55
60
RED
65
90
70
TESTIGO DE SEGURIDAD
75
ESCÁNER BIOMÉTRICO
95
80
TECLADO/ RATÓN
85

FIG. 1

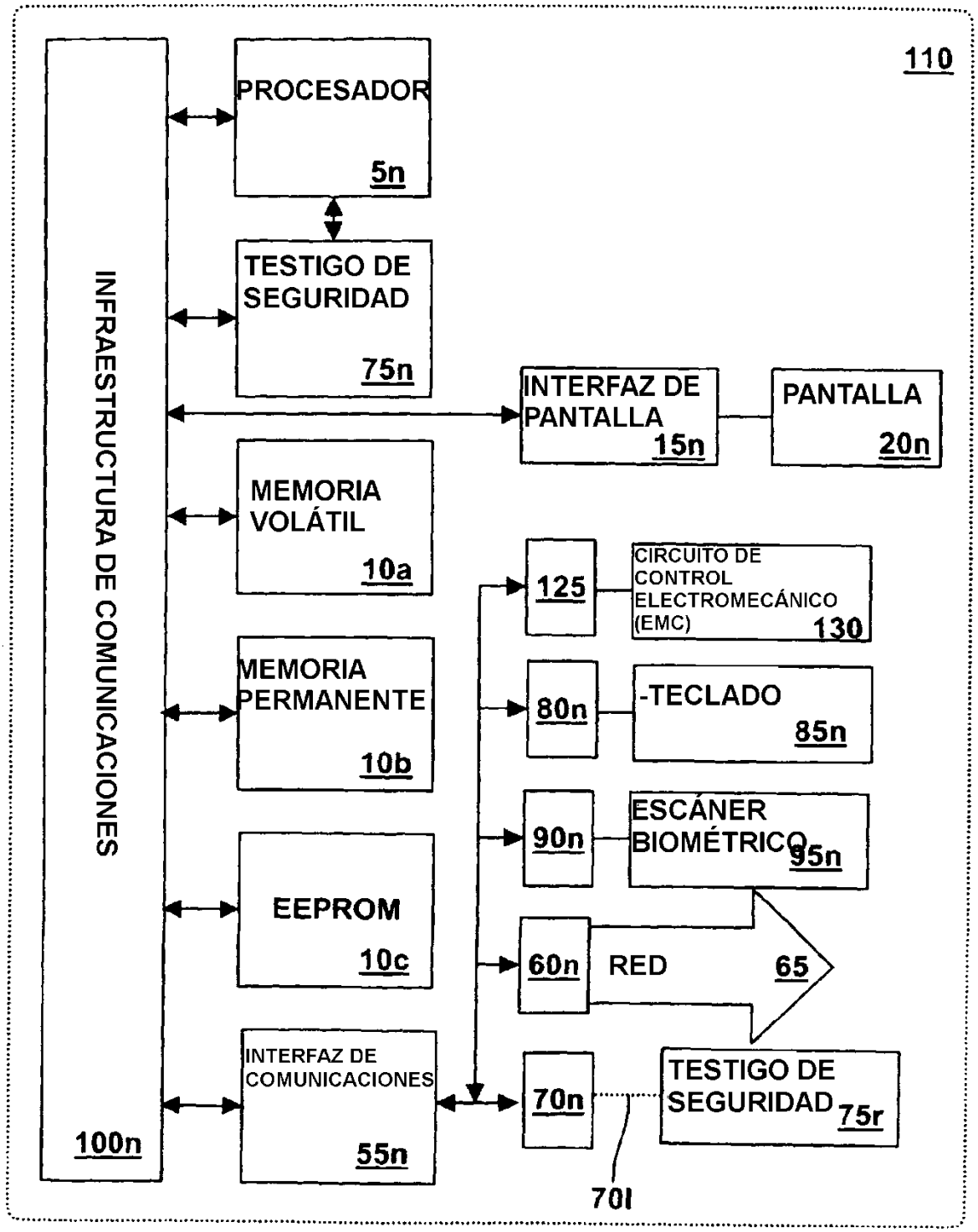
110
PROCESADOR
5n
TESTIGO DE SEGURIDAD
75n
INTERFAZ DE PANTALLA
15n
PANTALLA
20n
MEMORIA VOLÁTIL
10a
MEMORIA PERMANENTE
10b
EEPROM
10c
INTERFAZ DE COMUNICACIONES
55n
INFRAESTRUCTURA DE COMUNICACIONES
100n
125
CIRCUITO DE CONTROL ELECTROMECÁNICO (EMC)
130
80n
-TECLADO
85n
90n
ESCÁNER BIOMÉTRICO
95n
60n
RED
65
70n
TESTIGO DE SEGURIDAD
75r
70l

FIG. 1A

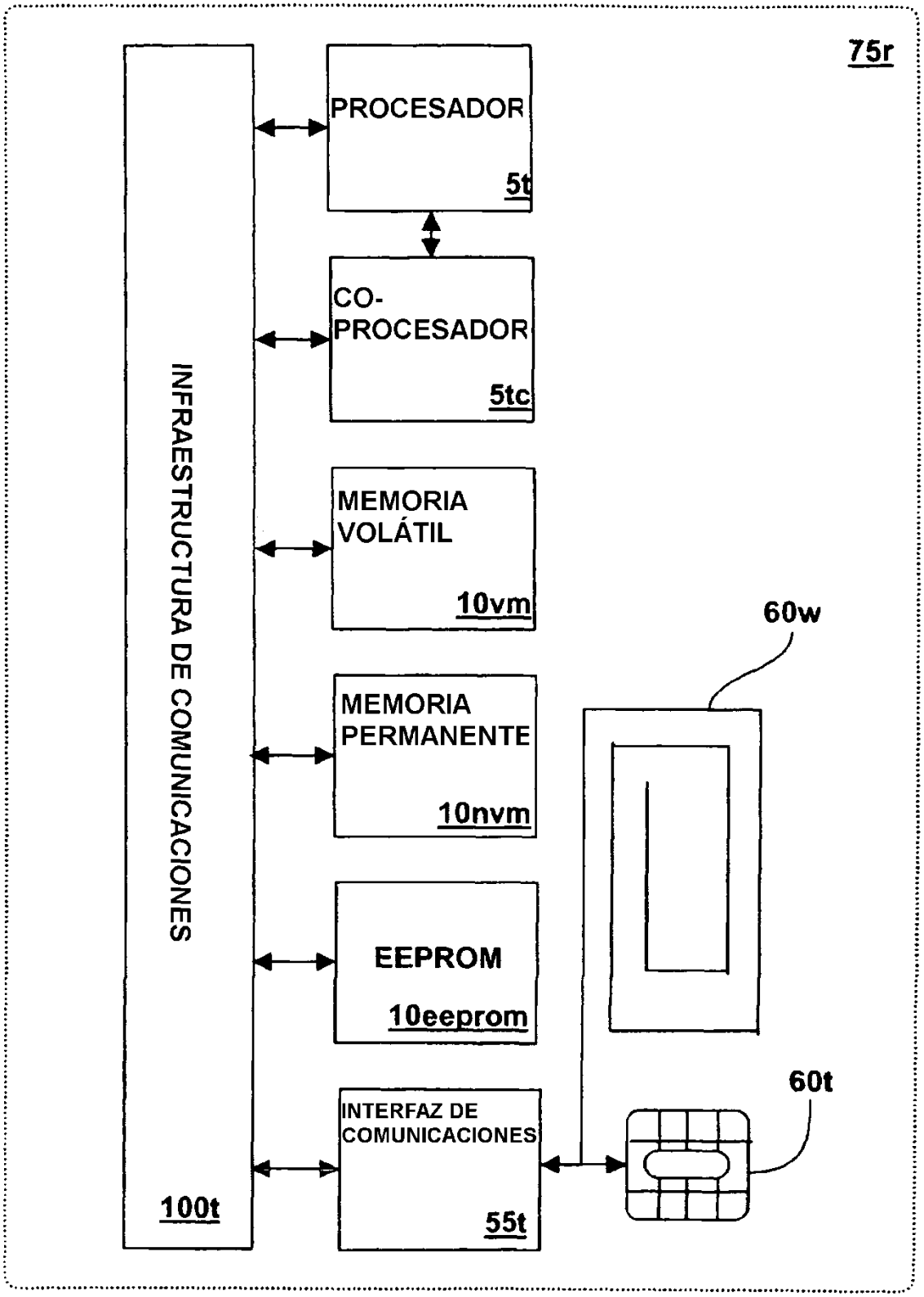
75r
PROCESADOR
5t
CO-
PROCESADOR
5tc
MEMORIA
VOLÁTIL
10vm
MEMORIA
PERMANENTE
10nvm
EEPROM
10eeprom
INTERFAZ DE
COMUNICACIONES
55t
INFRAESTRUCTURA DE COMUNICACIONES
100t
60w
60t

FIG. 1B

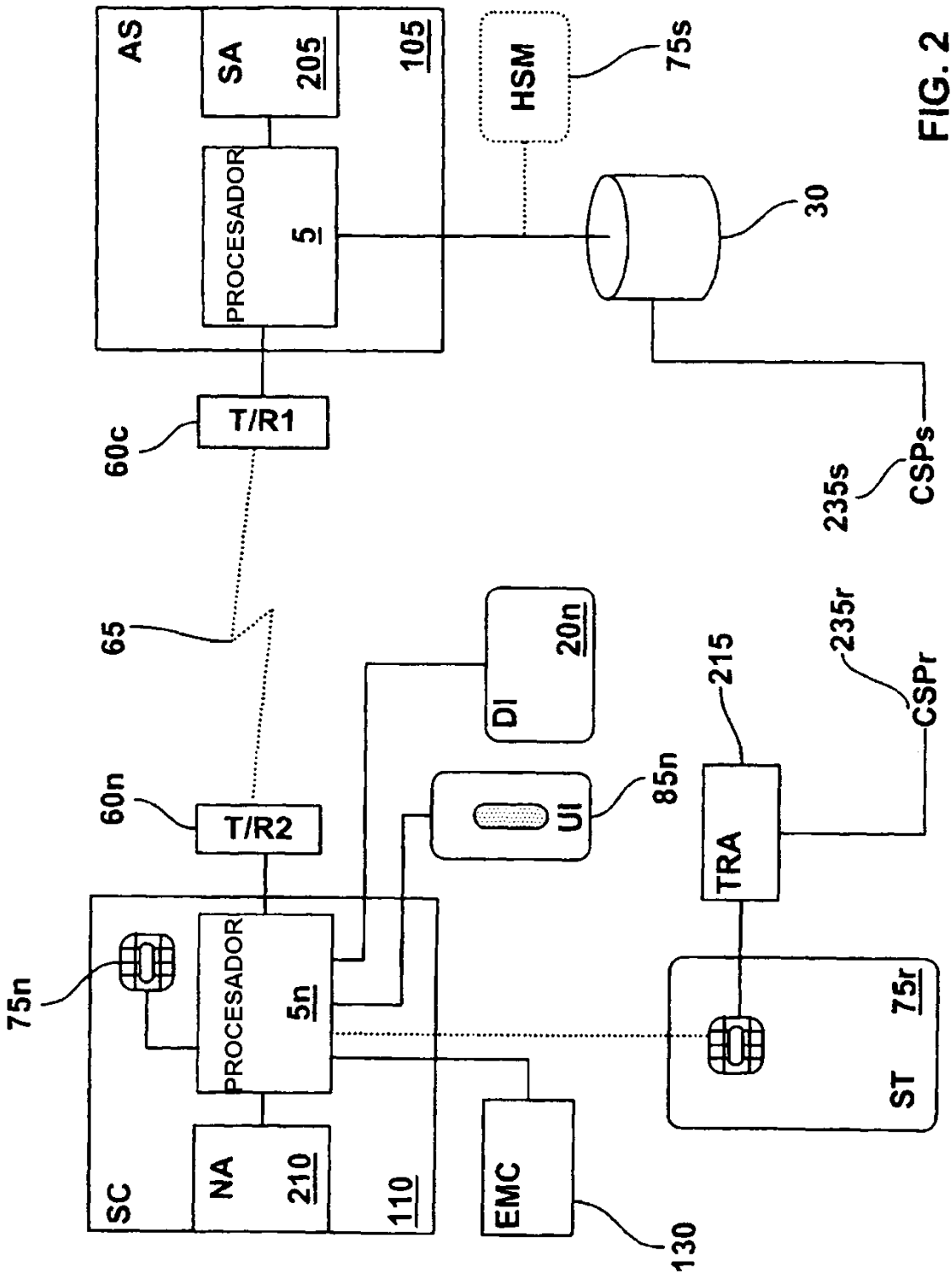
AS
SA
205
105
PROCESADOR
5
HSM
75s
30
T/R1
60c
235s
CSPs
65
DI
20n
215
235r
CSPr
60n
T/R2
UI
85n
TRA
75n
PROCESADOR
5n
ST
75r
SC
NA
210
110
EMC
130

FIG. 2

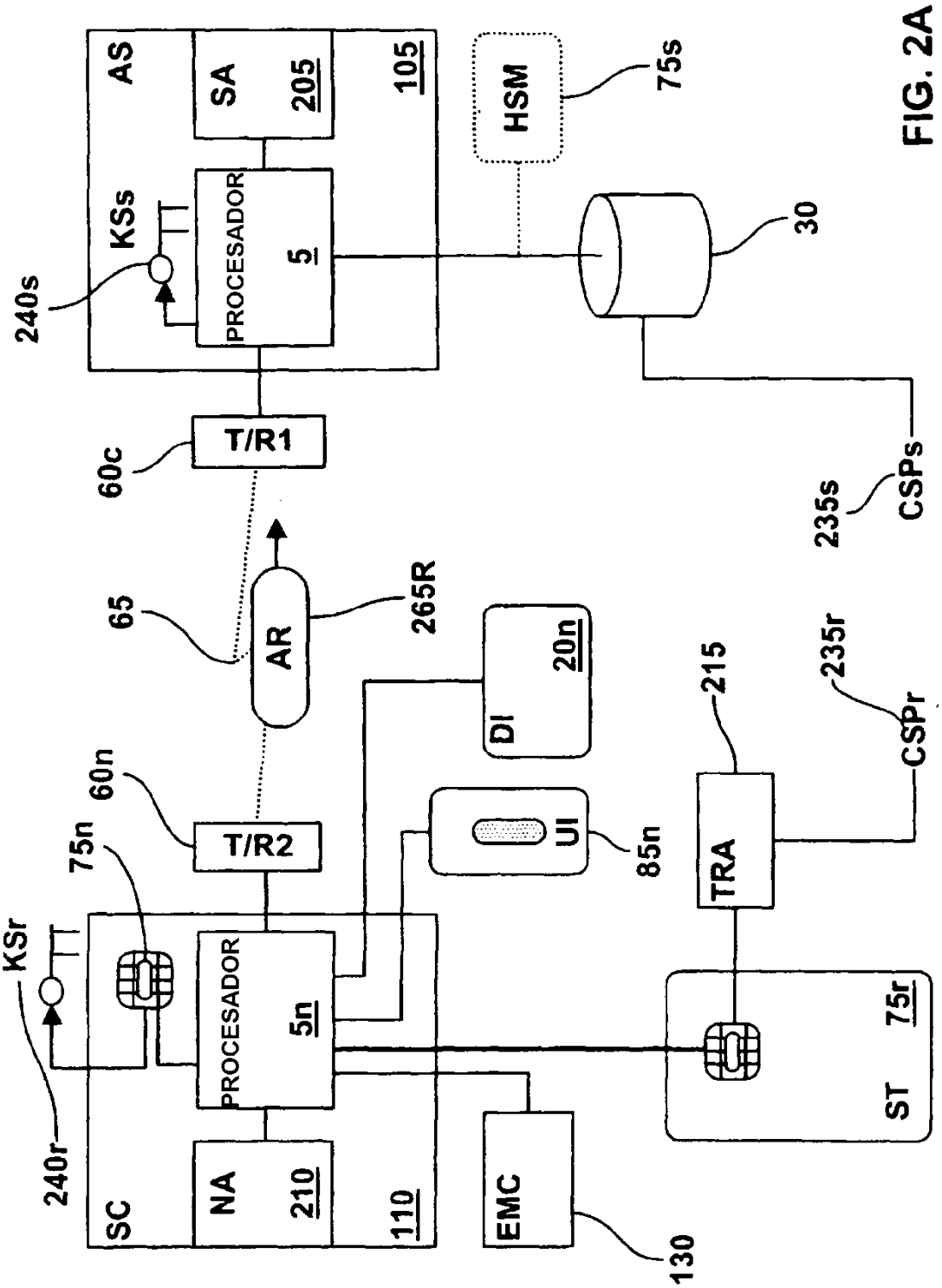
AS
SA
205
105
HSM
75s
KSs
PROCESADOR
5
30
240s
T/R1
60c
235s
CSPs
65
AR
265R
DI
20n
215
235r
CSPr
60n
T/R2
UI
85n
TRA
75n
KSr
PROCESADOR
5n
ST
75r
240r
SC
NA
210
110
EMC
130

FIG. 2A

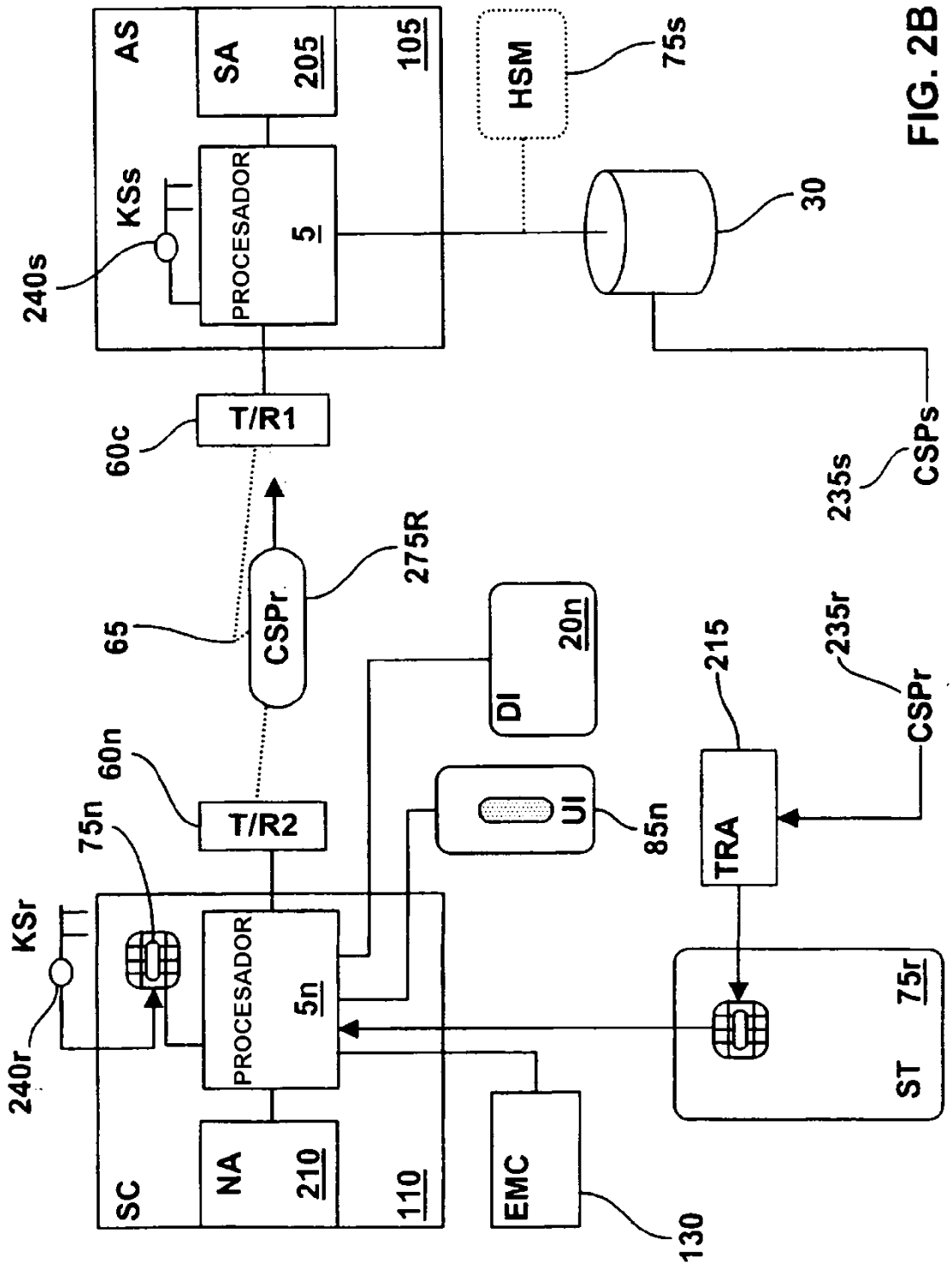
AS
SA
205
105
HSM
75s
KSs
PROCESADOR
5
30
240s
T/R1
60c
235s
CSPs
275R
CSPr
65
DI
20n
215
235r
CSPr
60n
T/R2
UI
85n
TRA
75n
KSr
PROCESADOR
5n
ST
75r
240r
SC
NA
210
110
EMC
130

FIG. 2B

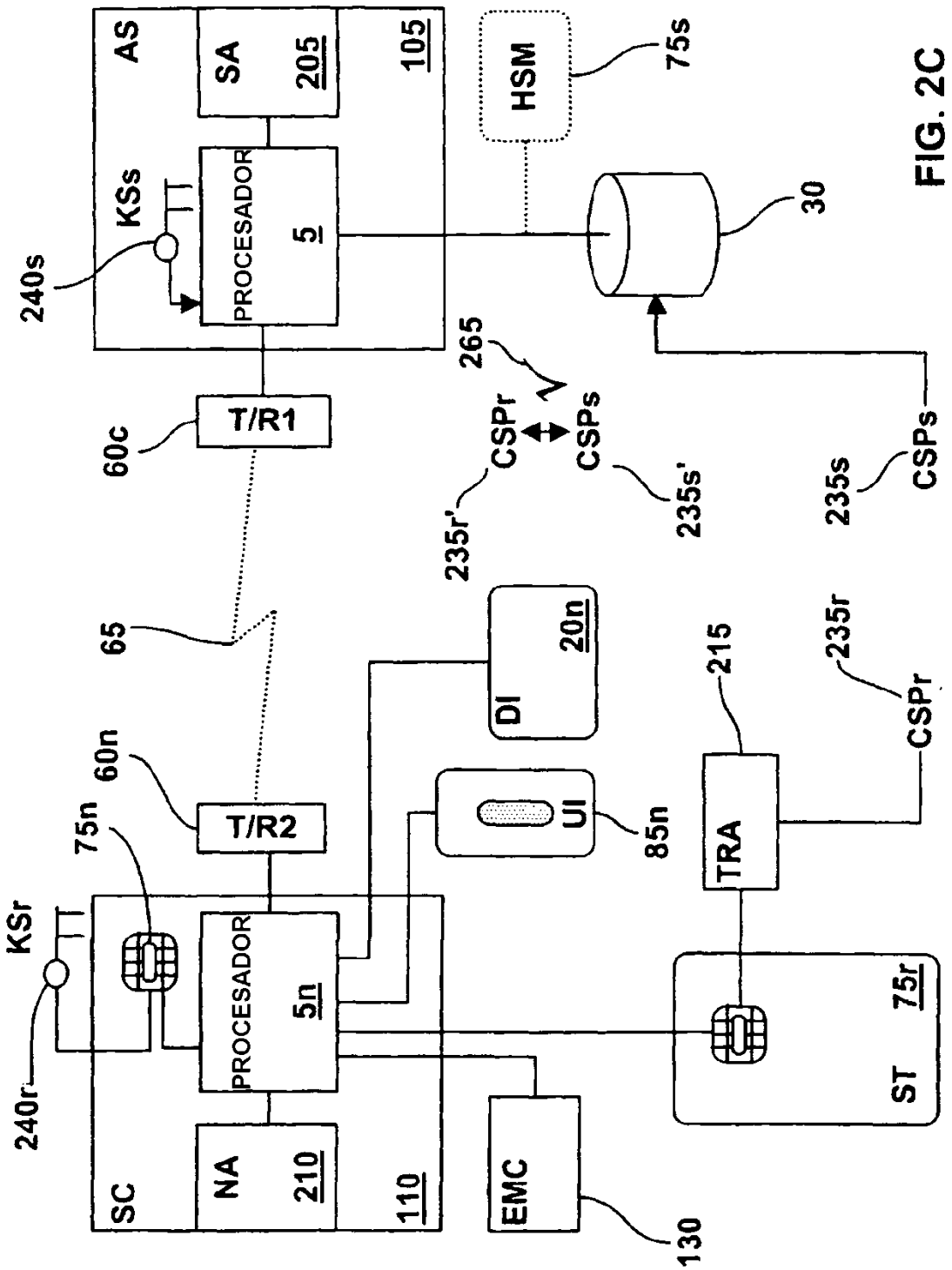
AS
SA
205
105
HSM
75s
KSs
PROCESADOR
5
30
240s
265
T/R1
60c
CSPr
CSPs
235r'
235s'
235s
CSPs
65
DI
20n
60n
T/R2
UI
85n
215
235r
CSPr
75n
TRA
KSr
PROCESADOR
5n
ST
75r
240r
SC
NA
210
110
EMC
130

FIG. 2C

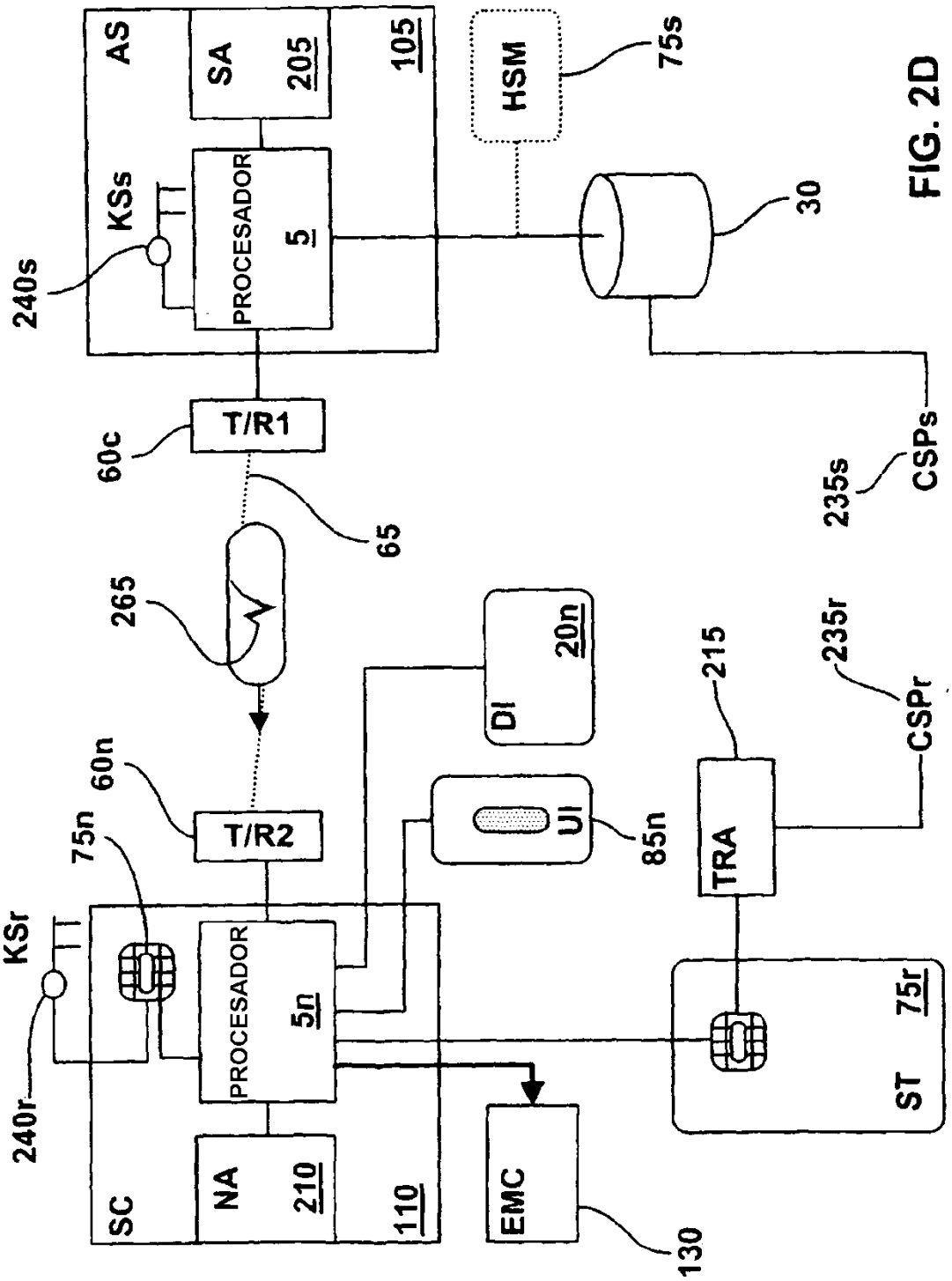
AS
SA
205
105
HSM
75s
KSs
PROCESADOR
5
30
240s
T/R1
60c
65
CSPs
235s
265
DI
20n
215
235r
CSPr
60n
T/R2
UI
85n
TRA
75n
KSr
PROCESADOR
5n
ST
75r
240r
SC
NA
210
110
EMC
130

FIG. 2D

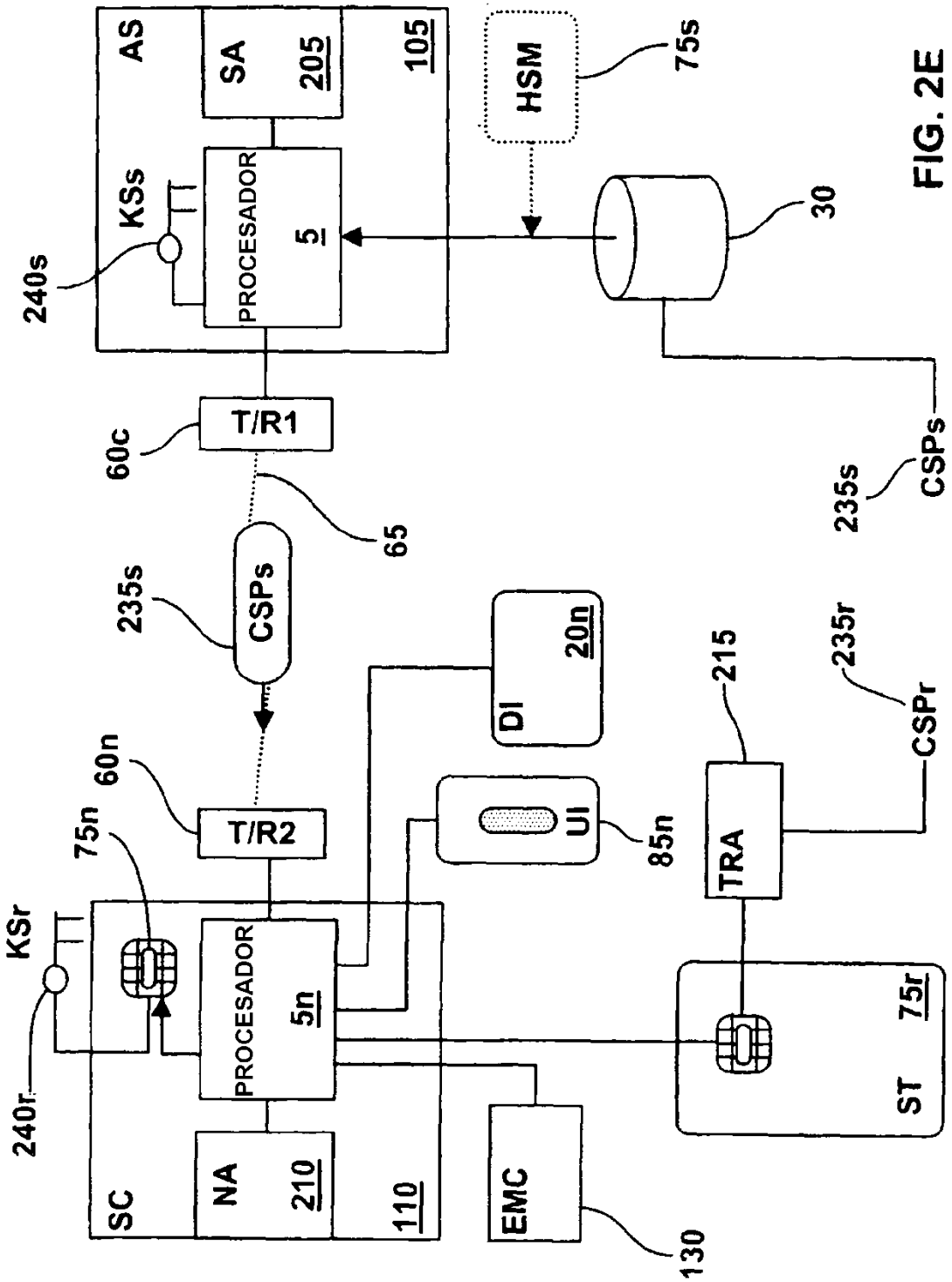
AS
SA
205
105
HSM
75s
KSs
PROCESADOR
5
240s
30
T/R1
60c
65
235s
CSPs
CSPs
235s
DI
20n
215
235r
CSPr
60n
T/R2
75n
UI
85n
TRA
KSr
PROCESADOR
5n
ST
75r
240r
SC
NA
210
110
EMC
130

FIG. 2E

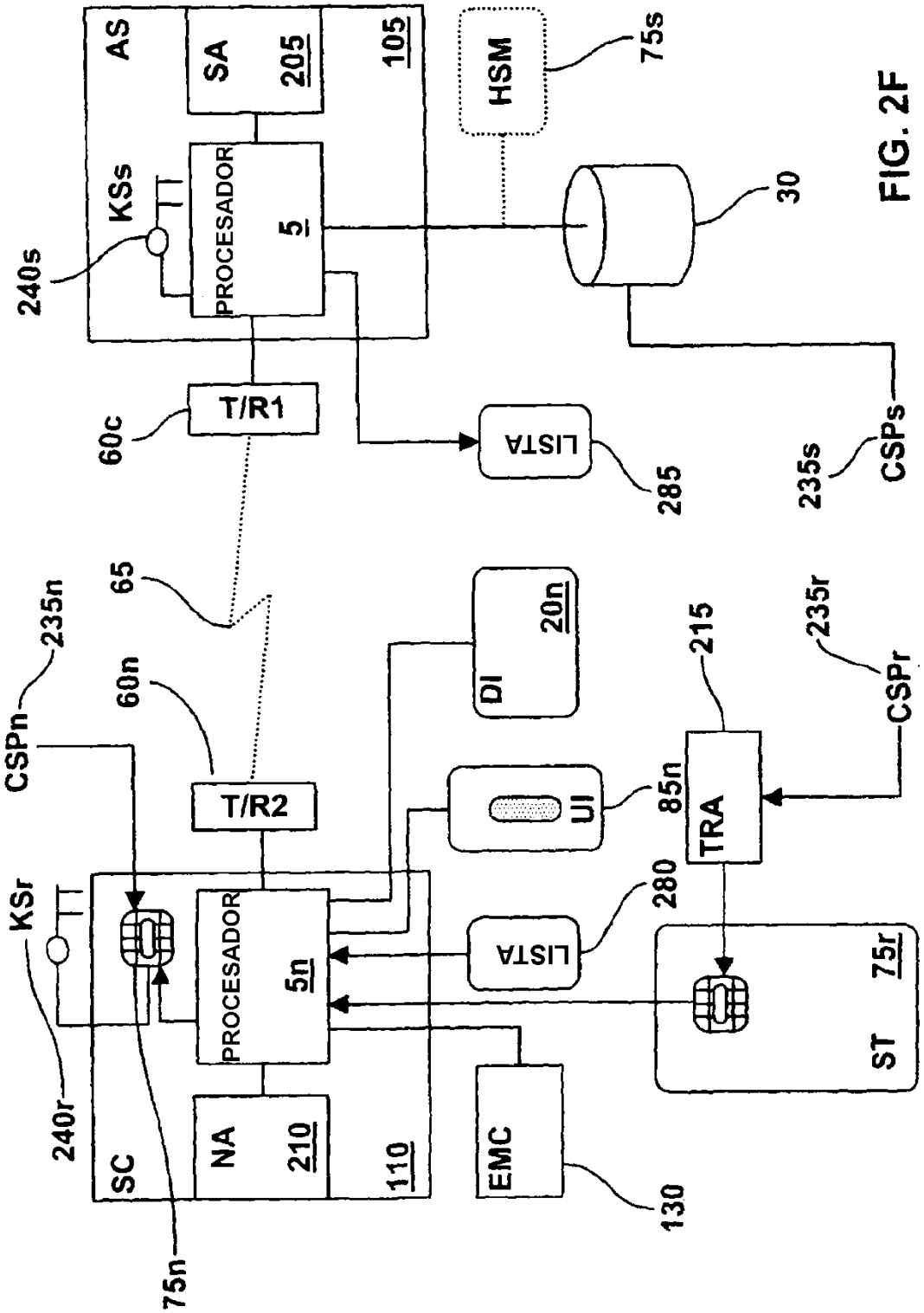
AS
SA
205
105
HSM
75s
KSs
PROCESADOR
5
30
240s
T/R1
60c
LISTA
285
235s
CSPs
65
235n
CSPn
60n
T/R2
DI
20n
215
235r
CSPr
UI
85n
TRA
KSr
PROCESADOR
5n
LISTA
280
ST
75r
240r
SC
NA
210
110
EMC
130
75n

FIG. 2F

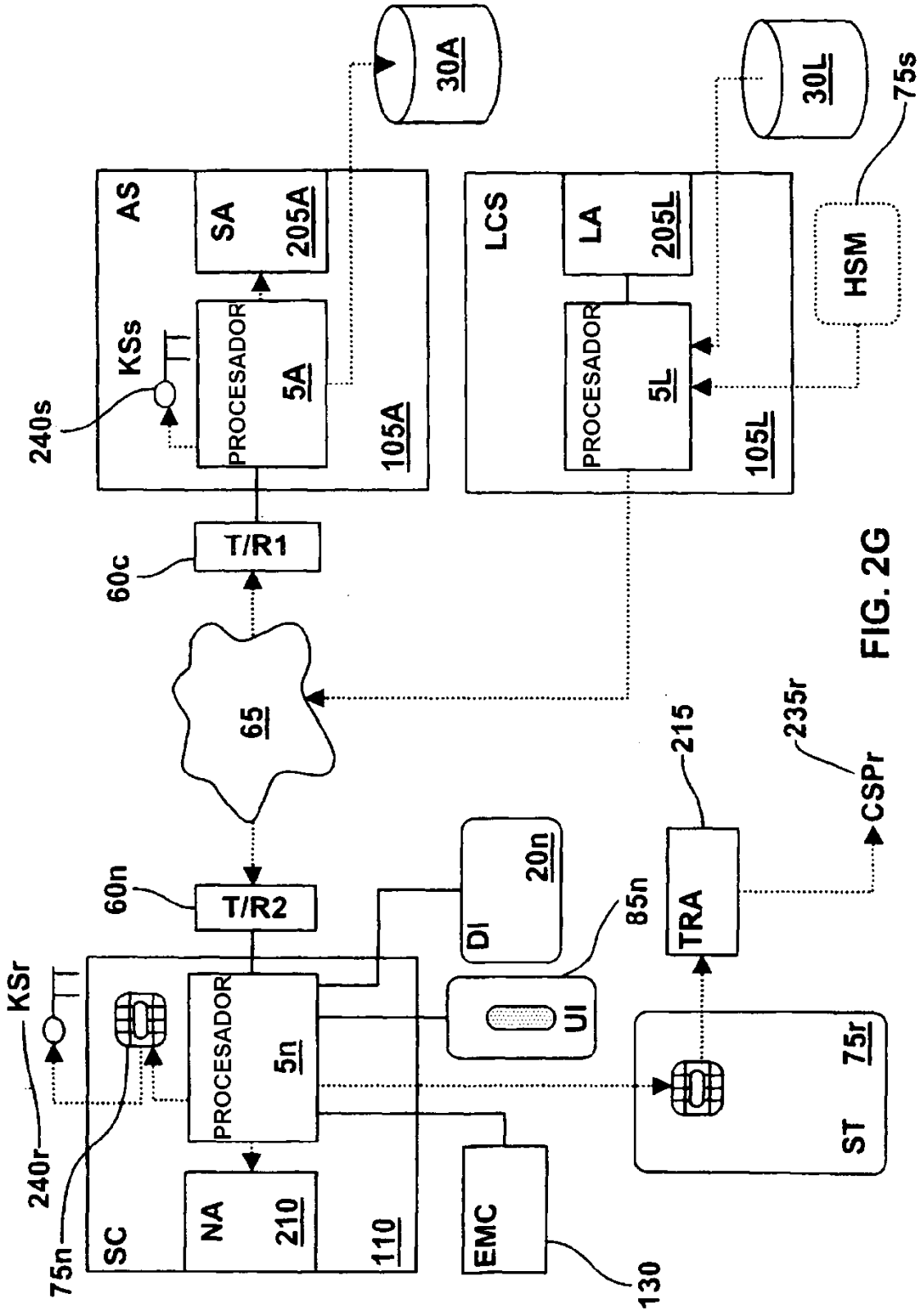
30A
30L
75s
AS
SA
205A
KSs
PROCESADOR
5A
105A
LCS
LA
205L
PROCESADOR
5L
105L
HSM
240s
T/R1
60c
65
60n
T/R2
DI
20n
85n
UI
215
TRA
235r
CSPr
KSr
PROCESADOR
5n
ST
75r
240r
75n
SC
NA
210
110
EMC
130

FIG. 2G

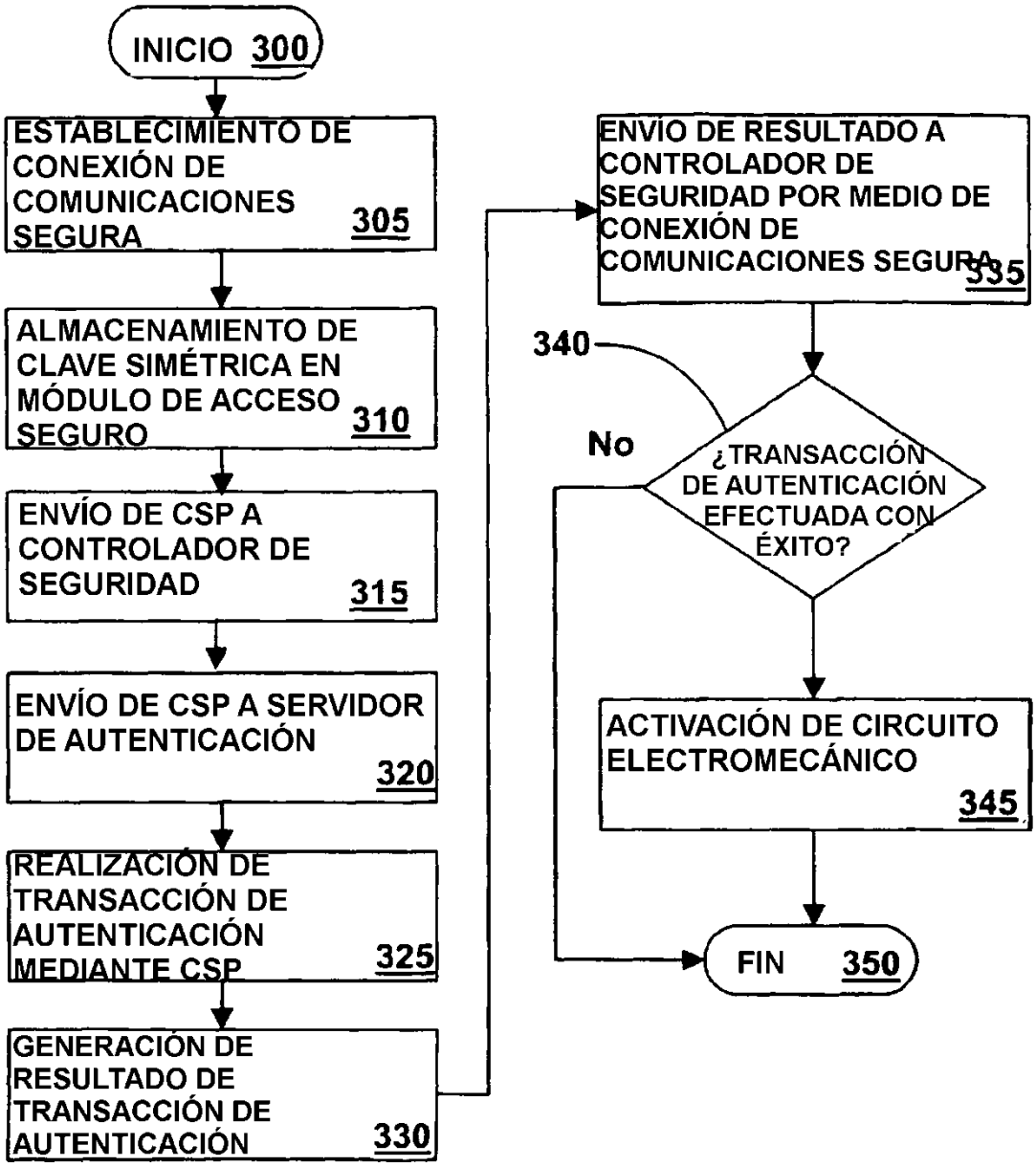
INICIO 300
ESTABLECIMIENTO DE CONEXIÓN DE COMUNICACIONES SEGURA 305
ALMACENAMIENTO DE CLAVE SIMÉTRICA EN MÓDULO DE ACCESO SEGURO 310
ENVÍO DE CSP A CONTROLADOR DE SEGURIDAD 315
ENVÍO DE CSP A SERVIDOR DE AUTENTICACIÓN 320
REALIZACIÓN DE TRANSACCIÓN DE AUTENTICACIÓN MEDIANTE CSP 325
GENERACIÓN DE RESULTADO DE TRANSACCIÓN DE AUTENTICACIÓN 330
ENVÍO DE RESULTADO A CONTROLADOR DE SEGURIDAD POR MEDIO DE CONEXIÓN DE COMUNICACIONES SEGURA 335
340
No
¿TRANSACCIÓN DE AUTENTICACIÓN EFECTUADA CON ÉXITO?
ACTIVACIÓN DE CIRCUITO ELECTROMECÁNICO 345
FIN 350

FIG. 3

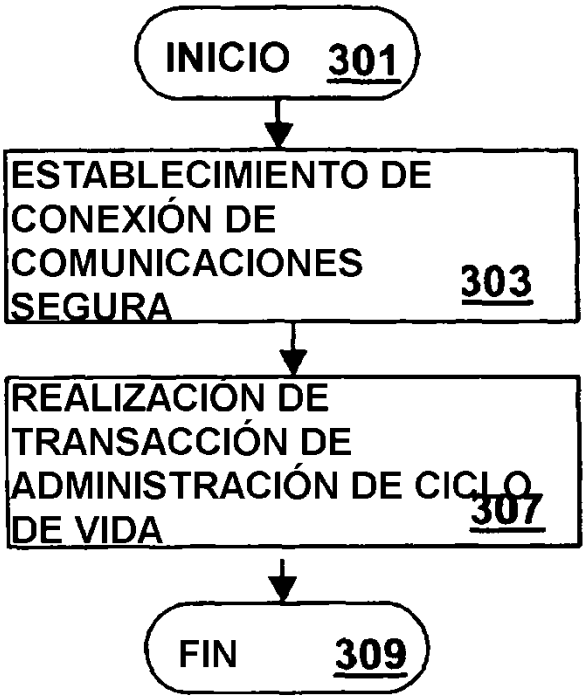
INICIO 301
ESTABLECIMIENTO DE CONEXIÓN DE COMUNICACIONES SEGURA 303
REALIZACIÓN DE TRANSACCIÓN DE ADMINISTRACIÓN DE CICLO DE VIDA 307
FIN 309

FIG. 3A

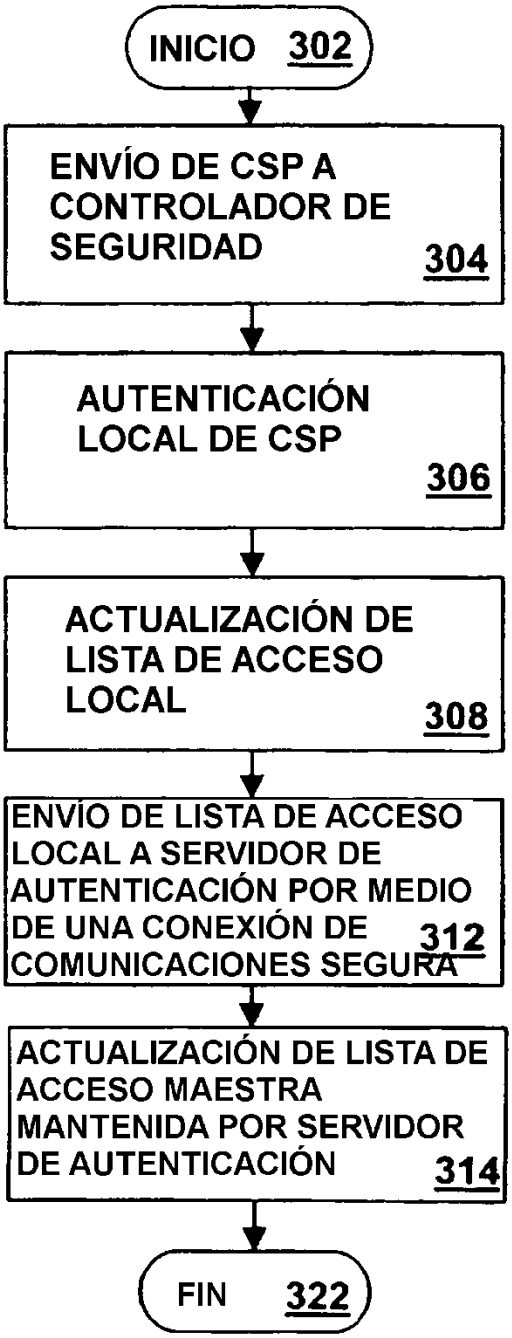
INICIO 302
ENVÍO DE CSP A CONTROLADOR DE SEGURIDAD 304
AUTENTICACIÓN LOCAL DE CSP 306
ACTUALIZACIÓN DE LISTA DE ACCESO LOCAL 308
ENVÍO DE LISTA DE ACCESO LOCAL A SERVIDOR DE AUTENTICACIÓN POR MEDIO DE UNA CONEXIÓN DE COMUNICACIONES SEGURA 312
ACTUALIZACIÓN DE LISTA DE ACCESO MAESTRA MANTENIDA POR SERVIDOR DE AUTENTICACIÓN 314
FIN 322

FIG. 3B