(19) OFICINA ESPAÑOLA DE PATENTES Y MARCAS

ESPAÑA

(11) Número de publicación: **2 388 216**

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

(12) TRADUCCIÓN DE PATENTE EUROPEA T3

(96) Número de solicitud europea: **04293090 .9**
(96) Fecha de presentación: **22.12.2004**
(97) Número de publicación de la solicitud: **1551149**
(97) Fecha de publicación de la solicitud: **06.07.2005**

(54) Título: **Mensajería universal segura para testigos de seguridad remotos**

(30) Prioridad:
22.12.2003 US 740920

(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:
Wen, Wu;
Le Saint, Eric F. y
Becquart, Jérome Antoine Marie

(74) Agente/Representante:
Curell Aguilá, Mireia

DESCRIPCIÓN

Mensajería universal segura para testigos de seguridad remotos.

Campo de la invención

La presente invención se refiere en general a un sistema, procedimiento y producto de programa informático de procesamiento de datos y, más particularmente, a una conexión de comunicaciones inalámbricas de extremo a extremo segura entre un sistema informático activado por testigo de seguridad y un dispositivo inteligente remoto que presenta un testigo de seguridad funcionalmente acoplado.

Antecedentes

En los entornos operativos de alta seguridad, el US National Institute of Standards and Technology (NIST) indica, en el documento FIPS PUB 140-2, "Security Requirements For Security tokens" para los niveles de seguridad 3 y 4, que los parámetros críticos de seguridad (CSP), tales como los datos de autenticación, las contraseñas, los PIN, los CSP, las muestras biométricas, las claves criptográficas secretas y privadas, deben introducirse o extraerse del testigo de seguridad en un formato encriptado, utilizando generalmente alguna forma de trayectoria física y/o lógica de confianza o un canal de mensajes seguro para prevenir la interceptación de los parámetros críticos de seguridad.

Los testigos de seguridad a los que se hace referencia en la presente memoria comprenden 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.

En el documento XP 002207127 de Deutsche Telekom AG: "Das TeleSecLine Crypt L für sichere Netzwerkverbindugen", se describe un sistema que ofrece la transferencia de datos protegidos a través de redes 2P basadas en Ethernet.

En el documento EP-A-0 733 971, se describe un procedimiento para administrar las conexiones entre los objetos de un sistema de objetos distribuidos.

Los intentos de proveer una trayectoria física de confianza comprenden el uso de dispositivos criptográficos de hardware instalados entre los dispositivos de entrada, tales como el teclado y posiblemente el ratón. Se da a conocer un ejemplo de dichos dispositivos de interfaz criptográfica en la patente US nº 5.841.868 de Helbig. No obstante, los gastos de hardware y la carga administrativa adicional incrementan en gran medida el coste del sistema informático.

En otra propuesta (patente US nº 4.945.468 de Carson, *et al.*), se genera una trayectoria de confianza facilitando una nueva ventana de terminal virtual que permite la entrada segura de los CSP. La nueva ventana de terminal virtual se aísla eficazmente de los demás procesos en ejecución. Este procedimiento constituye una propuesta razonablemente segura, pero no extiende la trayectoria de confianza hasta los dispositivos periféricos de seguridad, tales como los módulos criptográficos, los testigos de seguridad y los escáneres biométricos.

En otra propuesta, el documento US 2002/0095587 A1 de Doyle *et al.* da a conocer una conexión SSL inalámbrica o equivalente en la que se utilizan claves criptográficas de tiempo limitado negociadas para mantener una cadena de confianza entre los dispositivos de seguridad interconectados. No obstante, el mecanismo dado a conocer depende en gran medida de varios pares de claves de criptografía de clave pública, hecho que dificulta su mantenimiento y que puede reducir el rendimiento global debido a la lentitud relativa del procesamiento de las transacciones cuando se emplea con una tarjeta inteligente. Además, la negociación de las claves criptográficas de tiempo limitado depende de los dispositivos que contienen un reloj de sistema para el cambio de claves criptográficas. Las tarjetas inteligentes y dispositivos similares no comprenden relojes de sistema y por lo tanto dependen de su anfitrión para la temporización de los eventos, hecho que puede provocar problemas de seguridad cuando el anfitrión no es de confianza.

En la técnica correspondiente, se dispone de mecanismos criptográficos que pueden adaptarse para encriptar un CSP de entrada con una clave criptográfica para su transporte seguro, a través de una desencriptación final activada por testigo de seguridad llevada a cabo por una aplicación de seguridad instalada en el testigo de seguridad. No obstante, el mecanismo criptográfico empleado por el sistema informático activado por testigo de seguridad debe aportar un nivel suficiente de seguridad para prevenir la interceptación de las claves criptográficas utilizadas en la encriptación del CSP y además limita la vulnerabilidad a los ataques de repetición.

Otro tipo común de vulnerabilidad en la técnica relativa se refiere a la falta de capacidad para enlazar un CSP con una sesión, lo cual permite el acceso potencial de una entidad no autorizada a un testigo de seguridad

desbloqueado. Para hacer frente a esta potencial vulnerabilidad, el CSP se almacena habitualmente en caché o en memoria y se presenta mediante software al testigo de seguridad cada vez que se requiere el acceso. Los CSP almacenados en caché o memoria son igualmente vulnerables a la interceptación u otros peligros potenciales causados por una entidad no autorizada. Por consiguiente, sería sumamente conveniente ofrecer un sistema de transporte seguro de CSP que limite la capacidad de interceptar una clave criptográfica durante las sesiones de comunicaciones inalámbricas, sea relativamente invulnerable a un ataque tipo repetición, reduzca al mínimo la cantidad de veces que se solicita al usuario que introduzca los CSP que ya se han facilitado en una sesión y no almacene los CSP ni en memoria ni en caché.

Sumario

Con este propósito, la presente invención es un procedimiento para establecer una conexión de comunicaciones de extremo a extremo segura según la reivindicación 1, un correspondiente sistema según la reivindicación 20 y un producto de programa informático según la reivindicación 43.

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

La presente invención aborda las limitaciones descritas anteriormente y ofrece una conexión de comunicaciones de extremo a extremo segura y eficaz para intercambiar de forma segura información entre un sistema informático activado por testigo de seguridad y un dispositivo remoto inteligente que presenta un testigo de seguridad acoplado. La parte del procedimiento de la presente invención comprende las etapas de realización de una primera transacción de seguridad en la que se autentica un testigo de seguridad ante un sistema informático activado por testigo de seguridad, establecimiento de una conexión de comunicaciones segura entre el testigo de seguridad y el sistema informático activado por testigo de seguridad que integra un conjunto de claves simétricas compartidas generado durante la primera transacción de seguridad, asignación de por lo menos una clave del conjunto de claves simétricas compartidas a un canal de comunicaciones dedicado accesible para el testigo de seguridad y realización de una segunda transacción de seguridad en la que se autentica un usuario ante dicho testigo de seguridad.

Si la segunda transacción de seguridad se realiza con éxito, se efectúan entonces unas etapas para señalar el resultado afirmativo al sistema informático activado por testigo de seguridad. El segundo estado de seguridad es necesario para que dicho testigo de seguridad pueda utilizar la conexión de comunicaciones segura.

La primera transacción de seguridad se lleva a cabo mediante un protocolo de desafío/respuesta (en inglés, "*challenge/response protocol*") que integra un par de claves asimétricas. El sistema informático activado por testigo de seguridad genera un desafío que se encripta con la clave pública asociada al testigo de seguridad.

El desafío encriptado se envía entonces al testigo de seguridad. El testigo de seguridad desencripta el desafío mediante la parte complementaria de la clave privada a la clave pública y devuelve el desafío en texto no encriptado al sistema informático activado por testigo de seguridad para su comprobación.

La clave pública se transfiere al sistema informático activado por testigo de seguridad por medio de un certificado digital como parte del establecimiento de la conexión de comunicaciones inalámbricas.

La segunda transacción de seguridad autentica al usuario ante el testigo de seguridad por medio del parámetro crítico de seguridad del usuario que se facilita de forma directa o indirecta al testigo de seguridad a través del dispositivo inteligente remoto. Una vez que la segunda transacción de seguridad se ha realizado con éxito, se da permiso al usuario para que acceda a uno o más recursos seguros asociados al testigo de seguridad, el sistema informático activado por testigo de seguridad o a ambos.

En formas de realización relacionadas de la presente invención, el testigo de seguridad y el sistema informático activado por testigo de seguridad mantienen unos estados de seguridad. Los estados de seguridad se establecen cuando la primera y la segunda transacciones de seguridad se han realizado con éxito.

La conexión de comunicaciones seguras se establece generando, en el sistema informático activado por testigo de seguridad, un conjunto de claves simétricas compartidas, encriptando una de las claves simétricas generadas con la clave pública, enviando la clave simétrica encriptada al testigo de seguridad, desencriptando la clave simétrica con la clave privada equivalente y asignando la clave simétrica desencriptada a un canal de comunicaciones dedicado. El canal de comunicaciones dedicado impide que el número de conexiones de comunicaciones inalámbricas seguras con el testigo de seguridad sobrepase un límite predeterminado. Habitualmente, el límite predeterminado se fija en 1.

En otra forma de realización de la presente invención, el dispositivo inteligente remoto facilita la respuesta de retorno del usuario, tras solicitarle que seleccione una transacción de autenticación local o remota y que indique el parámetro crítico de seguridad.

En otra forma de realización de la presente invención, se impide la autenticación del usuario si este se halla fuera del alcance predefinido de un detector de proximidad acoplado al sistema informático activado por testigo de seguridad.

En otra forma de realización de la presente invención, el sistema informático activado por testigo de seguridad facilita la respuesta de retorno sensorial del usuario que indica que una transacción de autenticación remota está en curso. La respuesta sensorial del usuario comprende una respuesta de retorno visual, táctil, auditiva o vibratoria.

Una primera forma de realización sistemática de la presente invención comprende un sistema informático activado por testigo de seguridad que establece comunicaciones inalámbricas con un dispositivo inteligente remoto que presenta un testigo de seguridad acoplado funcionalmente. El sistema informático activado por testigo de seguridad comprende unos primeros medios de transacción de seguridad para por lo menos autenticar el testigo de seguridad ante el sistema informático activado por testigo de seguridad, y unos primeros medios de conexión de comunicaciones seguros para por lo menos establecer un enlace codificado criptográficamente entre el sistema informático activado por testigo de seguridad y el testigo de seguridad. Los primeros medios de transacción de seguridad comprenden unos medios de protocolo de desafío/respuesta y unos medios de criptografía asimétrica. Los primeros medios de conexión de comunicaciones seguros comprenden unos medios de generación de conjunto de claves simétricas y unos medios de intercambio de claves simétricas seguros.

El sistema informático activado por testigo de seguridad comprende además unos primeros medios de acceso seguros para permitir al usuario el acceso a uno o más recursos seguros tras la recepción de una señal afirmativa.

La ejecución con éxito de los primeros medios de transacción seguros y la recepción de la señal de resultado afirmativo determinan el establecimiento de un primer estado de seguridad y un segundo estado de seguridad, respectivamente, asociados al sistema informático activado por testigo de seguridad.

El dispositivo inteligente remoto comprende unos medios de interfaz de testigo de seguridad para por lo menos acoplar funcionalmente el testigo de seguridad al dispositivo inteligente remoto, y unos medios de interfaz de usuario para por lo menos recibir y encaminar un parámetro crítico de seguridad facilitado por el usuario a través de los medios de interfaz de testigo de seguridad. Los medios de la interfaz de usuario comprenden unos medios condicionales para recibir condicionalmente el parámetro crítico de seguridad. Los medios condicionales están diseñados para limitar o prevenir la recepción del parámetro crítico de seguridad hasta que se establece el enlace codificado criptográficamente. Los medios de interfaz de testigo de seguridad comprenden unos medios de comunicaciones de testigo de seguridad y unos medios de transferencia de potencia electromagnética.

El testigo de seguridad comprende un medios de conexión de comunicaciones seguros para por lo menos establecer el enlace codificado criptográficamente en conjunción con los primeros medios de conexión de comunicaciones seguros, unos medios de canal de comunicaciones dedicado para impedir que se establezca un enlace concurrente codificado criptográficamente con el testigo de seguridad, un segundos medios de transacción de seguridad para por lo menos autenticar al usuario ante el testigo de seguridad mediante por lo menos el parámetro crítico de seguridad, y unos medios de señalización afirmativa para enviar una señal afirmativa al sistema informático activado por testigo de seguridad tras el éxito de la ejecución de los segundos medios de transacciones de seguridad. En una forma de realización de la presente invención, los medios de canal de comunicaciones dedicado comprenden unos medios de identificación de canal exclusivo que son direccionables por el sistema informático activado por testigo de seguridad.

En una forma de realización relacionada de la presente invención, el establecimiento del enlace codificado criptográficamente determina el establecimiento de un primer estado de seguridad del testigo, y el éxito de la ejecución de los segundos medios de transacción de seguridad determina el establecimiento de un segundo estado de seguridad del testigo. En una forma de realización relacionada de la presente invención, el segundo estado de seguridad es necesario para que el testigo de seguridad pueda utilizar la conexión de comunicaciones segura.

Una segunda forma de realización sistemática de la presente invención comprende un sistema informático activado por testigo de seguridad que establece comunicaciones de procesamiento con un dispositivo inteligente remoto y un testigo de seguridad acoplado al dispositivo inteligente remoto. El sistema informático activado por testigo de seguridad comprende un primer procesador, una primera memoria acoplada al primer procesador, por lo menos una aplicación de autenticación remota almacenada funcionalmente en una primera parte de la primera memoria, que presenta instrucciones lógicas ejecutables por el primer procesador para autenticar el testigo de seguridad, establecer una conexión de comunicaciones de extremo a extremo segura con el testigo de seguridad y permitir al usuario el acceso a uno o más recursos seguros tras la recepción de una señal afirmativa enviada desde el testigo de seguridad.

El sistema informático activado por testigo de seguridad comprende además un primer transceptor inalámbrico acoplado funcionalmente al primer procesador, y una clave pública asociada al testigo de seguridad, almacenada en una segunda parte de la primera memoria y recuperable.

Dicha por lo menos una aplicación de autenticación remota comprende además instrucciones lógicas ejecutables por el primer procesador para generar un conjunto de claves simétricas y realizar un intercambio de claves seguro con el testigo de seguridad.

El dispositivo inteligente remoto comprende un segundo procesador, una segunda memoria acoplada al segundo

procesador, una interfaz de testigo de seguridad acoplada al segundo procesador, una interfaz de usuario acoplada al segundo procesador y por lo menos una aplicación de interfaz de dispositivo remoto almacenada funcionalmente en una parte de la segunda memoria. Dicha por lo menos una aplicación de interfaz de dispositivo remoto comprende instrucciones lógicas ejecutables por el segundo procesador para emular una interfaz de dispositivo de testigo de seguridad acoplada localmente a por lo menos el sistema informático activado por testigo de seguridad, y recibir y encaminar condicionalmente un parámetro crítico de seguridad que el usuario facilita al testigo de seguridad por medio de la interfaz de usuario. El dispositivo inteligente remoto comprende además un segundo transceptor inalámbrico acoplado funcionalmente al segundo procesador.

La interfaz de comunicaciones y energía electromagnética comprende unos medios inductivos, capacitivos o de contacto eléctrico para acoplar funcionalmente el testigo de seguridad con el dispositivo inteligente remoto. Dicha por lo menos una aplicación de interfaz de dispositivo remoto comprende además instrucciones lógicas ejecutables por el segundo procesador para impedir la recepción del parámetro crítico de seguridad del usuario antes del establecimiento de la conexión de comunicaciones de extremo a extremo segura.

El testigo de seguridad comprende por lo menos un tercer procesador, una tercera memoria acoplada a por lo menos un tercer procesador, una interfaz de comunicaciones y potencia electromagnética acoplada a por lo menos un tercer procesador y la interfaz de testigo de seguridad, y por lo menos una aplicación de autenticación remota de testigo almacenada funcionalmente en una primera parte de la tercera memoria.

Dicha por lo menos una aplicación de autenticación de testigo remota comprende instrucciones lógicas ejecutables por el por lo menos un tercer procesador para establecer la conexión de comunicaciones de extremo a extremo segura en conjunción con el sistema informático activado por testigo de seguridad, restringir la conexión de comunicaciones de extremo a extremo segura a una única conexión de comunicaciones inalámbricas segura, autenticar al usuario y enviar la señal afirmativa al sistema informático activado por testigo de seguridad si la autenticación del usuario se ha realizado con éxito. El testigo de seguridad comprende además una clave privada recuperable almacenada en una segunda parte de la tercera memoria y un parámetro crítico de seguridad de referencia recuperable almacenado en una tercera parte de la tercera memoria. La clave privada es la parte complementaria de la clave pública. Dicha por lo menos una aplicación de autenticación de testigo remota autentica al usuario comparando el parámetro crítico de seguridad facilitado por el usuario con el parámetro crítico de seguridad de referencia.

La restricción a la conexión de comunicaciones de extremo a extremo segura se aplica a un canal de comunicaciones dedicado controlado por la por lo menos una aplicación de autenticación de testigo remota. El canal de comunicaciones dedicado comprende un identificador exclusivo direccionable por el sistema informático activado por testigo de seguridad.

Las claves públicas y privadas se integran en un protocolo de desafío/respuesta utilizado para autenticar el testigo de seguridad ante el sistema informático activado por testigo de seguridad, y se utilizan además para realizar un intercambio de claves simétricas seguro desde el sistema informático activado por testigo de seguridad hasta el testigo de seguridad.

En otra forma de realización de la presente invención, un detector de proximidad se acopla al sistema informático accionado por testigo de seguridad que impide la autenticación o la utilización del canal de comunicaciones seguro si el testigo de seguridad se halla fuera del alcance predefinido del sistema informático activado por testigo de seguridad.

En una última forma de realización de la presente invención, se ofrece un producto de programa informático. La forma de realización del producto de programa informático es tangible y legible por un procesador de testigo de seguridad y comprende unas instrucciones ejecutables almacenadas en memoria que causan la utilización, por el procesador de testigo de seguridad, de uno o más servicios de emulación de testigo de seguridad prestados por un procesador de dispositivo inteligente remoto, el establecimiento de una conexión de comunicaciones de extremo a extremo segura en conjunción con un procesador de sistema informático activado por testigo de seguridad, la restricción de la conexión de comunicaciones de extremo a extremo segura a una única conexión de comunicaciones inalámbricas segura, la autenticación del usuario y el envío de una señal afirmativa al procesador del sistema informático activado por testigo de seguridad si la autenticación del usuario se realiza con éxito.

El producto de programa informático comprende además instrucciones ejecutables almacenadas en memoria para causar la autenticación del testigo de seguridad por el procesador del sistema informático activado por testigo de seguridad, el establecimiento de la conexión de comunicaciones de extremo a extremo segura con el testigo de seguridad y la habilitación del acceso a uno o más recursos seguros para el usuario tras la recepción de la señal afirmativa enviada desde el testigo de seguridad.

El producto de programa informático comprende además instrucciones ejecutables almacenadas en memoria para causar la prestación, por el procesador del dispositivo inteligente remoto, del servicio o los servicios de emulación de testigo de seguridad al procesador de testigo de seguridad, y la recepción y el encaminamiento de un parámetro

crítico de seguridad facilitado por el usuario por medio de la interfaz de usuario al testigo de seguridad.

La forma tangible del producto de programa informático comprende unos medios magnéticos, unos medios ópticos o unos medios lógicos almacenados en formato de código que comprende el código de octetos, el código compilado, el código interpretado, el código compilable y el código interpretable.

Breve descripción de los dibujos

Las características y las ventajas de la presente invención resultarán evidentes 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 y sentido verdaderos de la presente invención definido en las reivindicaciones adjuntas.

La figura 1 es un diagrama de bloques generalizado de un sistema informático activado por testigo de seguridad.

La figura 1A es un diagrama de bloques generalizado de un dispositivo inteligente remoto.

La figura 1B es un diagrama de bloques generalizado 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 sistema informático activado por testigo de seguridad establece comunicaciones de procesamiento con un dispositivo inteligente remoto provisto de un testigo de seguridad a través de un enlace inalámbrico.

La figura 2A es un diagrama de bloques detallado de la presente invención, en el que se representa cómo se transfiere una clave pública al sistema informático activado por testigo de seguridad.

La figura 2B es un diagrama de bloques detallado de la presente invención, en el que se representa cómo recibe el testigo de seguridad un desafío encriptado generado por el sistema informático activado por testigo de seguridad como parte inicial de un protocolo de desafío/respuesta de autenticación.

La figura 2C es un diagrama de bloques detallado de la presente invención, en el que se representa cómo devuelve el testigo de seguridad el desafío en texto no encriptado al sistema informático activado por testigo de seguridad como parte final del protocolo de desafío/respuesta de autenticación.

La figura 2D es un diagrama de bloques detallado de la presente invención, en el que se representa cómo se genera un conjunto de claves simétricas y cómo se realiza un intercambio de claves seguro entre el sistema informático activado por testigo de seguridad y el testigo de seguridad.

La figura 2E es un diagrama de bloques detallado de la presente invención, en el que se representa cómo se establece una conexión de comunicaciones de extremo a extremo segura entre el sistema informático activado por testigo de seguridad y el testigo de seguridad.

La figura 2F es un diagrama de bloques detallado de la presente invención, en el que se representa cómo se transmite el parámetro crítico de seguridad del usuario al dispositivo inteligente remoto y cómo se encamina este hacia el testigo de seguridad acoplado funcionalmente para autenticar al usuario.

La figura 2G es un diagrama de bloques detallado de la presente invención, en el que se representa cómo la autenticación del dispositivo inteligente remoto ante el sistema informático activado por testigo de seguridad se ha realizado con éxito.

La figura 3 es un diagrama de flujo que ilustra las etapas principales asociadas al establecimiento de la conexión de comunicaciones de extremo a extremo segura entre el sistema informático activado por testigo de seguridad y un dispositivo inteligente remoto que presenta un testigo de seguridad acoplado funcionalmente.

Descripción detallada

La presente invención se refiere a una conexión de comunicaciones de extremo a extremo segura y anónima que permite a un dispositivo inteligente remoto emular un dispositivo de testigo de seguridad conectado localmente sin necesidad de establecer una conexión física real con un sistema informático activado por testigo de seguridad. La conexión de comunicaciones de extremo a extremo segura y anónima se establece a través de un enlace o una red de comunicaciones inalámbricas. Las aplicaciones están concebidas para programarse en un lenguaje de alto nivel, tal como Java ™, C++, C #, C o Visual Basic ™.

Con referencia a la figura 1, se ilustra un diagrama de bloques de un sistema informático activado por testigo de seguridad 105.

El sistema informático activado por testigo de seguridad 105 comprende un procesador 5c, una memoria principal 10c, una pantalla 20c acoplada eléctricamente a una interfaz de pantalla 15c, un subsistema de memoria secundaria 25c acoplado eléctricamente a una unidad de disco duro 30c, una unidad de memoria extraíble 35c acoplada eléctricamente a un dispositivo de memoria extraíble 40c y una interfaz de memoria auxiliar extraíble 45 acoplada eléctricamente a un dispositivo de memoria auxiliar extraíble 50c.

Un subsistema de interfaz de comunicaciones 55c está acoplado a un transceptor inalámbrico 60c y una red o un enlace inalámbrico 65, un testigo de seguridad opcional 75 acoplado eléctricamente a una interfaz de testigo de seguridad 70c y una interfaz de entrada del usuario 80c que comprende un ratón y un teclado 85, un escáner biométrico opcional 95c acoplado eléctricamente a una interfaz de escáner biométrico opcional 90c y un detector de proximidad opcional 115c acoplado a la interfaz de comunicaciones 55c. El detector de proximidad 115c impide que se realicen las autenticaciones remotas cuando el testigo de seguridad 75r (figura 1A) no está dentro de la distancia predefinida del detector de proximidad 115c o dentro del alcance de detección del detector de proximidad 115c. Un ejemplo de sistema de proximidad adecuado adaptable al uso en la presente invención es el comercializado por Ensure Technologies (Xyloc), 3526 West Liberty Road, Suite 100, Ann Arbor, Michigan 48103; www.ensuretech.com. Las bases técnicas para los sistemas de detección de proximidad de Xyloc se dan a conocer en las patentes y solicitudes de patentes US nº 6.456.958, US nº 6.307.471, US nº 6.070.240, US 20020104012 A1, US 20020069030A1 y US 20020065625, todas ellas asignadas a Ensure Technologies.

El procesador 5c, la memoria principal 10c, la interfaz de pantalla 15c, el subsistema de memoria secundaria 25c y el sistema de interfaz de comunicaciones 55c están acoplados eléctricamente a una infraestructura de comunicaciones 100c. El sistema informático activado por testigo de seguridad 105 comprende un sistema operativo, por lo menos una aplicación de autenticación remota, software para otras aplicaciones, software de criptografía capaz de realizar funciones de criptografía simétrica y asimétrica, software de mensajería segura y software de interfaz de dispositivo. Con referencia a la figura 1A, se ilustra un diagrama de bloques de un dispositivo inteligente remoto 110. El dispositivo inteligente remoto 110 comprende un procesador 5r, una memoria principal 10r, una pantalla 20r acoplada eléctricamente a una interfaz de pantalla 15r, un subsistema de memoria secundaria 25r acoplada eléctricamente a una unidad de disco duro opcional 30r, una unidad de almacenamiento virtual 35r y un módulo de memoria extraíble 50r acoplado eléctricamente a una interfaz de módulo de memoria extraíble 45r.

Un subsistema de interfaz de comunicaciones 55r se acopla a un transceptor inalámbrico 60r y una red o un enlace inalámbrico 65, un testigo de seguridad 75 acoplado eléctricamente a una interfaz de testigo de seguridad 70r y una interfaz de entrada del usuario 80r que comprende un ratón y un teclado 85r, y un escáner biométrico opcional 95r acoplado eléctricamente a una interfaz de escáner biométrico opcional 90r.

El procesador 5r, la memoria principal 10r, la interfaz de pantalla 15r, el subsistema de memoria secundaria 25r y el sistema de interfaz de comunicaciones 55r están acoplados eléctricamente a una infraestructura de comunicaciones 100r. El dispositivo inteligente remoto comprende un sistema operativo, por lo menos una aplicación de dispositivo remoto, software para otras aplicaciones, software de criptografía capaz de realizar funciones criptográficas simétricas y asimétricas, software de mensajería segura y software de interfaz de dispositivo.

Con referencia a la figura 1B, se ilustra un diagrama de bloques del testigo de seguridad 75. El testigo de seguridad 75 comprende unos medios de conexión inalámbrica, óptica y/o eléctrica 60t, 60w compatibles con las interfaces de testigo de seguridad 70c, 70r, un procesador 5t, un coprocesador criptográfico opcional 5tc acoplado al procesador 5t, 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 los medios de conexión 60t.

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 una infraestructura de comunicaciones 100t. La EEPROM 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 dispositivo inteligente remoto y el software de criptografía activado por testigo de seguridad, por lo menos una aplicación de autenticación remota por testigo, uno o más recursos seguros protegidos por parámetro crítico de seguridad acoplados a la por lo menos una aplicación de autenticación remota por testigo y un par de claves de infraestructura de clave pública (PKI) acoplado funcionalmente a la por lo menos una aplicación de autenticación remota por testigo.

En la memoria permanente 10nvm, 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 generalizada de la presente invención. La presente invención comprende un dispositivo inteligente remoto IRD 110 que establece comunicaciones de procesamiento a través de

un enlace inalámbrico 65 con un sistema informático activado por testigo de seguridad 105. Un testigo de seguridad ST 75 se acopla funcionalmente al dispositivo inteligente remoto IRD 110 por medio de un dispositivo de interfaz de testigo de seguridad STI 70r.

El dispositivo inteligente remoto IRD 110 comprende un transceptor inalámbrico funcionalmente acoplado T/R2 60r, una interfaz de testigo de seguridad STI 70r, unos medios de entrada del usuario UI 85 y una pantalla DI 202r que facilita al usuario información relacionada con las opciones de autenticación y los estados de autenticación disponibles.

La interfaz de testigo de seguridad STI 70r comprende dispositivos de interfaz de contacto óptico, capacitivo, inductivo y eléctrico directo y suministra potencia electromagnética y aporta continuidad en las comunicaciones con el dispositivo inteligente remoto IRD 110. Por último, se instala por lo menos una aplicación de interfaz de dispositivo remoto RDI 210 en el dispositivo inteligente remoto IRD 110.

Dicha por lo menos una aplicación de interfaz de dispositivo remoto RDI 210 es generalmente una aplicación de software intermediario que permite al dispositivo inteligente remoto IRD 110 emular un periférico de dispositivo de testigo de seguridad local acoplado al sistema informático activado por testigo de seguridad CS 105 sin necesidad de una conexión física real. Cuando está activada, la por lo menos una aplicación de interfaz de dispositivo remoto RDI 210 presta servicios de interfaz de testigo de seguridad para intercambiar datos con el sistema informático activado por testigo de seguridad, recibir un parámetro crítico de seguridad del usuario facilitado por medio de la interfaz de usuario UI 85r y encaminar el parámetro crítico de seguridad del usuario hacia el testigo de seguridad ST 75 para la autenticación o la verificación del usuario.

Dicha por lo menos una aplicación de interfaz de dispositivo remoto RDI 210 facilita además instrucciones y respuestas de retorno del usuario por medio de una pantalla DI 20r.

El testigo de seguridad ST 75 está acoplado funcionalmente al dispositivo de interfaz de testigo de seguridad STI 70r a través de unos medios de conexión 60t y comprende un par de clave pública y clave privada Kpub 225t, Kpri 230 y un parámetro crítico de seguridad de referencia CSPr 235 almacenado en la memoria del testigo y recuperable. Por lo menos una aplicación de acceso remoto por testigo TRA 215 está igualmente instalada en la memoria del testigo.

Dicha por lo menos una aplicación de acceso remoto por testigo TRA 215 permite al testigo de seguridad ST 75 establecer una conexión de comunicaciones de extremo a extremo segura en conjunción con el sistema informático activado por testigo de seguridad CS105, restringir la conexión de comunicaciones de extremo a extremo segura a una única conexión de comunicaciones inalámbricas segura por medio de un canal de comunicaciones inalámbricas dedicado Wc 220w, autenticar al usuario comparando el parámetro crítico de seguridad facilitado por el usuario con el parámetro crítico de seguridad de referencia CSPr 235 y enviar una señal afirmativa al sistema informático activado por testigo de seguridad CS105 si la autenticación del usuario se realiza con éxito. El canal de comunicaciones local Lc1, Lc2, Lcn 220 permite establecer varias sesiones de comunicaciones cuando el ST 75 está conectado localmente al dispositivo inteligente remoto IRD 110 o al sistema informático activado por testigo de seguridad CS 105.

El canal de comunicaciones inalámbricas dedicado Wc 220w restringe el número de sesiones de comunicaciones que se pueden establecer a distancia. La por lo menos una aplicación de acceso remoto por testigo TRA 215 comprende una tabla de estados de autenticación 240, 245 que debe cumplimentarse para obtener el permiso de acceso 250t a uno o más recursos de testigo seguros SRt 255t. En una forma de realización de la presente invención, la sesión de comunicación no está disponible para el testigo de seguridad ST 75 hasta que no se ha cumplimentado correctamente la tabla de estados de autenticación 240, 245 mediante la autenticación del usuario.

El sistema informático activado por testigo de seguridad 105 comprende un transceptor inalámbrico T/R1 compatible con el transceptor inalámbrico T/R2 instalado en el dispositivo inteligente remoto IRD 110 y por lo menos una aplicación de acceso remoto RAA 205. La por lo menos una aplicación de acceso remoto RAA 205 es generalmente una aplicación de software intermediario que permite al sistema informático activado por testigo CS 105 autenticar el testigo de seguridad ST 75, establecer la conexión de comunicaciones de extremo a extremo segura con el testigo de seguridad ST 75 a través del enlace inalámbrico 65 y permitir al usuario el acceso 250c a uno o más recursos seguros tras la recepción de una señal afirmativa enviada desde el testigo de seguridad ST 75.

En una forma de realización de la presente invención, la por lo menos una aplicación de acceso remoto RAA 205 comprende una tabla de estados de autenticación 260, 265 que debe cumplimentarse para obtener permiso para acceder 250c al recurso o los recursos de sistema informático seguros SRc 255c. El sistema informático activado por testigo de seguridad 105 comprende además una pantalla 20c que facilita al usuario información relacionada por lo menos con el estado de autenticación 203c.

El protocolo de mensajería utilizado para comunicarse con el testigo de seguridad ST 75 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 RAA 205 instalada en el sistema informático activado por testigo de seguridad CS 110 o mediante la interfaz de dispositivo remoto RDI 210 instalada en el dispositivo inteligente remoto IRD 110.

Se describe una disposición segura para intercambiar mandatos y respuestas APDU entre el testigo de seguridad ST 75 y el sistema informático activado por testigo de seguridad CS 105 en el documento US 2002-0162021, que puede consultarse.

También pueden integrarse protocolos de autenticación ampliables (EAP), tales como los descritos en las normas de Internet RFC 2284 o RFC 2716, en la conexión de comunicaciones.

Las tablas de estados de autenticación 240, 245, 260, 265 pueden formar parte de un conjunto preestablecido de políticas de seguridad. En una forma de realización de la presente invención, las políticas de seguridad mantenidas en el testigo de seguridad ST 75 determinan los requisitos de acceso, tal como se describe en el documento US 2004-0123152 A1, titulado "Uniform Framework for Security Tokens", que puede consultarse.

Pueden combinarse políticas de seguridad adicionales con las políticas de seguridad establecidas para el testigo de seguridad, tal como se describe en el documento US 2004-0221174 A1, que asimismo puede consultarse.

Con referencia a la figura 2A, el usuario inicia la conexión de comunicaciones de extremo a extremo segura al seleccionar una opción de autenticación remota 204r en la pantalla DI 20r asociada al dispositivo inteligente remoto IRD 110. Dicha por lo menos una aplicación de acceso remoto por testigo 215 causa el envío de la clave pública Kpub 225t al sistema informático activado por testigo CS 105 desde el testigo de seguridad ST 75.

En una forma de realización alternativa de la presente invención, no se requiere ninguna interacción del usuario para iniciar la conexión de comunicaciones de extremo a extremo segura. En la forma de realización alternativa de la presente invención, la conformación de conexión de las comunicaciones entre los dos transceptores inalámbricos T/R1 60c, T/R2 60r causa de forma automática la ejecución de la por lo menos una aplicación de acceso remoto por testigo 215.

En la forma de realización preferida de la presente invención, se envía una clave pública Kpub 225t o un duplicado de esta Kpub 225c al sistema informático activado por testigo de seguridad CS 105 en un certificado X.509, donde se almacena y puede recuperarse posteriormente. La clave pública Kpub 225c se utilizará para autenticar el testigo de seguridad ST 75 ante el sistema informático activado por testigo de seguridad CS 105, y para realizar un intercambio de claves simétricas seguro entre el sistema informático activado por testigo de seguridad CS 105 y el testigo de seguridad ST 75.

Con referencia a la figura 2B, la recepción de la clave pública Kpub 225c causa la generación, por la por lo menos una aplicación de acceso remoto, de un desafío [C] 270c que se encripta 275e mediante la clave pública Kpub 225c, y a continuación el criptograma resultante [C]Kpub 280c se envía a través del enlace inalámbrico 65 al testigo de seguridad ST 75.

La pantalla DI 20c asociada al sistema informático activado por testigo de seguridad CS 105 facilita una respuesta de retorno del usuario 205c, en la que se indica que se ha iniciado una transacción de autenticación remota. Dicha por lo menos una aplicación de acceso remoto por testigo TRA 215 recibe y desencripta 275d el criptograma [C]Kpub 280c mediante la clave privada complementaria Kpri 230 que genera la respuesta en texto no encriptado del testigo [C] 270r al desafío.

Con referencia a la figura 2C, la respuesta del testigo al desafío [C] 270r se transmite al sistema informático activado por testigo de seguridad CS 105, donde la aplicación de acceso remoto RAA 205 compara 222 la respuesta recibida [C] 270r con el desafío inicial [C] 270c. Si la respuesta del testigo [C] 270r coincide con el desafío inicial [C] 270c, se realiza la parte de autenticación de PKI de la tabla de estados de autenticación del sistema informático 260. Si el testigo de seguridad ST 75 no puede realizar esta primera transacción de autenticación, el procesamiento termina, y entonces es necesario intentar establecer de nuevo la conexión de comunicaciones de extremo a extremo segura.

Con referencia a la figura 2D, la aplicación de acceso remoto RAA 205 inicia una primera parte de la conexión de comunicaciones de extremo a extremo segura y anónima que genera un conjunto de claves simétricas. Los conjuntos de claves simétricas KSt 285t y KSc 285s están constituidos por claves simétricas idénticas generadas u obtenidas a partir de un número aleatorio que preferentemente tiene una fortaleza de por lo menos 64 bits, suficiente para ofrecer una seguridad y un rendimiento adecuados.

Dicha por lo menos una aplicación de acceso remoto RAA 205 encripta 275e una de las claves simétricas KSt 285t mediante la clave pública Kpub 225c, y a continuación el criptograma resultante [KSt]Kpub 290t se envía al testigo de seguridad ST 75 a través del enlace inalámbrico 65. En una forma de realización de la presente invención, se incorpora un identificador de canal Wc 220w a un encabezamiento del mensaje asociado al criptograma, que indica el canal de comunicaciones dedicado en el que debe utilizarse la clave simétrica. La por lo menos una aplicación de

acceso remoto por testigo TRA 215 recibe y desencripta 275d el criptograma [KSt]Kpub 290t mediante la clave privada complementaria Kpri 230 que restaura la clave simétrica compartida del testigo KSt 285t.

Con referencia a la figura 2E, la clave simétrica compartida del testigo KSt 285t se asigna al canal de comunicaciones dedicado Wc 220w que establece la conexión de comunicaciones de extremo a extremo segura 200. Las claves simétricas compartidas KSt 285t, KSc 285c se utilizan como claves de encriptación de bloques durante el intercambio de información a través de la conexión de comunicaciones de extremo a extremo segura. El establecimiento de la conexión de comunicaciones de extremo a extremo segura 200 determina la cumplimentación de un primer elemento de la tabla de estados de autenticación 240 del testigo. El canal de comunicaciones dedicado restringe la conexión de comunicaciones de extremo a extremo segura a una única conexión de comunicaciones inalámbricas segura 200 con el testigo de seguridad para prevenir la interceptación por entidades no autorizadas de subsiguientes transacciones del testigo de seguridad.

Con referencia a la figura 2F, en la última transacción de seguridad que se realiza, se solicita al usuario 206r, a través de la pantalla 20r asociada al dispositivo inteligente remoto IRD 110, que facilite su parámetro crítico de seguridad CSPu 235u. El parámetro crítico de seguridad del usuario CSPu 235u se introduce 295 en el dispositivo inteligente remoto IRD 110 por medio de la interfaz de usuario UI 85 y se encamina hacia el testigo de seguridad ST 75 para la autenticación.

La aplicación de acceso remoto por testigo TRA 215 compara 227 el parámetro crítico de seguridad del usuario CSPu 235 con el parámetro crítico de seguridad de referencia CSPr 235r. Si se halla una coincidencia entre el parámetro crítico de seguridad del usuario CSPu 235 y el parámetro crítico de seguridad de referencia CSPr 235r, se cumplimenta el elemento del parámetro crítico de seguridad CSP 245 de la tabla de estados de autenticación del testigo. Si el parámetro crítico de seguridad no supera la segunda transacción de autenticación, el procesamiento termina, y es necesario realizar un nuevo intento de establecimiento de la conexión de comunicaciones de extremo a extremo segura.

Con referencia a la figura 2G, se ilustra la fase final de la implementación de la presente invención, en la que se transmite una señal de resultado afirmativo 299t desde el testigo de seguridad ST 75 hasta el sistema informático activado por testigo de seguridad, por medio de la conexión de comunicaciones de extremo a extremo segura 200. La recepción de la señal de resultado afirmativo 299c determina la cumplimentación del segundo elemento ST 265 de la tabla de estados de autenticación del sistema informático, que permite el acceso 250t, 250c al recurso o los recursos seguros 255t, 255c asociados al testigo de seguridad ST 75, el sistema informático activado por testigo de seguridad CS 105 o a ambos dispositivos.

La pantalla del usuario DI 20r asociada al dispositivo inteligente remoto IRD 110 facilita opcionalmente por lo menos una indicación visual 208r que comunica que una sesión de mensajería segura está en curso. Del mismo modo, la pantalla del usuario DI 20c asociada al sistema informático activado por testigo de seguridad CS 105 presenta por lo menos una indicación visual 207c en la que se comunica que se ha concedido permiso de acceso remotamente. Se prevén también otros tipos de respuesta de retorno visual, auditiva y vibratoria.

Con referencia a la figura 3, se ilustran las etapas de implementación principales de la presente invención. El proceso se inicia 300 mediante el establecimiento de una conexión de comunicaciones inalámbricas entre un sistema informático activado por testigo de seguridad y un dispositivo inteligente remoto que presenta un testigo de seguridad acoplado funcionalmente. Se envía una clave pública desde el testigo de seguridad hasta el sistema informático activado por testigo de seguridad 310 por medio del dispositivo inteligente remoto, preferentemente como parte de un certificado digital en formato X.509. La transferencia de la clave pública puede realizarse automáticamente durante la conformación de conexión de las comunicaciones o mediante la interacción del usuario.

El sistema informático activado por testigo de seguridad autentica 315 el testigo de seguridad mediante un protocolo de desafío/respuesta, gracias al cual se genera un desafío, se encripta mediante la clave pública recibida y finalmente se transmite al testigo de seguridad a través de la conexión de comunicaciones inalámbricas. El testigo de seguridad recibe el criptograma y desencripta el desafío mediante la parte complementaria de la clave privada de la clave pública. El desafío en texto no encriptado se devuelve entonces al sistema informático activado por testigo de seguridad para la autenticación. Si el testigo de seguridad no se autentica 320, el procesamiento termina 370. Si el testigo de seguridad se autentica 320, se genera un conjunto de claves simétricas en el sistema informático activado por testigo de seguridad 325 y se realiza un intercambio de claves seguro 330 con el testigo de seguridad, mediante el cual por lo menos una de las claves simétricas se encripta con la clave pública y se envía al testigo de seguridad a través de la conexión de comunicaciones inalámbricas.

La clave simétrica encriptada recibida se desencripta mediante la clave privada y se asigna a un canal de comunicaciones dedicado, y el canal de comunicaciones dedicado se bloquea si no se sobrepasa un límite predeterminado de conexiones de comunicaciones inalámbricas preexistente 335. Si se sobrepasa el límite predeterminado 345, el procesamiento termina 375. El límite predeterminado habitualmente se establece en 1 en la forma de realización preferida de la presente invención.

El testigo de seguridad, el sistema informático activado por testigo de seguridad o ambos establecen un primer estado de seguridad que indica que se ha establecido un canal de comunicaciones seguro. En una forma de realización de la presente invención, el canal de comunicaciones seguro no se habilita hasta que el usuario se autentica tal como se describe a continuación.

Si no se sobrepasa el límite predeterminado 345, se solicita 350 al usuario que facilite su parámetro crítico de seguridad al dispositivo inteligente remoto. Entonces, el testigo de seguridad autentica 355 el parámetro crítico de seguridad facilitado comparando el parámetro crítico de seguridad de referencia con el parámetro crítico de seguridad recibido. Si el usuario no se autentica 360, el procesamiento termina. Si el usuario se autentica 355, el testigo de seguridad genera una señal de resultado afirmativo que se envía al sistema informático activado por testigo de seguridad 365. La recepción de la señal de resultado afirmativo permite el acceso a uno o más recursos seguros 370. El procesamiento termina 375 normalmente cuando el usuario termina la sesión de comunicaciones segura, cuando se extrae el testigo de seguridad del dispositivo inteligente remoto o cuando se sale del alcance de proximidad predeterminado del sistema informático activado por testigo de seguridad.

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, es posible realizar variantes y formas de realización diferentes, no pretendiéndose limitar el alcance de la presente invención conforme a la descripción detallada facilitada, sino con las reivindicaciones adjuntas.

REIVINDICACIONES

1. Procedimiento para establecer una conexión de comunicaciones de extremo a extremo segura entre un sistema informático activado por testigo de seguridad (105) y un testigo de seguridad (75) asociado a un dispositivo inteligente inalámbrico remoto (110), que comprende las etapas siguientes:

a. realizar una primera transacción de seguridad que autentica dicho testigo de seguridad (75) ante dicho sistema informático activado por testigo de seguridad (105),

b. establecer una conexión de comunicaciones segura entre dicho testigo de seguridad (75) y dicho sistema informático activado por testigo de seguridad (105) que incorpora un conjunto de claves simétricas compartidas (285t, 285s) generado durante dicha primera transacción de seguridad,

c. asignar por lo menos una clave (285t) de dicho conjunto de claves simétricas compartidas (285t, 285s) a un canal de comunicaciones dedicado (220w) entre el sistema informático activado por testigo de seguridad (105) y el testigo de seguridad (75), accesible para dicho testigo de seguridad (751), y

d. establecer por lo menos un primer estado de seguridad que indica que el canal de comunicaciones dedicado seguro (220) se ha establecido,

e. realizar una segunda transacción de seguridad tras dicha primera transacción de seguridad, que autentica a un usuario ante dicho testigo de seguridad (75) facilitando un parámetro crítico de seguridad (235) a dicho testigo de seguridad por medio de dicho dispositivo inteligente remoto (110),

f. transmitir una señal de resultado afirmativo desde el testigo de seguridad (75) hasta el sistema informático activado por testigo de seguridad (105) por medio de la conexión de comunicaciones de extremo a extremo segura si el usuario es autenticado, y establecer por lo menos un segundo estado de seguridad que indica que el testigo de seguridad (75) ha autenticado al usuario, y

g. activar el uso de dicha conexión de comunicaciones segura tras el establecimiento de dicho por lo menos un segundo estado de seguridad.

2. Procedimiento según la reivindicación 1, en el que dicha conexión de comunicaciones segura es anónima para dicho testigo de seguridad (75), pero es controlada por el mismo.

3. Procedimiento según la reivindicación 1, en el que dicha primera transacción de seguridad comprende un protocolo de desafío/respuesta que incorpora un par de claves asimétricas.

4. Procedimiento según la reivindicación 1, que incluye además la etapa de señalar, mediante dicho testigo de seguridad (75), a dicho sistema informático activado por testigo de seguridad (105) si dicha segunda transacción de seguridad se realiza con éxito.

5. Procedimiento según la reivindicación 1, en el que dicha conexión de comunicaciones segura se establece, por lo menos en parte, a través de una conexión de telecomunicaciones inalámbricas.

6. Procedimiento según la reivindicación 1, que incluye además la etapa que consiste en permitir el acceso del usuario a uno o más recursos tras la realización con éxito de dicha segunda transacción de seguridad.

7. Procedimiento según la reivindicación 1, en el que la etapa 1b incluye además las etapas siguientes:

1b.1 generar, mediante dicho sistema informático activado por testigo de seguridad (105), dicho conjunto de claves simétricas compartidas (285t. 285s),

1b.2 encriptar dicha por lo menos una clave (285t) con una clave pública (225c) asociada a dicho testigo de seguridad (75),

1b.3 enviar dicha por lo menos una clave encriptada (285t) a dicho testigo de seguridad (75), y

1b.4 desencriptar dicha por lo menos una clave (285t) con una clave privada (230) asociada a dicho testigo de seguridad (75).

8. Procedimiento según la reivindicación 1, en el que dicho canal de comunicaciones dedicado (220w) impide que el número de conexiones de comunicaciones inalámbricas seguras concurrentes con dicho testigo de seguridad (75) sobrepase un límite predeterminado.

9. Procedimiento según la reivindicación 8, en el que dicho límite predeterminado es 1.

10. Procedimiento según la reivindicación 6, en el que dicha conexión de comunicaciones segura solo está disponible cuando dicho testigo de seguridad (75) se halla dentro del alcance predefinido de dicho sistema informático activado por testigo de seguridad (105).

11. Procedimiento según la reivindicación 1, que comprende además la etapa que consiste en establecer una conexión de comunicaciones inalámbricas entre dicho dispositivo inteligente remoto (110) y dicho sistema informático activado por testigo de seguridad (105).

12. Procedimiento según la reivindicación 11, que incluye además la etapa que consiste en permitir el acceso de dicho usuario, a uno o más recursos seguros (255t, 255c) tras la realización con éxito de dicha segunda transacción de seguridad.

13. Procedimiento según la reivindicación 11, en el que la etapa e incluye además la etapa e1 que invita a dicho usuario a proporcionar dicho parámetro crítico de seguridad (235).

14. Procedimiento según la reivindicación 11, que incluye además la etapa de envío de un certificado digital a dicho sistema informático activado por testigo de seguridad (105).

15. Procedimiento según la reivindicación 11, que incluye además la etapa que consiste en invitar a dicho usuario a seleccionar una transacción de autenticación local o remota.

16. Procedimiento según la reivindicación 11, que incluye además la etapa que consiste en proporcionar a dicho usuario una respuesta de retorno sensorial (205c) desde por lo menos dicho sistema informático activado por testigo de seguridad (105), que indica que una transacción de autenticación remota está en curso.

17. Procedimiento según la reivindicación 11, en el que dicha conexión de comunicaciones inalámbricas seguras está asociada a un canal de comunicaciones dedicado (220w) que impide que se establezcan conexiones de comunicaciones inalámbricas seguras con dicho testigo de seguridad (75).

18. Procedimiento según la reivindicación 16, en el que dicha respuesta de retorno sensorial (205c) incluye una respuesta de retorno visual, táctil, auditiva o vibratoria.

19. Procedimiento según la reivindicación 11, en el que dicha conexión de comunicaciones inalámbricas segura solo está disponible cuando dicho testigo de seguridad (75) se halla dentro de un alcance predefinido de dicho sistema informático activado por testigo de seguridad (105).

20. Sistema para establecer una conexión de comunicaciones de extremo a extremo segura entre un sistema informático activado por testigo de seguridad (105) y un testigo de seguridad (75) asociado a un dispositivo inteligente inalámbrico y remoto (110), que comprende:

dicho sistema informático activado por testigo de seguridad (105), que incluye:

unos primeros medios de transacción de seguridad para por lo menos autenticar dicho testigo de seguridad (75) ante dicho sistema informático activado por testigo de seguridad (105);

unos primeros medios de conexión de comunicaciones seguras para establecer por lo menos una conexión de comunicaciones segura entre dicho sistema informático activado por testigo de seguridad (105) y dicho testigo de seguridad (75);

en el que

dicho dispositivo inteligente remoto (110) incluye:

unos medios de interfaz de testigo de seguridad (70r) para acoplar por lo menos funcionalmente dicho testigo de seguridad (75) a dicho dispositivo inteligente remoto (110);

unos medios de interfaz de usuario (85r) para por lo menos recibir y encaminar un parámetro crítico de seguridad (235) proporcionado por dicho usuario hacia dichos medios de interfaz de testigo de seguridad (70r);

dicho testigo de seguridad (75) incluye:

unos segundos medios de conexión de comunicaciones seguras para establecer por lo menos dicha conexión de comunicaciones segura junto con dichos primeros medios de conexión de comunicaciones seguras;

unos medios de canal de comunicaciones dedicado (220w) para impedir el establecimiento de una conexión de comunicaciones segura concurrente con dicho testigo de seguridad (75); y

unos segundos medios de transacción de seguridad para por lo menos autenticar dicho usuario ante dicho testigo de seguridad (75), después de dicha primera transacción de seguridad, mediante por lo menos dicho parámetro crítico de seguridad (235);

en el que el sistema comprende unos medios para activar dichos medios de interfaz de usuario (85r) para recibir y encaminar dicho parámetro crítico de seguridad (235), una vez que dichos primeros medios de conexión de comunicaciones seguras han establecido dicha conexión de comunicaciones segura;

y en el que el sistema comprende unos medios para transmitir una señal de resultado afirmativo desde el testigo de seguridad (75) hasta el sistema informático activado por testigo de seguridad (105), por medio de la conexión de comunicaciones de extremo a extremo segura, si el usuario es autenticado.

21. Sistema según la reivindicación 20, en el que dicho sistema informático activado por testigo de seguridad (105) establece comunicaciones inalámbricas con dicho dispositivo inteligente remoto (110) y dicho testigo de seguridad (75) acoplado funcionalmente.

22. Sistema según la reivindicación 20, en el que dichos primeros medios de transacción de seguridad incluyen unos medios de protocolo de desafío/respuesta y unos medios de criptografía asimétrica.

23. Sistema según la reivindicación 20, en el que dichos primeros medios de conexión de comunicaciones seguras incluyen unos medios de generación de conjunto de claves simétricas y unos medios de intercambio de claves simétricas seguros.

24. Sistema según la reivindicación 20, en el que los medios de interfaz de testigo de seguridad (70r) incluyen unos medios de comunicaciones de testigo de seguridad y unos medios de transferencia de potencia electromagnética.

25. Sistema según la reivindicación 20, en el que dichos medios de canal de comunicaciones dedicado (220w) incluyen unos medios de identificación de canal exclusivo que son accesibles para dicho sistema informático activado por testigo de seguridad (105).

26. Sistema según la reivindicación 20, en el que la ejecución satisfactoria de dichos primeros medios de transacción de seguridad establece un primer estado de seguridad de sistema informático asociado a dicho cliente activado por el testigo de seguridad (75).

27. Sistema según la reivindicación 20, en el que el establecimiento de dicha conexión de comunicaciones segura establece un primer estado de seguridad de testigo asociado a dicho testigo de seguridad (75).

28. Sistema según la reivindicación 20, en el que la ejecución satisfactoria de dichos segundos medios de transacción de seguridad establece un segundo estado de seguridad de testigo (75) asociado a dicho testigo de seguridad (75).

29. Sistema según la reivindicación 20, en el que dicho sistema informático activado por testigo de seguridad (105) incluye además unos medios de detección de proximidad (115c).

30. Sistema según la reivindicación 20, en el que

dicho sistema informático activado por testigo de seguridad (105) incluye:

un primer procesador (5c);

una primera memoria (10c) acoplada a dicho primer procesador (5c);

por lo menos una aplicación de autenticación remota almacenada funcionalmente en una primera parte de dicha primera memoria, que presenta instrucciones lógicas ejecutables por dicho primer procesador (5c) para:

realizar dicha autenticación de dicho testigo de seguridad (75);

establecer dicha conexión de comunicaciones segura con dicho testigo de seguridad (75);

dicho dispositivo inteligente remoto (110) incluye:

un segundo procesador (5r);

una segunda memoria (10r) acoplada a dicho segundo procesador (5r);
una interfaz de testigo de seguridad (70r) acoplada a dicho segundo procesador (5r);

una interfaz de usuario (85r) acoplada a dicho segundo procesador (5r); y

por lo menos una aplicación de interfaz de dispositivo remoto almacenada funcionalmente en una parte de dicha segunda memoria (10r), que presenta instrucciones lógicas ejecutables por dicho segundo procesador (5r) para:

emular una interfaz de dispositivo de testigo de seguridad acoplada localmente por lo menos a dicho sistema informático activado por testigo de seguridad (105); y

recibir y encaminar condicionalmente dicho parámetro crítico de seguridad (235) proporcionado por dicho usuario, por medio de dicha interfaz de usuario (85r), a dicho testigo de seguridad (75); y

dicho testigo de seguridad (75) incluye:

por lo menos un tercer procesador (5t);

una tercera memoria acoplada a dicho por lo menos un tercer procesador (5t);

una interfaz de comunicaciones y potencia electromagnética acoplada a dicho por lo menos un tercer procesador (5t) y a dicha interfaz de testigo de seguridad (70r);

por lo menos una aplicación de autenticación remota por testigo almacenada funcionalmente en una segunda parte de dicha tercera memoria, que presenta instrucciones lógicas ejecutables por dicho por lo menos un tercer procesador (5t) para:

establecer dicha conexión de comunicaciones segura con dicho sistema informático activado por testigo de seguridad (105);

restringir dicha conexión de comunicaciones segura a un único canal de comunicaciones inalámbricas; y

realizar dicha autenticación de dicho usuario basándose por lo menos en parte en dicho parámetro de seguridad crítico (235).

31. Sistema según la reivindicación 30, que incluye además un primer transceptor inalámbrico (60c) acoplado funcionalmente a dicho primer procesador (5c) que establece comunicaciones de procesamiento con un segundo transceptor inalámbrico (60r) acoplado funcionalmente a dicho segundo procesador (5r).

32. Sistema según la reivindicación 30, que incluye además una clave pública (225c) asociada a dicho testigo de seguridad (75) almacenada de manera recuperable en una segunda parte de dicha primera memoria (10c), y una clave privada (230) almacenada de manera recuperable en una segunda parte de dicha tercera memoria, siendo dicha clave privada (230) parte complementaria de dicha clave pública (225c).

33. Sistema según la reivindicación 30, que incluye además un parámetro crítico de seguridad de referencia (235r) almacenado de manera recuperable en una tercera parte de dicha tercera memoria.

34. Sistema según la reivindicación 32, en el que dichas claves pública (225c) y privada (230) están incorporadas en dicho protocolo de desafío/respuesta utilizado para autenticar dicho testigo de seguridad (75) ante dicho sistema informático activado por testigo de seguridad (105).

35. Sistema según la reivindicación 34, en el que dicha por lo menos una aplicación de autenticación remota incluye además instrucciones lógicas ejecutables por dicho primer procesador (5c) para generar dicho conjunto de claves simétricas (285t, 285s) y realizar un intercambio de claves seguro con dicho testigo de seguridad (75).

36. Sistema según la reivindicación 35, en el que dicho intercambio de claves seguro se realiza utilizando dichas claves pública (225c) y privada (230).

37. Sistema según la reivindicación 35, en el que dicho conjunto de claves simétricas (285t, 285s) está incorporado en dicha conexión de comunicaciones de extremo a extremo segura.

38. Sistema según la reivindicación 30, en el que dicha por lo menos una aplicación de autenticación por testigo remota autentica a dicho usuario comparando dicho parámetro crítico de seguridad proporcionado (235) con dicho parámetro crítico de seguridad de referencia (235r).

39. Sistema según la reivindicación 30, en el que dicha por lo menos una aplicación de autenticación por testigo remota restringe la utilización de dicha conexión de comunicaciones de extremo a extremo segura hasta que dicho usuario sea autenticado.

40. Sistema según la reivindicación 30, en el que dicha conexión de comunicaciones de extremo a extremo segura se restringe a una única conexión inalámbrica con dicho testigo de seguridad (75) utilizando un canal de comunicaciones dedicado (220w) controlado por dicha por lo menos una aplicación de autenticación por testigo remota.

41. Sistema según la reivindicación 36, en el que dicho canal de comunicaciones dedicado (220w) incluye un identificador exclusivo disponible para dicho sistema informático activado por testigo de seguridad (105).

42. Sistema según la reivindicación 30, en el que dicha interfaz de comunicaciones y potencia electromagnética incluye unos medios inductivos, unos medios capacitivos o unos medios de contacto eléctrico.

43. Producto de programa informático realizado en una forma tangible y legible por un procesador de testigo de seguridad (5t), en el que dicho producto de programa informático incluye instrucciones ejecutables almacenadas para implementar el procedimiento según la reivindicación 1.

44. Producto de programa informático según la reivindicación 43, en el que dicha forma tangible incluye unos medios magnéticos, unos medios ópticos o unos medios lógicos.

45. Producto de programa informático según la reivindicación 43, en el que dichas instrucciones ejecutables se almacenan en un formato de código que comprende el código de octetos, el código compilado, el código interpretado, el código compilable y el código interpretable.

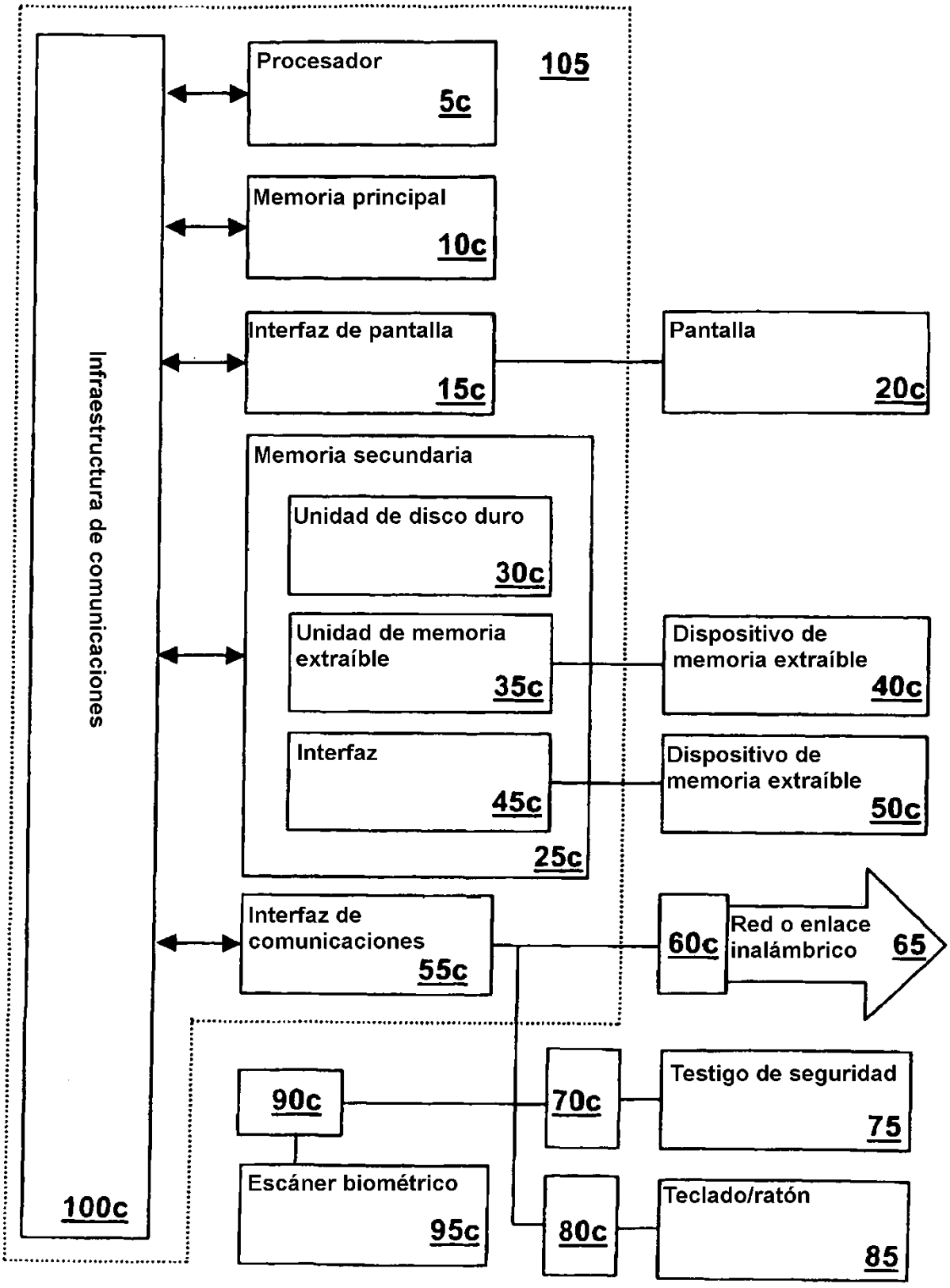
Procesador
5c
105
Memoria principal
10c
Interfaz de pantalla
15c
Pantalla
20c
Infraestructura de comunicaciones
Memoria secundaria
Unidad de disco duro
30c
Unidad de memoria extraíble
35c
Dispositivo de memoria extraíble
40c
Interfaz
45c
Dispositivo de memoria extraíble
50c
25c
Interfaz de comunicaciones
55c
60c
Red o enlace inalámbrico
65
90c
70c
Testigo de seguridad
75
Escáner biométrico
95c
80c
Teclado/ratón
85
100c

FIG. 1

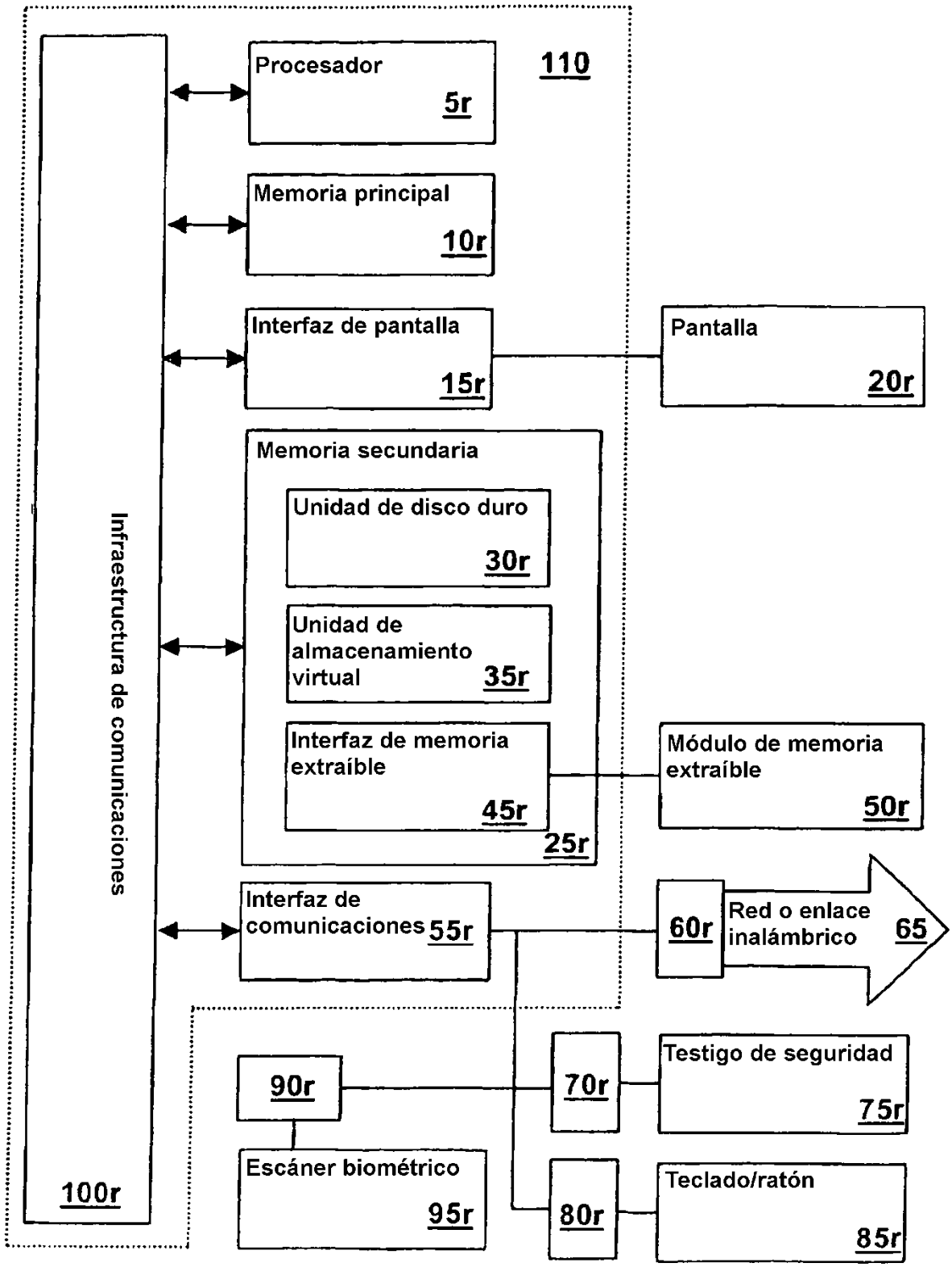
Procesador
5r
110
Memoria principal
10r
Interfaz de pantalla
15r
Pantalla
20r
Memoria secundaria
Unidad de disco duro
30r
Unidad de almacenamiento virtual
35r
Interfaz de memoria extraíble
45r
25r
Módulo de memoria extraíble
50r
Infraestructura de comunicaciones
Interfaz de comunicaciones
55r
60r
Red o enlace inalámbrico
65
90r
70r
Testigo de seguridad
75r
Escáner biométrico
95r
80r
Teclado/ratón
85r
100r

FIG. 1A

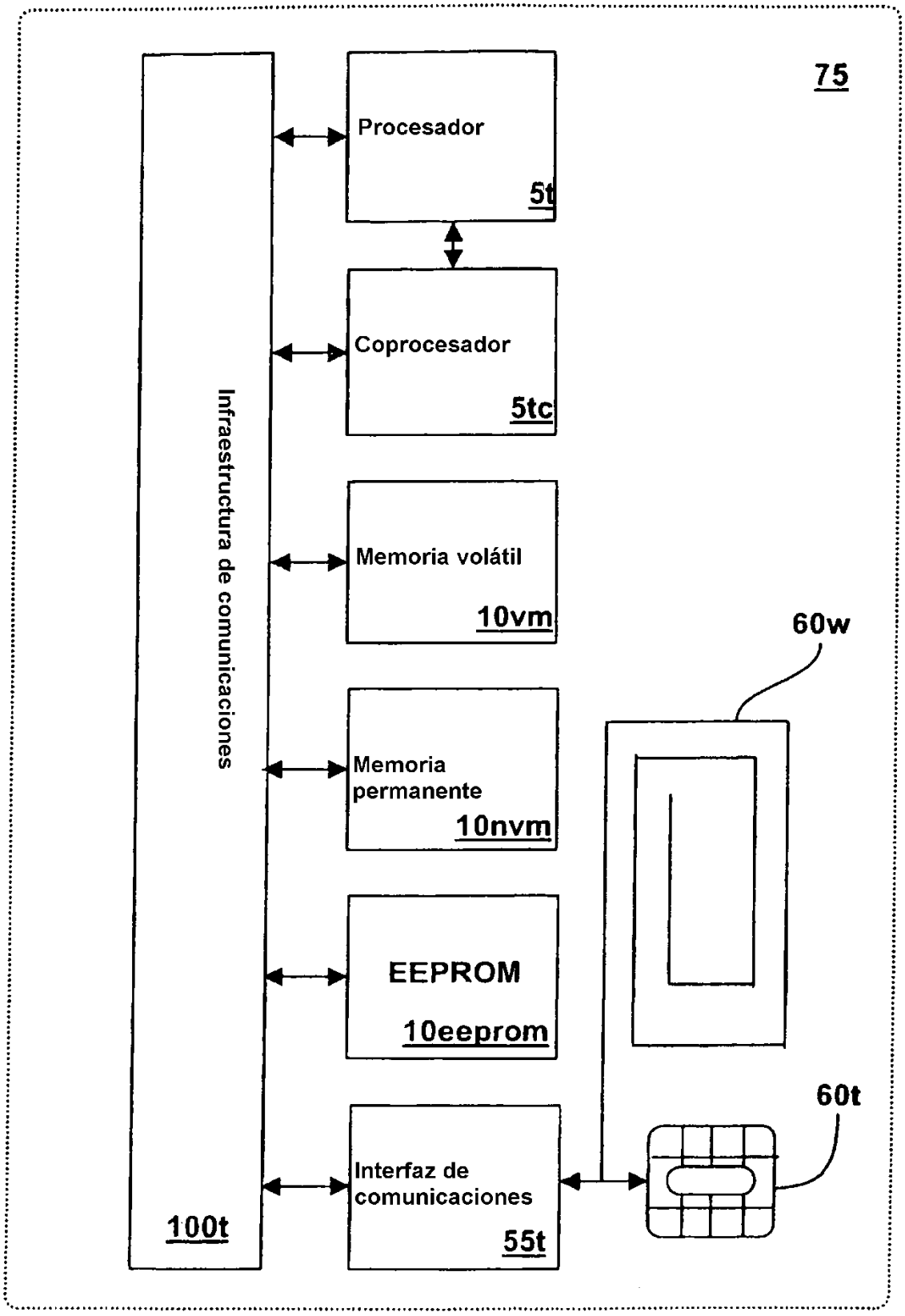
75
Procesador
5t
Coprocesador
5tc
Memoria volátil
10vm
Memoria permanente
10nvm
EEPROM
10eeprom
Interfaz de comunicaciones
55t
Infraestructura de comunicaciones
100t
60w
60t

FIG. 1B

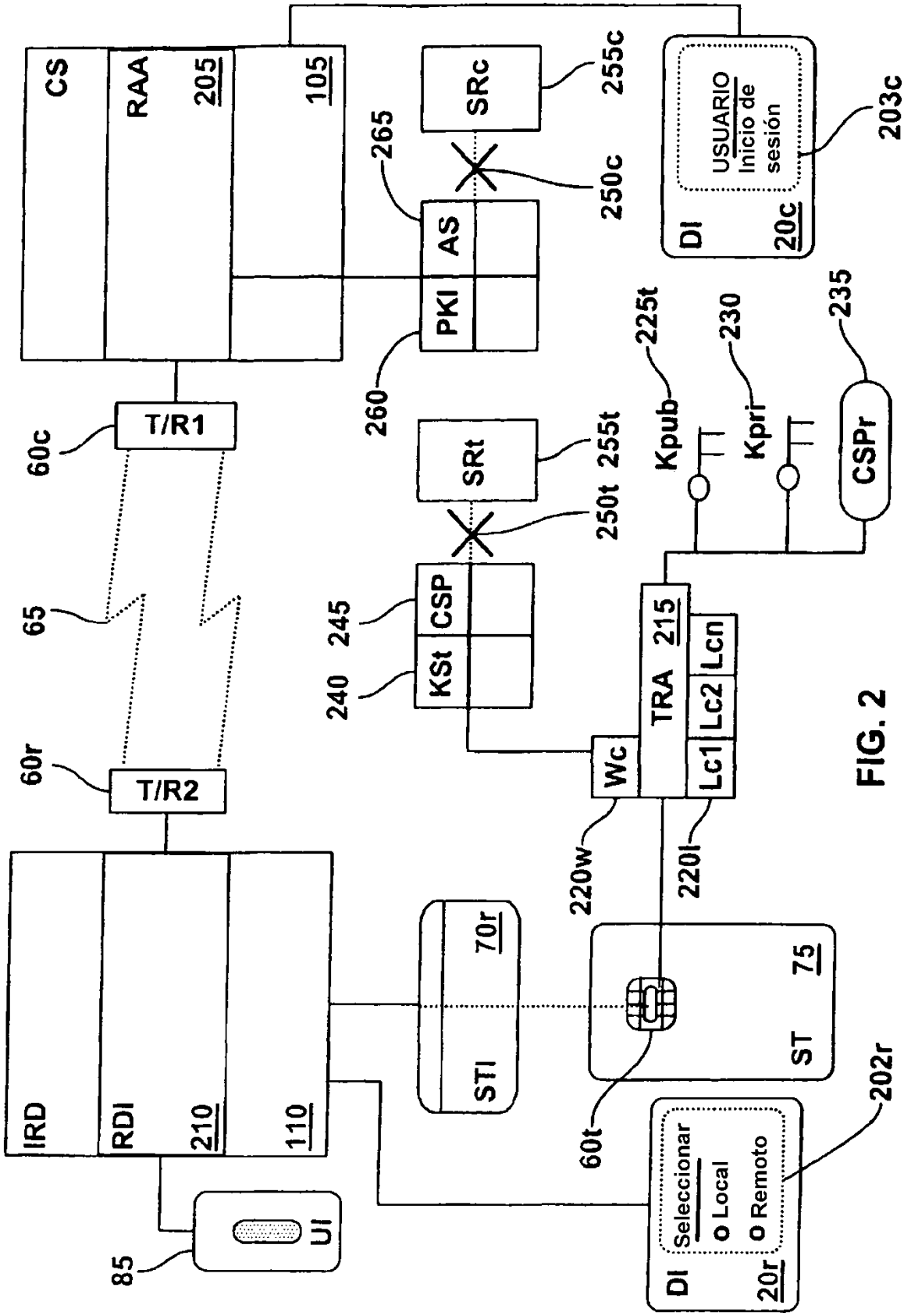
CS
RAA
205
105
SRc
255c
265
250c
AS
PKI
260
DI
USUARIO
Inicio de sesión
20c
203c
60c
T/R1
SRt
255t
250t
225t
Kpub
230
Kpri
235
CSPr
65
245
CSP
240
KSt
TRA
215
Lcn
Lc2
Lc1
Wc
60r
T/R2
220w
220l
IRD
RDI
210
110
70r
STI
75
ST
60t
202r
Seleccionar
Local
Remoto
20r
85
UI

FIG. 2

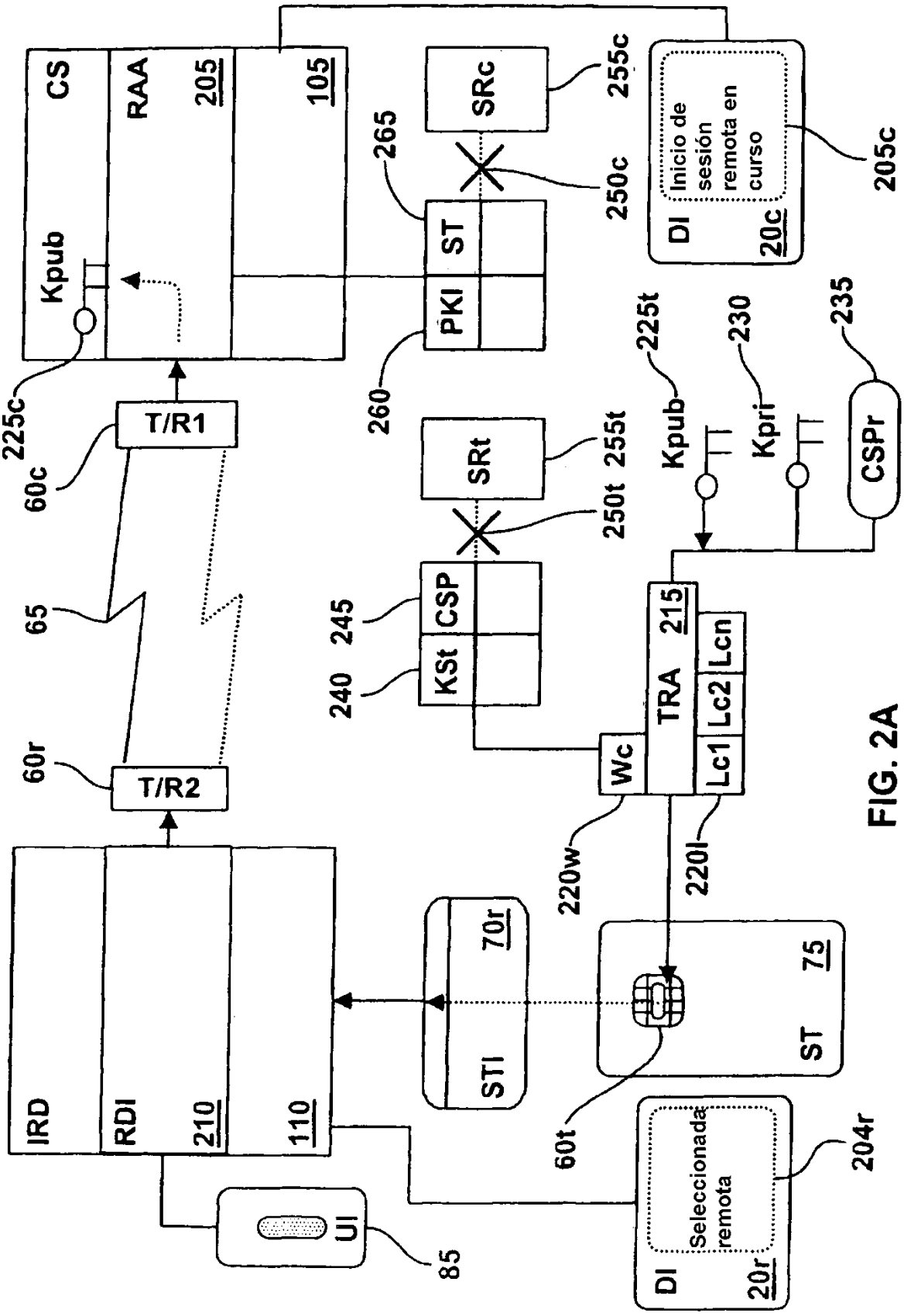
CS
RAA
205
105
Kpub
225c
60c
T/R1
65
60r
T/R2
IRD
RDI
210
110
UI
85
SRc
255c
250c
265
ST
PKI
260
Inicio de sesión remota en curso
DI
20c
205c
SRt
255t
250t
CSP
KSt
245
240
225t
Kpub
230
Kpri
235
CSPr
TRA
215
Lcn
Lc2
Lc1
Wc
220w
220l
70r
STI
75
ST
60t
Seleccionada remota
DI
20r
204r

FIG. 2A

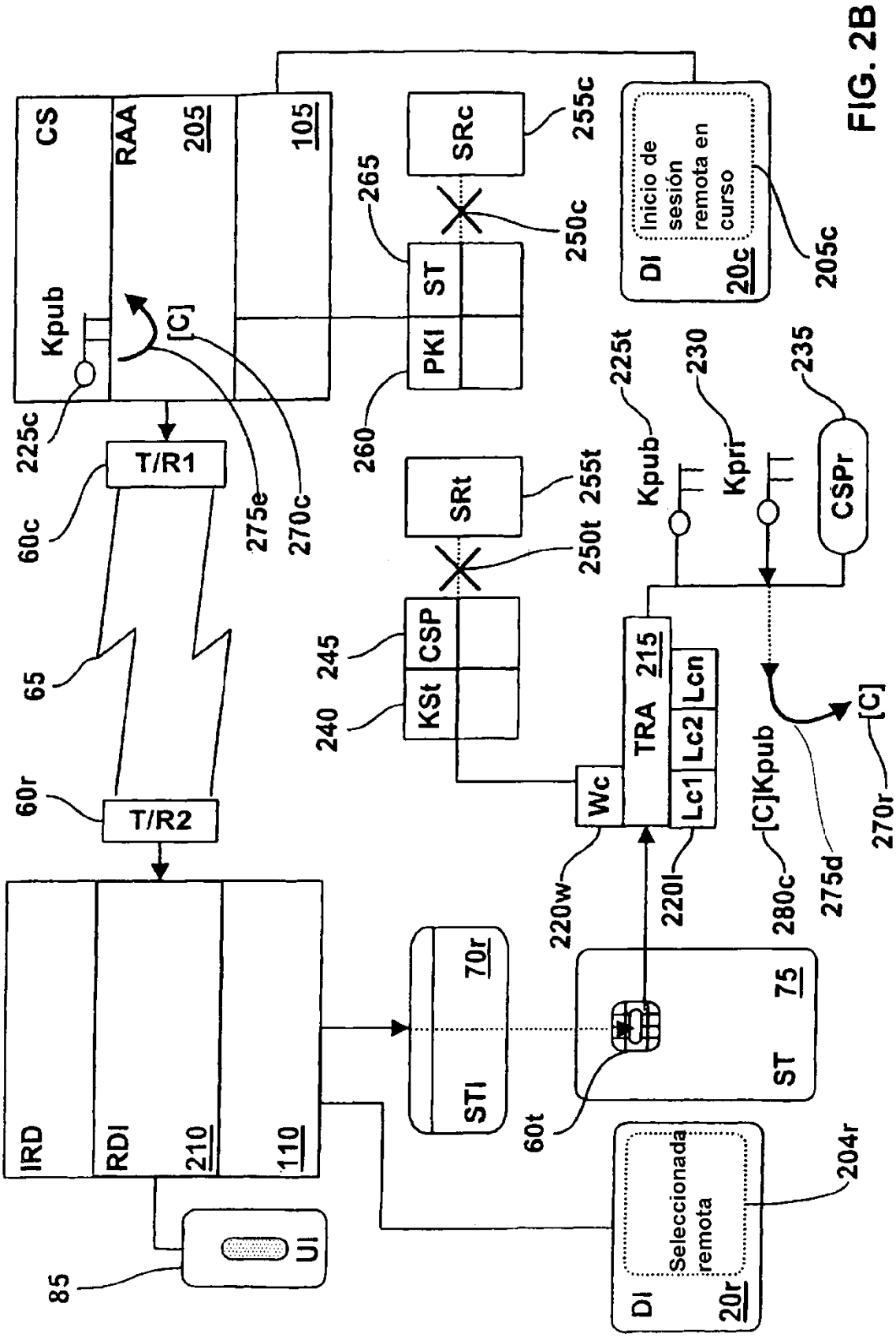
CS
RAA
205
105
Kpub
[C]
225c
T/R1
60c
65
60r
T/R2
275e
270c
265
ST
PKI
260
SRc
255c
250c
DI
Inicio de sesión remota en curso
20c
205c
SRt
255t
250t
240
245
KSt
CSP
225t
230
235
Kpub
Kpri
CSPr
TRA
215
Wc
Lc1
Lc2
Lcn
220w
220l
[C]Kpub
280c
275d
270r
[C]
IRD
RDI
210
110
70r
STl
60t
ST
75
204r
Seleccionada remota
DI
20r
UI
85

FIG. 2B

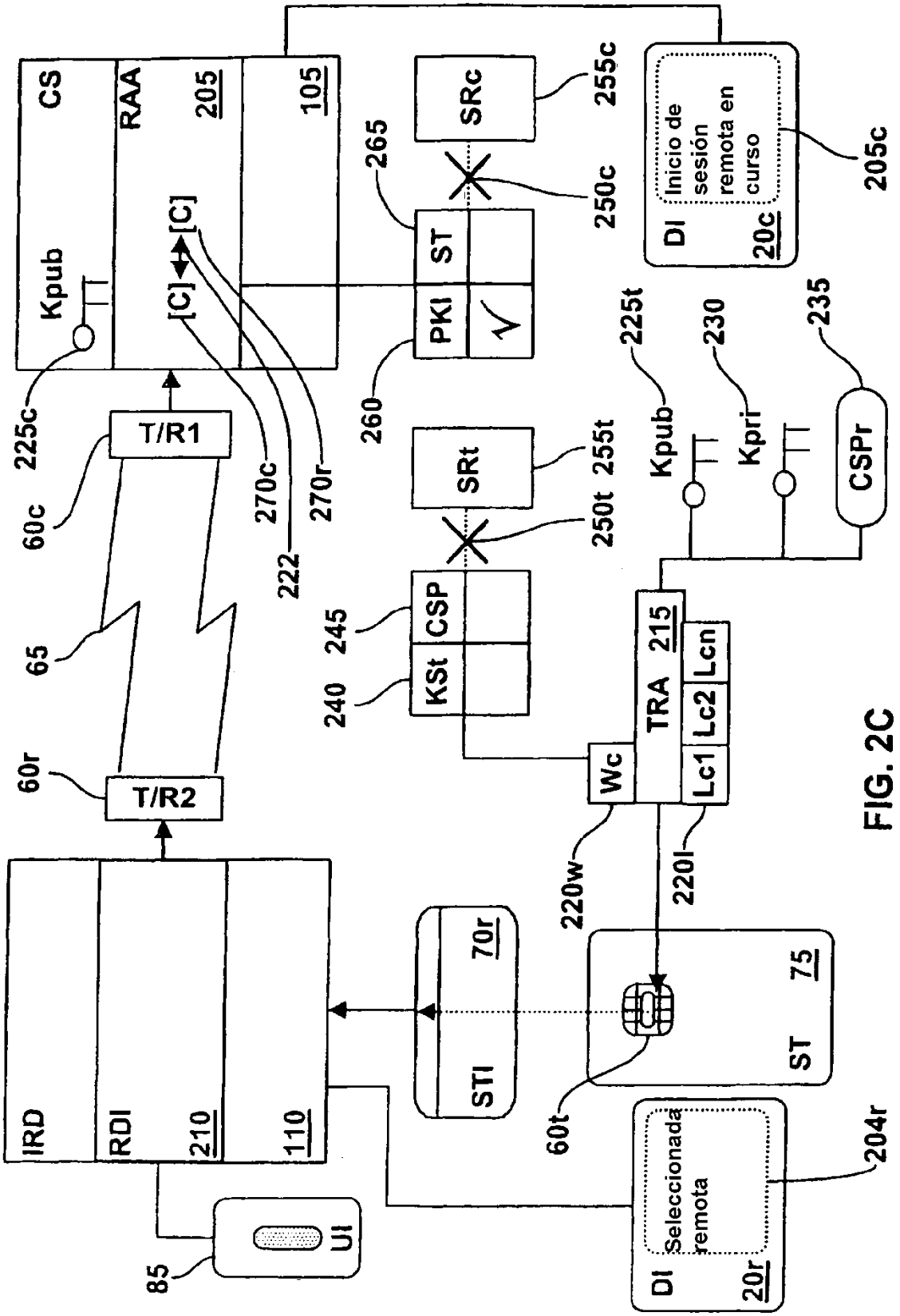
CS
RAA
205
105
Kpub
[C]
[C]
225c
60c
T/R1
65
60r
T/R2
IRD
RDI
210
110
85
UI
270c
270r
222
265
SRc
255c
250c
ST
PKI
260
SRt
255t
250t
CSP
KSt
245
240
Inicio de sesión remota en curso
DI
20c
205c
225t
Kpub
230
Kpri
235
CSPr
TRA
215
Wc
Lc1
Lc2
Lcn
220w
220l
70r
STI
75
ST
60t
Seleccionada remota
DI
20r
204r

FIG. 2C

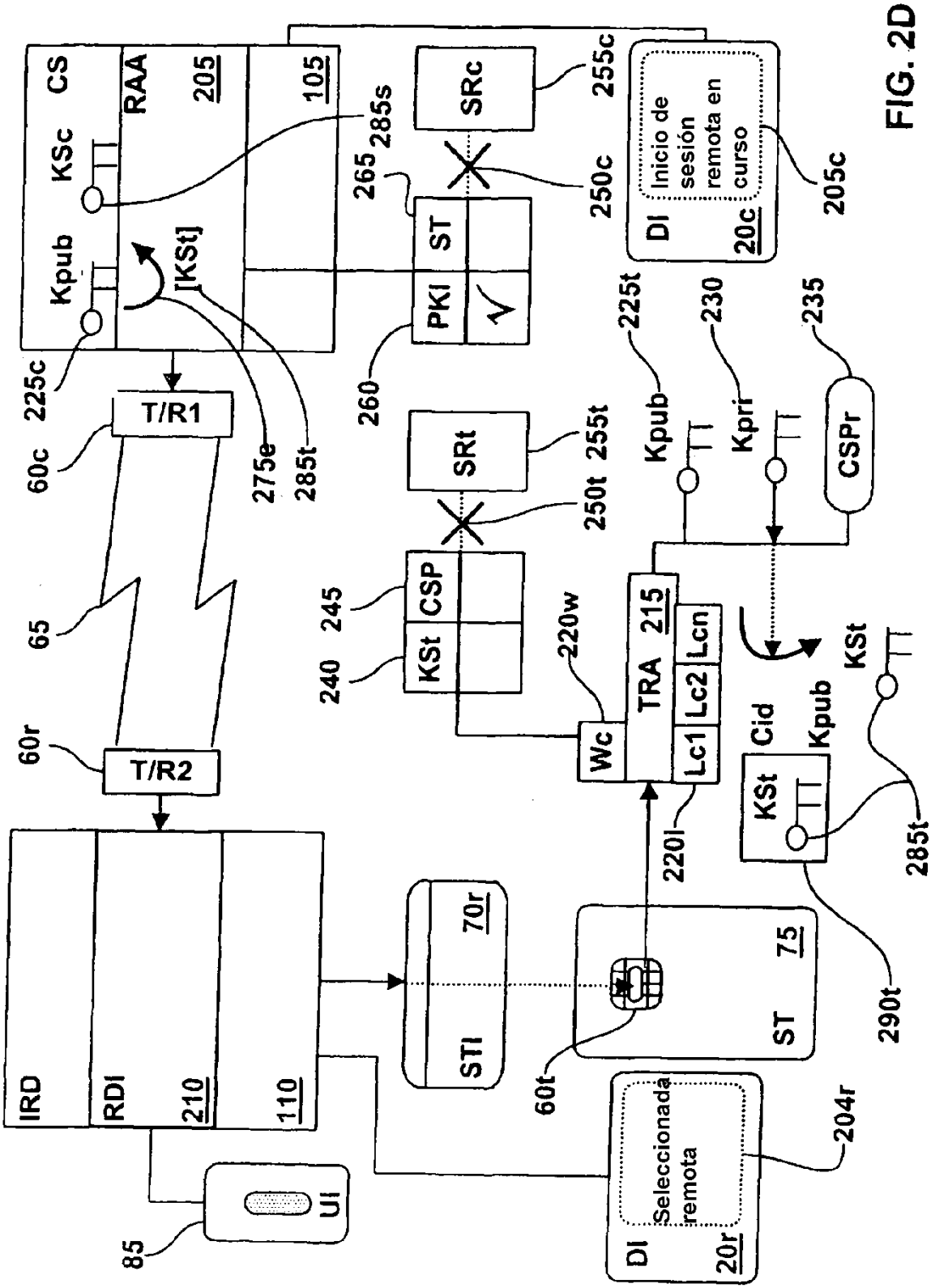
CS
KSc
RAA
205
105
Kpub
[KSt]
225c
60c
T/R1
275e
285t
285s
265
260
PKI
ST
SRc
255c
250c
DI
Inicio de sesión remota en curso
20c
205c
SRt
255t
250t
225t
230
235
Kpub
Kpri
CSPr
245
CSP
240
KSt
220w
Wc
TRA
215
Lcn
Lc2
Lc1
220l
Cid
Kpub
KSt
285t
290t
65
60r
T/R2
IRD
RDI
210
110
70r
STI
75
ST
60t
204r
Seleccionada remota
DI
20r
UI
85

FIG. 2D

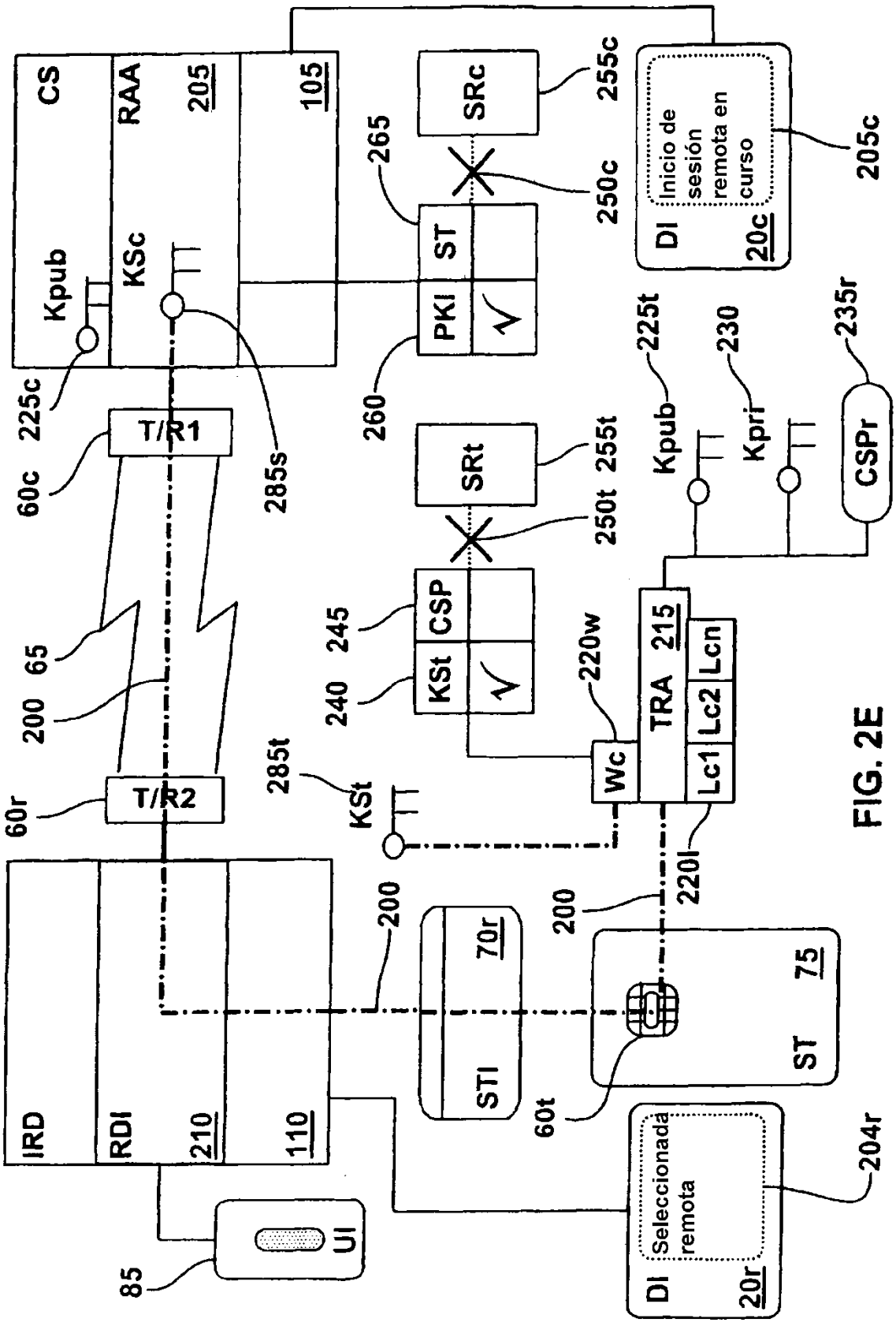
CS
RAA
205
105
Kpub
KSc
225c
60c
T/R1
285s
SRc
255c
250c
265
ST
PKI
260
DI
Inicio de sesión remota en curso
20c
205c
SRt
255t
250t
CSP
KSt
245
240
225t
230
235r
Kpub
Kpri
CSPr
220w
TRA 215
Wc
Lc1
Lc2
Lcn
220l
285t
KSt
60r
T/R2
65
200
IRD
RDI
210
110
70r
STI
60t
ST 75
DI
Seleccionada remota
20r
204r
UI
85

FIG. 2E

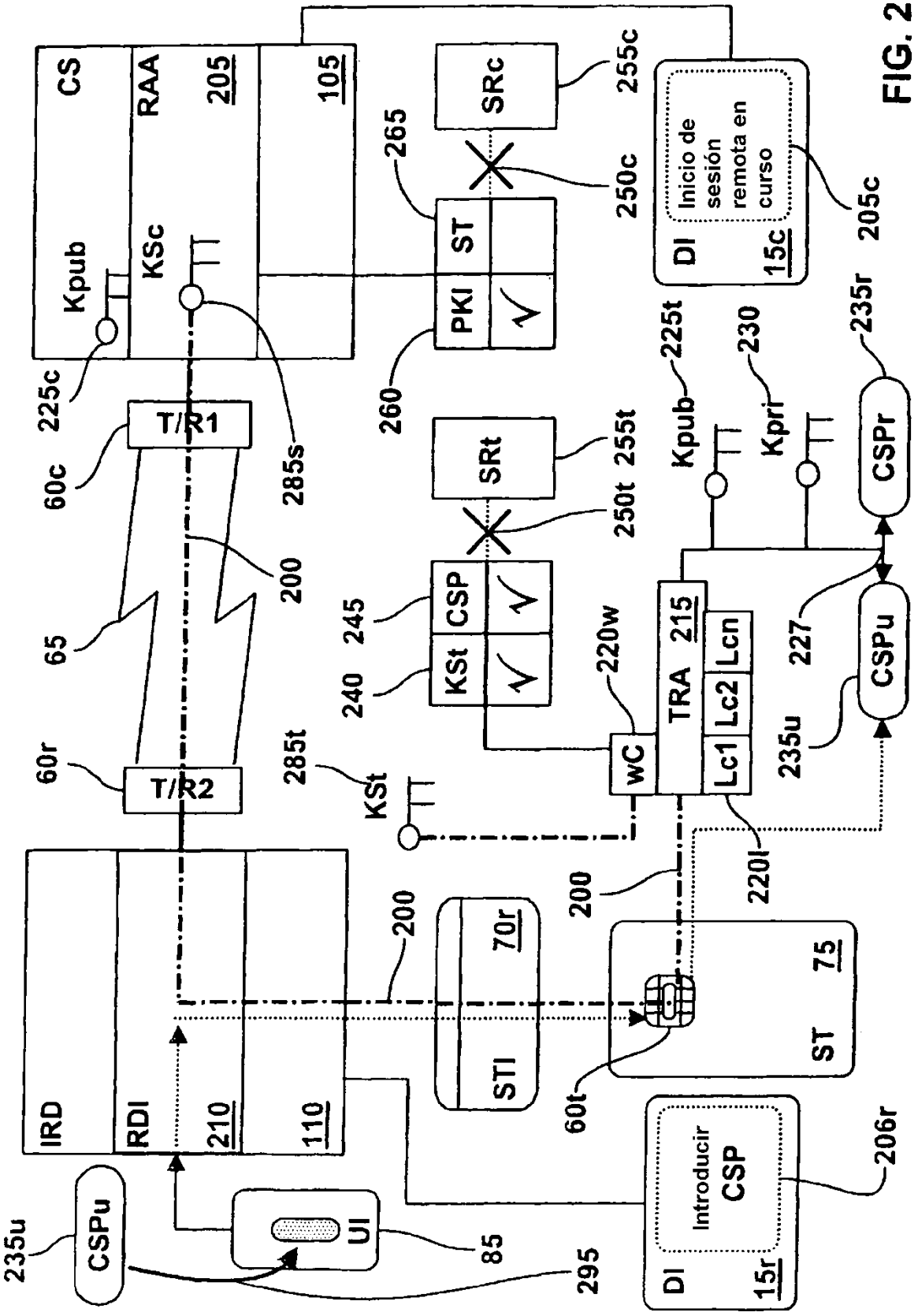
CS
RAA
205
105
Kpub
KSc
225c
60c
T/R1
285s
200
65
60r
T/R2
285t
KSt
IRD
RDI
210
110
200
70r
STI
200
60t
ST
75
220l
wC
TRA
215
Lc1
Lc2
Lcn
220w
CSP
KSt
245
240
SRt
255t
250t
PKI
ST
260
265
SRc
255c
250c
DI
Inicio de sesión remota en curso
15c
205c
Kpub
225t
Kpri
230
CSPr
235r
227
CSPu
235u
235u
CSPu
UI
85
295
DI
Introducir CSP
15r
206r

FIG. 2F

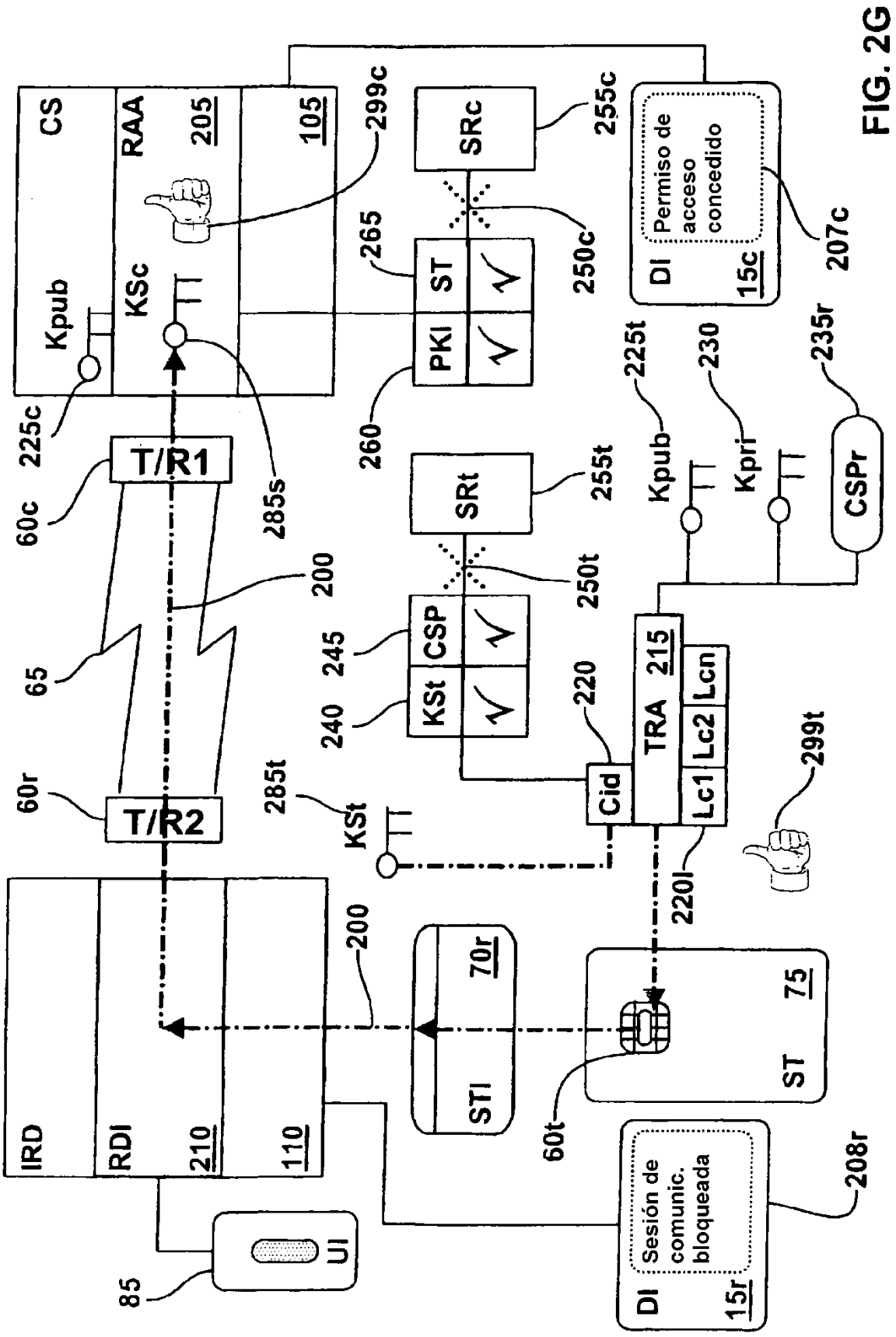
CS
RAA
205
105
Kpub
KSc
225c
299c
SRc
255c
265
ST
PKI
250c
260
DI
Permiso de acceso concedido
15c
207c
T/R1
60c
285s
SRt
255t
225t
230
235r
Kpub
Kpri
CSPr
200
65
CSP
KSt
245
240
250t
220
TRA
215
Cid
Lc1
Lc2
Lcn
T/R2
60r
285t
KSt
299t
220l
IRD
RDI
210
110
200
70r
STl
ST
75
60t
DI
Sesión de comunic. bloqueada
15r
208r
UI
85

FIG. 2G

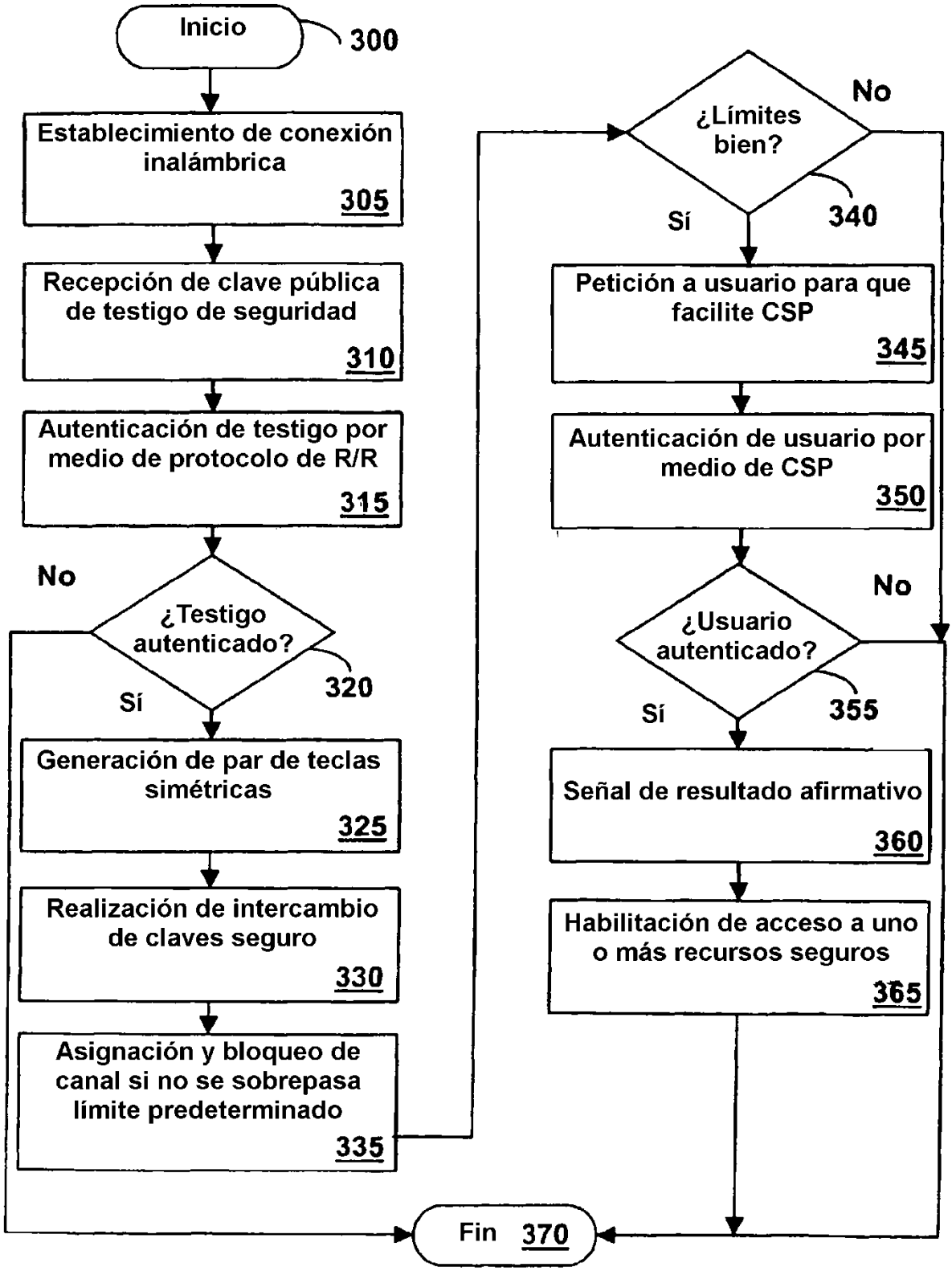
Inicio
300
Establecimiento de conexión inalámbrica
305
Recepción de clave pública de testigo de seguridad
310
Autenticación de testigo por medio de protocolo de R/R
315
No
¿Testigo autenticado?
320
Sí
Generación de par de teclas simétricas
325
Realización de intercambio de claves seguro
330
Asignación y bloqueo de canal si no se sobrepasa límite predeterminado
335
No
¿Límites bien?
340
Sí
Petición a usuario para que facilite CSP
345
Autenticación de usuario por medio de CSP
350
No
¿Usuario autenticado?
355
Sí
Señal de resultado afirmativo
360
Habilitación de acceso a uno o más recursos seguros
365
Fin 370

FIG. 3