(19) OFICINA ESPAÑOLA DE PATENTES Y MARCAS

ESPAÑA

(11) Número de publicación: **2 481 396**

(51) Int. CI.:

H04L 29/06 (2006.01)
G06F 21/31 (2013.01)
G06F 21/34 (2013.01)
G07F 7/10 (2006.01)

(12) TRADUCCIÓN DE PATENTE EUROPEA T3

(96) Fecha de presentación y número de la solicitud europea: **22.12.2004 E 04293088 (3)**

(97) Fecha y número de publicación de la concesión europea: **21.05.2014 EP 1549018**

(54) Título: **Dispositivo remoto para emular un dispositivo de seguridad local**

(30) Prioridad:

22.12.2003 US 740497

(45) Fecha de publicación y mención en BOPI de la traducción de la patente:
30.07.2014

(73) Titular/es:

ASSA ABLOY AB (100.0%)
Klarabergsviadukten 90
111 64 Stockholm, SE

(72) Inventor/es:

LE SAINT, ERIC F. y
FEDRONIC, DOMINIQUE LOUIS JOSEPH

(74) Agente/Representante:

CURELL AGUILÁ, Mireia

DESCRIPCIÓN

Dispositivo remoto para emular un dispositivo de seguridad local.

Campo de la invención

La presente invención se refiere en general a un método, un sistema y un producto de programa de ordenador para procesado de datos, y, más específicamente, a un dispositivo remoto inteligente equipado con un testigo de seguridad que se usa para emular, con fines relacionados con la autenticación, un dispositivo periférico local de testigo de seguridad conectado a un sistema de ordenador anfitrión.

Antecedentes

El crecimiento brusco del uso de dispositivo y aparatos de red inteligentes portátiles ha creado una demanda de un despliegue de mecanismos de seguridad que saque provecho de la mayor flexibilidad de uso ofrecida por estos dispositivos. Un uso ideal para estos dispositivos es simplificar el acceso a uno o más sistemas de ordenador con los cuales puede ser necesaria la interacción por parte de un usuario. Por ejemplo, en un entorno informático empresarial, un usuario típico puede tener un sistema de ordenador que es usado en una posición de trabajo principal y un portátil que se usa cuando el usuario está viajando.

En muchos casos, se requieren diferentes credenciales de usuario para acceder al sistema de ordenador y al portátil, como medida defensiva para evitar puntos débiles de seguridad en cascada. Además, la práctica del uso de nombres de usuario y contraseñas estáticos ha caído en desgracia ya que este tipo de credenciales de usuario se ven comprometidas frecuentemente, son olvidadas temporalmente y hacen que aumenten los gastos administrativos al requerirse una disposición de tipo “servicio de asistencia” para ayudar a usuarios cuyos nombres de usuario y contraseñas o bien han sido olvidados o bien se han visto comprometidos.

Una solución más segura consiste en proporcionar un dispositivo de seguridad portátil, tal como un testigo de seguridad, que reduzca al mínimo el número de credenciales que es necesario recordar por parte de un usuario y que proporcione un mecanismo mucho más seguro para autenticar al usuario con respecto a un sistema de ordenador. No obstante, equipar a cada sistema de ordenador con un testigo de seguridad, un lector y software de interfaz independientes puede resultar caro de desplegar y mantener, presentándose así una barrera económica enorme ante la mejora de la seguridad de los sistemas de ordenador con respecto al uso de nombres de usuario y contraseñas estáticos.

Una posible solución es proporcionar un mecanismo alternativo para autenticarse en uno o más sistemas de ordenador, que reduzca al mínimo el número de testigos de seguridad, lectores y software de interfaz que se requiere instalar y mantener. Un ejemplo de ello se muestra en la solicitud de patente europea EP 1 061 482 A1 de Cuong. La solicitud de Cuong da a conocer un dispositivo portátil inteligente que permite que un usuario se autentique en una pluralidad de proveedores de servicios financieros usando un único testigo de seguridad universal en forma de una tarjeta inteligente. El objetivo básico de esta solicitud es reducir el número de tarjetas inteligentes que es necesario que lleve el usuario.

Otra solución se da a conocer en la patente US nº 6.016.476 de Maes, *et al*. La patente de Maes da a conocer un dispositivo portátil inteligente para ser usado por un consumidor para transacciones en puntos de venta y otras transacciones financieras usando el mismo concepto de un único testigo de seguridad universal en forma de una tarjeta inteligente. Esta patente se dirige a mecanismos de seguridad tales como la autenticación biométrica para evitar el acceso no autorizado al testigo de seguridad universal del usuario.

El documento EP 0 957 651 da a conocer un teléfono con medios de cifrado adicionales. Los medios de cifrado comprenden una conexión para una tarjeta inteligente adicional que contiene claves de cifrado. Esta tarjeta inteligente adicional es una tarjeta inteligente de cifrado (ESC) que contiene medios de memoria y medios de procesado, y posibilita el cifrado de habla o datos de una manera preprogramada de la cual solo tiene conocimiento una ESC correspondiente en un teléfono receptor ya que solamente la ESC del teléfono receptor deseado está provista de las mismas claves de cifrado que el teléfono originador.

El teléfono está provisto también de una tarjeta SIM con fines identificativos y las dos tarjetas tienen contenidos diferentes. La ESC es sencilla de extraer del teléfono en cualquier momento. Los usuarios pueden poseer una serie de ESC para trayectos de comunicación diferentes o personas diferentes con los cuales deseen comunicarse secretamente. Además de la ESC, el teléfono puede estar equipado con otras dos tarjetas para la identificación y autenticación de la red. Una tarjeta inteligente de comunicaciones se usa para la identificación y autenticación mutuas entre el teléfono y el proveedor de servicios de red de comunicaciones. La ESC también puede incluir códigos pin u otras opciones elegidas por el usuario así como el número de teléfono correspondiente al teléfono receptor.

El documento EP 1 271 436 A2 da a conocer un método y un sistema remotos de autenticación de huellas

dactilares.

El documento US nº 5.878.142 da a conocer un dispositivo de comunicaciones de autenticación y cifrado para establecer un enlace de comunicaciones seguro entre un emplazamiento de ordenador remoto y un dispositivo de ordenador de un usuario a través de un trayecto de transferencia de datos, comprendiendo dicho dispositivo de comunicaciones: un dispositivo de cifrado para cifrar datos de transmisión que se transmitirán hacia dicho sitio de ordenador remoto a través de dicho trayecto de transferencia de datos, y para descifrar datos de recepción recibidos por dicho dispositivo de comunicaciones desde una fuente; un autenticador para autenticar en dicho sitio de ordenador remoto que dicho dispositivo de comunicaciones está autorizado; un adaptador de red para transmitir los datos de transmisión y para recibir los datos de recepción a través de dicho trayecto de transferencia de datos; y una caja de bolsillo, compacta, que contiene dicho dispositivo de cifrado, dicho autenticador y dicho adaptador de red, estando dicho dispositivo de cifrado, dicho autenticador y dicho adaptador de red interconectados eléctricamente y estando configurados eléctricamente para su interconexión con dicho trayecto de transferencia de datos y dicho dispositivo de ordenador de dicho usuario. El dispositivo portátil de cifrado y autenticación hace uso preferentemente de un teclado montado en la caja para introducir un número de identificación personal (PIN). El autenticador también se puede hacer funcionar mediante la inserción de una tarjeta inteligente que contiene un pin o código que identifica de manera exclusiva al usuario.

La solicitud de Cuong, la patente de Maes, *et al*. y la patente EP 0 957 651 están destinadas a usarse sobre una red pública en una disposición de cliente-servidor donde el usuario se autentica en una organización externa en lugar de su propia organización. No se pone ningún énfasis particular en la seguridad del enlace de telecomunicaciones.

Todavía en otro planteamiento, la solicitud de patente US 2002-0194499-A1, proporciona una solución que se puede implementar sobre una red pública o privada usando una disposición de autenticación de cliente-servidor y/o entre entidades pares. Esta solicitud afronta las limitaciones antes descritas pero no trata las cuestiones de seguridad relacionadas con enlaces de telecomunicaciones inalámbricas o mecanismos alternativos de inicio de sesión de usuario asociados al acceso al sistema de ordenador no atendido del usuario.

En la técnica relevante, se ha determinado que algunos de los protocolos más antiguos de seguridad inalámbrica podrían verse comprometidos por un atacante razonablemente sofisticado. Por ejemplo, la privacidad equivalente inalámbrica (WEP) especificada por la norma IEEE 802.11:1999 estaba destinada a proporcionar aproximadamente el mismo nivel de confidencialidad para datos inalámbricos que el disponible en una LAN por cable (Ethernet) que no está protegida mediante cifrado.

Versiones posteriores de las normativas IEEE 802.11 han mejorado el nivel de seguridad de las conexiones inalámbricas. No obstante, no es aconsejable una dependencia total del desarrollo de protocolos de seguridad. Como tal, deberían proporcionarse medidas de seguridad adicionales para garantizar que la información de autenticación no se ve comprometida o es vulnerable a ataques del tipo “hombre en el medio”, por “diccionario” o de “reproducción”.

Por último, es necesario establecer un mecanismo seguro que permita que un usuario se autentique en su sistema de ordenador y que no requiera cambios significativos en mecanismos existentes de autenticación de usuario incluidos en sistemas operativos de ordenadores y que no reduzca el nivel total de seguridad al que llegan los mecanismos de autenticación existentes.

Por lo tanto, una dispositivo de autenticación segura que permite que un dispositivo remoto inteligente emule un dispositivo periférico de seguridad local en una relación entre entidades pares a través de una red privada sin reducción del nivel global de seguridad resultaría altamente ventajoso en los entornos informáticos empresariales actuales.

Sumario

Este objetivo se logra mediante la combinación de características que se definen por medio de la reivindicación 1 para el método y que se definen por medio de la reivindicación 12 para el sistema.

Esta invención afronta las limitaciones descritas anteriormente y proporciona un dispositivo remoto inteligente equipado con un testigo de seguridad que emula un dispositivo periférico de seguridad local en una relación entre entidades pares a través de una red privada, sin reducción del nivel global de seguridad. El dispositivo remoto inteligente incluye un asistente personal de datos (PDA), un teléfono celular que tiene capacidades de redes privadas, un aparato de red o un dispositivo de seguridad personal, tal como un teclado seguro para introducir el PIN.

La expresión “testigo de seguridad” según se describe en la presente incluye dispositivos de seguridad basados en hardware, tales como módulos criptográficos, tarjetas inteligentes, tarjetas chip de circuito integrado, soportes de datos portátiles (PDC), dispositivos de seguridad personales (PSD), módulos de identificación de abonado (SIM), módulos de identificación inalámbrica (WIM), mochilas testigo USB, testigos de identificación, módulos de aplicación

segura (SAM), módulos de seguridad de hardware (HSM), testigos multi-media seguros (SMMC), chips de la *trusted platform computing alliance* (TPCA) y dispositivos similares.

En varias formas de realización del método de la invención, la invención comprende un método para acceder a un sistema de ordenador habilitado para testigos de seguridad usando un dispositivo remoto inteligente como interfaz de comunicaciones para un testigo de seguridad.

El método incluye el establecimiento de una primera conexión de comunicaciones entre el dispositivo remoto inteligente y una pasarela de red acoplada a una red en común con un sistema de ordenador. La red en común incluye redes inalámbricas privadas tales como BlueTooth, HomeRF, y IEEE 802.11 a/b/g y sus sucesores.

La conexión de comunicaciones utiliza protocolos existentes de seguridad establecidos para los dispositivos de interfaz de red y consiste esencialmente en el intercambio de señales de entrada en contacto para la conexión entre el dispositivo remoto inteligente y la pasarela de red. Sus ejemplos incluyen la capa de conexión segura (SSL), la seguridad de capa de transporte (TLS), la tecnología de comunicaciones privadas (PCT), la seguridad del protocolo de internet (IPsec) o una disposición de mensajería segura.

La disposición de mensajería segura incorpora un par de claves simétricas compartidas, con fines criptográficos, que es identificado de manera exclusiva por un identificador de sesión generado y asignado por el testigo de seguridad. De forma alternativa, o en combinación con la criptografía de claves simétricas, se puede establecer un conducto (*pipe*) de comunicaciones APDU entre el sistema de ordenador y el testigo de seguridad. El conducto de comunicaciones APDU permite el intercambio de órdenes y respuestas APDU de testigo de seguridad nativas que se encapsulan en protocolos de red normalizados, tales como el TCP/IP.

Una vez que se ha establecido la conexión de comunicaciones, en el testigo de seguridad se proporciona un parámetro de seguridad crítico (CSP) asociado a un usuario, usando el dispositivo remoto inteligente como interfaz de comunicaciones. Un parámetro de seguridad crítico según se define en la presente incluye datos de autenticación, contraseñas, PINs, claves criptográficas secretas y privadas que se van a introducir en o se les dará salida desde un módulo criptográfico, y pretende ser sinónimo de la definición de CSP incluida en FIPS PUB 140-2, “Security Requirements for Cryptographic Modules”.

El parámetro de seguridad crítico se proporciona desde otro sistema de ordenador y se envía al testigo de seguridad a través de otra conexión inalámbrica. Por ejemplo, un escáner biométrico puede estar acoplado a la red en común. En esta disposición, el poder computacional generalmente mayor del sistema de ordenador del usuario se puede usar para procesar una muestra biométrica que posteriormente se compara con el testigo de seguridad.

A continuación, el parámetro de seguridad crítico proporcionado del usuario se usa para llevar a cabo una transacción de autenticación, en la cual el usuario se autentica en el sistema de ordenador y el testigo de seguridad. Se puede incorporar también una transacción de autenticación de dos factores en la que el testigo de seguridad se autentica en el sistema de ordenador intercambiando información de autenticación durante el establecimiento de la conexión de comunicaciones. El proceso de autenticación de dos factores se puede llevar a cabo usando contraseñas dinámicas de un solo uso, desafío/respuesta o mediante intercambios de certificados digitales. Al completarse de manera exitosa la transacción de autenticación, al usuario se le permite acceder a por lo menos un recurso seguro asociado al sistema de ordenador.

Para garantizar la seguridad y para facilitar las comunicaciones entre el testigo de seguridad y el sistema de ordenador a través de un cortafuegos de tipo traducción de direcciones de red (NAT), la conexión de comunicaciones se inicia enviando un mensaje de solicitud de acceso desde el dispositivo remoto inteligente al sistema de ordenador. El mensaje de solicitud de acceso proporciona suficiente información a la pasarela de red para su encaminamiento al sistema de ordenador objetivo e incluye una dirección de red de retorno en la cual responderá el sistema de ordenador objetivo. Se puede establecer múltiples conexiones lógicas a través de la red con uno o más sistemas de ordenador para utilizar el dispositivo remoto inteligente como dispositivo periférico de seguridad. El mensaje de solicitud de acceso incluye además información que identifica al dispositivo remoto inteligente y al testigo de seguridad asociado.

El sistema de ordenador incluye un método de autenticación de usuarios que permite que el usuario se autentique de manera remota en el sistema de ordenador a través de la conexión de comunicaciones. El término “método”, según se define en la presente, se usa en su contexto más amplio el cual incluye una función, aplicación, rutina, método invocable de manera remota, subrutina o miniaplicación. El método alternativo de autenticación de usuario incluye un agente que monitoriza tráfico de red entrante dirigido al sistema de ordenador, en busca de un mensaje de solicitud de acceso. El agente invoca el método alternativo de autenticación de usuarios el cual es un adjunto o sustituto de un método principal de autenticación de usuarios.

Tras una autenticación exitosa al usuario se le proporciona un retorno sonoro o visual. Esto permite que el usuario determine qué sistema de ordenador de entre una pluralidad de sistemas de ordenador se ha autenticado. El retorno sonoro o visual se puede proporcionar en uno de entre el dispositivo remoto inteligente y el sistema de ordenador

autenticado o en ambos.

En otra forma de realización de la invención, se establece un trayecto de confianza entre el testigo de seguridad y el dispositivo remoto inteligente. El trayecto de confianza permite que el dispositivo remoto inteligente se use en entornos operativos de alta seguridad, tales como los niveles de seguridad FIPS 3 y 4, que requiere que los parámetros de seguridad críticos se introduzcan en o se les dé salida desde un módulo criptográfico en forma cifrada para evitar la interceptación de los parámetros de seguridad críticos.

En varias formas de realización de la invención, la porción de hardware de la invención incluye un dispositivo remoto inteligente equipado con un testigo de seguridad en el procesado de comunicaciones con un sistema de ordenador a través de una red. La red incluye una red privada inalámbrica, tal como BlueTooth, HomeRF, IEEE 802.11 a/b/g y sucesores, que incorporan un protocolo de comunicaciones seguro que comprende la capa de conexión segura (SSL), la seguridad de capa de transporte (TLS), la tecnología de comunicaciones privadas (PCT), la seguridad del protocolo de internet (IPsec) o una disposición de mensajería segura.

El dispositivo remoto inteligente incluye un asistente personal de datos (PDA), un teléfono celular que tiene capacidades de redes privadas, un aparato de red o un dispositivo de seguridad personal tal como un teclado seguro para introducir el PIN.

El dispositivo remoto inteligente está equipado con el hardware, software y microprogramas necesarios para emular un dispositivo periférico de testigo de seguridad que está conectado localmente al sistema de ordenador e incluye las capacidades de; acoplar operativamente el testigo de seguridad al dispositivo remoto inteligente, enviar un mensaje de solicitud de acceso a través de la red al sistema de ordenador para invocar el establecimiento de una conexión de comunicaciones segura entre el testigo de seguridad y el sistema de ordenador, proporcionar protección criptográfica de datos intercambiados entre el dispositivo remoto inteligente y el sistema de ordenador, recibir un parámetro de seguridad crítico proporcionado por el usuario o bien directamente o bien recibido a través de la conexión de comunicaciones segura, intercambiar información a través de la red usando un conducto de comunicaciones APDU y proporcionar retorno sonoro o visual al usuario al completarse de manera exitosa una transacción de autenticación de dos factores.

El testigo de seguridad está compuesto por dispositivos de seguridad basados en hardware, tales como módulos criptográficos, tarjetas inteligentes, tarjetas chip de circuito integrado, soportes de datos portátiles (PDC), dispositivos de seguridad personales (PSD), módulos de identificación de abonado (SIM), módulos de identificación inalámbricos (WIN), mochilas testigo USB, testigos de identificación, módulos de aplicación segura (SAM), módulos de seguridad por hardware (HSM), testigos multimedia seguros (SMMC), chips de la *trusted platform computing alliance* (TPCA) y dispositivos similares. El testigo de seguridad está provisto de por lo menos un parámetro de seguridad crítico de referencia instalado operativamente, asociado al usuario, e incluye las capacidades de; recibir un parámetro de seguridad crítico asociado al usuario, llevar a cabo una transacción de autenticación.

El sistema de ordenador incluye por lo menos una estación de trabajo, un servidor, un ordenador de sobremesa, un ordenador portátil, un ordenador personal, un miniordenador o un ordenador central (*mainframe*), que requiere autenticación del usuario antes de permitir que un usuario disponga de acceso. La porción de sistema de ordenador de la invención está equipada con el hardware, software y microprogramas necesarios para permitir que el usuario se autentique de manera remota en el sistema de ordenador a través de la red como si el usuario fuera local con respecto al sistema de ordenador e incluye las capacidades de; recibir una solicitud de acceso enviada a través de la red desde el dispositivo remoto inteligente, establecer la conexión de comunicaciones entre el sistema de ordenador y el testigo de seguridad, ejecutar un método alternativo de autenticación de usuarios que permite que el usuario se autentique de manera remota en el sistema de ordenador a través de la red usando la transacción de autenticación de dos factores, intercambiar información a través de la red o conexión de comunicaciones usando un conducto de comunicaciones APDU y permitir que el usuario acceda al sistema de ordenador tras completarse de manera exitosa la transacción de autenticación de dos factores.

El dispositivo remoto inteligente y el sistema de ordenador habilitado para testigos de seguridad incluyen un conjunto de interfaces de programación de aplicación materializadas en un soporte legible por ordenador para su ejecución por parte de un procesador, que permite que el dispositivo remoto inteligente emule un dispositivo periférico de testigo de seguridad conectado localmente al sistema de ordenador habilitado para testigos de seguridad. Las interfaces de programación de aplicaciones comprenden una primera interfaz que intercambia información entre un testigo de seguridad y el sistema de ordenador habilitado para testigos de seguridad en un protocolo nativo del testigo de seguridad, y una segunda interfaz que recibe y encamina un parámetro de seguridad crítico al testigo de seguridad.

En una forma de realización de la invención, el primer conjunto de programas de interfaz de aplicación instalados en el dispositivo remoto inteligente proporciona una conversión de protocolo a un protocolo nativo del testigo de seguridad. En otra forma de realización de la invención, el primer conjunto de programas de interfaz de aplicación instalados en el dispositivo remoto inteligente extrae la información de paquetes de comunicaciones ya en un protocolo nativo de dicho testigo de seguridad.

Los programas y datos asociados se pueden almacenar en soportes transportables de grabación digital, tales como CD ROM, disco flexible, cinta de datos, DVD, o disco duro extraíble para su instalación en el sistema de ordenador, el dispositivo remoto inteligente y/o el testigo de seguridad en forma de uno o más productos de programa de ordenador transportables. Los programas y datos asociados comprenden instrucciones ejecutables que se almacenan en un formato de código incluyendo código en bytes, compiladas, completadas, compatibles o interpretables.

El producto de programa de ordenador materializado en forma tangible es legible por una pluralidad de procesadores en el procesado de comunicaciones e incluye instrucciones ejecutables almacenadas para conseguir que uno o más de la pluralidad de procesadores; establezca una conexión de comunicaciones segura entre un testigo de seguridad y un sistema de ordenador habilitado para testigos de seguridad por medio de un dispositivo remoto inteligente, autentique por lo menos el testigo de seguridad en dicho sistema de ordenador habilitado para testigos de seguridad, proporcione un parámetro de seguridad crítico asociado a un usuario al testigo de seguridad y autentique el parámetro de seguridad crítico mediante el testigo de seguridad.

Breve descripción de los dibujos

Las características y ventajas de la invención se pondrán de manifiesto a partir de la siguiente descripción detallada haciendo referencia a los dibujos adjuntos. Cuando sea posible, se usan los mismos números y caracteres de referencia para indicar características, elementos, componentes o porciones iguales de la invención. Se pretende que, en la forma de realización descrita, se pueden efectuar cambios y modificaciones sin apartarse del verdadero alcance y espíritu de la invención en cuestión según se define en las reivindicaciones.

La figura 1 - es un diagrama de bloques generalizado de un sistema de ordenador habilitado para testigos de seguridad y un testigo de seguridad conectado funcionalmente.

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

La figura. 1B-1 - es un diagrama de bloques detallado de los módulos funcionales incorporados en el sistema de ordenador habilitado para testigos de seguridad.

La figura 1B-2 - es un diagrama de bloques detallado de los módulos funcionales incorporados en el dispositivo remoto inteligente.

La figura 1C - es un diagrama de bloques detallado de un proceso iniciador que permite que el dispositivo remoto inteligente emule un dispositivo periférico de seguridad local conectado al sistema de ordenador habilitado para testigos de seguridad.

La figura 1D - es un diagrama de bloques detallado del dispositivo remoto inteligente que emula un dispositivo periférico de seguridad local conectado al sistema de ordenador habilitado para testigos de seguridad.

La figura 2A - es un diagrama de bloques detallado de una forma de realización de una conexión de comunicaciones segura entre el testigo de seguridad y el sistema de ordenador habilitado para testigos de seguridad donde, en la conexión segura, se incorpora un par de claves simétricas compartidas.

La figura 2B - es un diagrama de bloques detallado de otra forma de realización de una conexión de comunicaciones segura entre el testigo de seguridad y el sistema de ordenador habilitado para testigos de seguridad donde, en la conexión segura, se incorporan dos conjuntos de pares de claves simétricas.

La figura 2C - es un diagrama de bloques detallado de otra forma de realización de una conexión de comunicaciones segura entre el testigo de seguridad y el sistema de ordenador habilitado para testigos de seguridad donde, en la conexión segura, se incorpora un conducto de comunicaciones APDU.

La figura 2D - es un diagrama de bloques detallado de otra forma de realización de la invención donde un sistema de ordenador adicional habilitado para testigos de seguridad y un servidor de autenticación se conectan de manera segura al testigo de seguridad.

La figura 3 - es un diagrama de flujo que ilustra las etapas principales asociadas a la habilitación de un dispositivo remoto inteligente para emular un dispositivo periférico de seguridad local conectado a un sistema de ordenador habilitado para testigos de seguridad.

Descripción detallada

La presente invención proporciona una disposición que permite que un dispositivo remoto inteligente emule de manera segura un dispositivo periférico de seguridad local conectado a un sistema de ordenador habilitado para

testigos de seguridad por medio de una red. Las aplicaciones están ideadas para ser programadas en un lenguaje de alto nivel tal como Java™, C++, C, C# o Visual Basic™.

Haciendo referencia a la figura 1, se muestra un diagrama de bloques funcional del sistema de ordenador habilitado para testigos de seguridad, que incluye un procesador central 5, una memoria principal 10, un dispositivo de visualización 20 acoplado eléctricamente a una interfaz de visualización 15, un subsistema de memoria secundario 25 acoplado eléctricamente a una controladora de disco duro 30, una controladora de almacenamiento extraíble 35 acoplada eléctricamente a una unidad de almacenamiento extraíble 40 y una interfaz de almacenamiento extraíble, auxiliar, 45 acoplada eléctricamente a una unidad de almacenamiento extraíble, auxiliar 50.

Un subsistema de interfaz de comunicaciones 55 está acoplado a una red 65 por medio de una interfaz de red 60. Un testigo de seguridad 75 está acoplado operativamente a la interfaz de comunicaciones 55 por medio de una interfaz de testigos de seguridad 70. Los dispositivos de entrada de usuario, incluyendo un ratón y un teclado 85, están acoplados operativamente a la interfaz de comunicaciones 55 por medio de una interfaz de usuario 80. Por último, un escáner biométrico opcional está acoplado operativamente a la interfaz de comunicaciones 55 por medio de una interfaz de escáner biométrico 90.

El procesador central 5, la memoria principal 10, la interfaz de visualización 15, el subsistema de memoria secundario 25 y el sistema de interfaz de comunicaciones 55 están acoplados eléctricamente a una infraestructura de comunicaciones 100. El sistema de ordenador anfitrión 105 incluye un sistema operativo que tiene una aplicación de seguridad de inicio de sesión, extensible, modificable o sustituible, una interfaz de programación de aplicaciones de testigos de seguridad, una o más aplicaciones compatibles con testigos de seguridad, una o más extensiones privativas para la aplicación de seguridad de inicio de sesión, un agente de comunicaciones con capacidad de detectar una solicitud de acceso entrante e invocar un método de inicio de sesión alternativo, software criptográfico con capacidad de llevar a cabo funciones criptográficas simétricas y asimétricas, software de mensajería segura y todo software necesario de interfaces y controladores de dispositivos.

El testigo de seguridad 75 incluye unos medios de conexión inalámbrica, óptica, y/o eléctrica compatibles con la interfaz de testigos de seguridad 70, un procesador, un coprocesador criptográfico, memoria volátil y no volátil acoplada eléctricamente al procesador y al coprocesador, un entorno operativo en tiempo de ejecución, extensiones criptográficas disponibles para el sistema operativo y con capacidad de llevar a cabo funciones criptográficas simétricas y asimétricas compatibles con el software criptográfico del sistema de ordenador, una aplicación ejecutiva de seguridad, una o más aplicaciones protegidas con CSP que incluyen autenticaciones de dos factores están acopladas funcionalmente a la aplicación ejecutiva de seguridad y un par de claves de la infraestructura de clave pública (PKI) acoplado funcionalmente a la aplicación ejecutiva de seguridad.

El testigo de seguridad 75 incluye además las aplicaciones de autenticación y extensiones criptográficas necesarias para llevar a cabo satisfactoriamente la transacción de autenticación de dos factores con el sistema de ordenador habilitado para testigos de seguridad. La memoria no volátil tiene almacenados operativamente en la misma uno o más CSP de referencia que son verificados por la aplicación ejecutiva de seguridad para autenticar un usuario con respecto al testigo de seguridad. El testigo de seguridad 75 se materializa en un factor de forma extraíble, aunque también funcionarán otros factores de forma.

La red 65 incluye una red privada inalámbrica, tal como Bluetooth, HomeRF, IEEE 802.11 a/b/g y sus sucesores, que incorporan un protocolo de comunicaciones seguro que comprende la capa de conexión segura (SSL), la seguridad de capa de transporte (TLS), el protocolo de la tecnología de comunicaciones privadas (PCT), la seguridad del protocolo de internet (IPsec) o una disposición de mensajería segura. La red 65 incluye además una pasarela de red que permite una conexión ad hoc con el dispositivo remoto inteligente.

Haciendo referencia a la figura 1A, se muestra un diagrama de bloques funcional de un dispositivo remoto inteligente 110. El dispositivo remoto inteligente 110 incorpora esencialmente los mismos componentes modulares incluidos en el ordenador habilitado para testigos de seguridad descrito anteriormente. El dispositivo remoto inteligente incluye un procesador 5', una memoria principal 10', un dispositivo de visualización 20' acoplado eléctricamente a una interfaz de visualización 15', un subsistema de memoria secundario 25' acoplado eléctricamente a una controladora de disco duro opcional 30', una controlador de almacenamiento virtual 35', y una interfaz de memoria extraíble 45' acoplada eléctricamente a un módulo de memoria extraíble 50'.

Un subsistema de la interfaz de comunicaciones 55' está acoplado a una red 65 por medio de una interfaz de red 60', un testigo de seguridad 75' acoplado a una interfaz de testigo de seguridad 70' y una disposición de entrada de usuario incluyendo un estilete, un lápiz táctil, un dispositivo de visualización sensible al tacto, un ratón y/o teclado en miniatura 85' acoplado a una interfaz de dispositivo de usuario 80' y un escáner biométrico opcional 95' acoplado a una interfaz de escáner biométrico opcional 90'. El procesador 5', la memoria principal 10', la interfaz de visualización 15', el subsistema de memoria secundario 25' y el sistema de interfaz de comunicaciones 55' están acoplados eléctricamente a una infraestructura de comunicaciones 100'.

El dispositivo remoto inteligente 110 incluye además un sistema operativo que tiene una aplicación de seguridad de

inicio de sesión, extensible, modificable o sustituible, una o más extensiones privativas para la aplicación de seguridad de inicio de sesión, una interfaz de programación de aplicaciones para testigos de seguridad, por ejemplo PC/SC, una o más aplicaciones compatibles con testigos de seguridad, una aplicación de emulador de testigos con capacidad de conseguir que el dispositivo remoto inteligente intercambie de manera transparente órdenes de testigos de seguridad y respuestas entre el sistema de ordenador de red, software criptográfico con capacidad de llevar a cabo funciones criptográficas simétricas y asimétricas, software de mensajería seguro y todo el software necesario de interfaces y controladores de dispositivos. El testigo de seguridad 75' puede ser el mismo dispositivo usado normalmente para acceder al sistema de ordenador habilitado para testigos de seguridad 105 u otro testigo de seguridad que contenga la información necesaria para completar de manera satisfactoria la transacción de autenticación de dos factores.

Haciendo referencia a la figura 1B-1, se muestra un diagrama funcional de capas del sistema de ordenador. Las diversas capas mostradas se basan aproximadamente en el modelo de Interconexión de Sistemas Abiertos (OSI). Para simplificar, ciertas capas no se muestran y deberían considerarse como presentes y/o incorporadas en capas adyacentes. La capa de aplicaciones superior 115 incluye aplicaciones de usuario y compatibles con testigos de seguridad, indicadas como Aplicaciones de Testigos de Seguridad 175.

La capa de soporte intermedio (*middleware*) 120 incluye aplicaciones de la interfaz de programación de aplicaciones para testigos de seguridad, indicadas como API de Testigos de Seguridad 145 que permiten que el usuario y aplicaciones compatibles con testigos de seguridad incluidas en la capa de aplicaciones 115 se comuniquen con el testigo de seguridad adjunto 75. Un ejemplo de la interfaz de programación de aplicaciones para testigos de seguridad se describe en las especificaciones del grupo de trabajo de PC/SC disponibles en el sitio web de la organización www.pcscworkgroup.com.

La capa de sistema operativo 125 incluye el software que controla la asignación y el uso de recursos de hardware tales como memoria, tiempo de la unidad de procesado central (CPU), espacio en el disco, y dispositivos periféricos. Incluidas en esta capa se encuentran la(s) aplicación(es) de seguridad de inicio de sesión 150 y extensiones añadidas 155 que permiten un método alternativo de autenticación del usuario. Se muestra un dispositivo de entrada de usuario 85 acoplado a la extensión añadida Ext 155.

Por ejemplo, en Windows® de Microsoft, se proporciona una biblioteca enlazada dinámicamente, personalizable o sustituible, (msgina.dll) que permite la inclusión de métodos alternativos de autenticación desarrollados por proveedores externos. En "The Essentials of Replacing the Microsoft® Graphical Identification and Authentication Dynamic Link Library", de Ben Hutz y Jack Fink, ambos de Microsoft Corporation, publicada en junio de 2001, se presenta una breve descripción sobre cómo un experto en la materia personalizaría o sustituiría la msgina.dll.

En sistemas operativos basados en Unix® y Linux®, se instalan una aplicación ejecutiva de seguridad independiente, controladores de hardware y software, y bibliotecas de políticas de seguridad que se comunican por interfaz con un Módulo de Autenticación Conectable (PAM) y un Entorno de Visualización Común (CDE). De forma análoga, el PAM y el CDE permiten personalización y sustitución. A partir del Movimiento para el Uso de Tarjetas Inteligentes en un Entorno Linux (MUSCLE) en www.linuxnet.com, se encuentra disponible una biblioteca extensiva de aplicaciones soportadas que incluyen códigos fuente y documentación.

La capa de comunicaciones 130 es esencialmente una consolidación de las capas de red y de transporte, e incluye un agente 160 y software de Interfaz de APDU 170, cuyos ejemplos se han proporcionado anteriormente. El agente se usa para monitorizar tráfico de red entrante en relación con un mensaje de solicitud de acceso. La detección de un mensaje de solicitud de acceso por parte del agente 160 invoca al método alternativo de autenticación de usuario.

La invocación del método alternativo de autenticación de usuario mediante la detección de un mensaje de solicitud de acceso por parte del agente 160 provoca que el gestor de recursos 165 conmute la interfaz del dispositivo de testigo de seguridad desde la interfaz de dispositivo de testigo de seguridad local 70 a la interfaz de dispositivo de testigo remoto 180. El software de la Interfaz de APDU proporciona una conversión de protocolos entre los diversos formatos de comunicaciones usados por el sistema de ordenador, la red y el testigo de seguridad. En una forma de realización alternativa de la invención, la conversión de protocolos de APDU se lleva a cabo mediante una aplicación equivalente instalada en el dispositivo remoto inteligente.

La capa de enlace de datos indicada como Controladores de Dispositivos 135 incluye un gestor de recursos 165 que controla el acceso al testigo de seguridad 75, y es la aplicación responsable de seleccionar o bien el controlador de dispositivo de testigos local 175 ó bien el controlador de dispositivo de testigos remoto 180 basándose en políticas establecidas de inicio de sesión. Los controladores de dispositivos de software se pueden basar en la PC/SC (Ordenador Personal/Tarjeta Inteligente) promulgada por el consorcio industrial Open Card (SM). Se encuentra disponible información adicional a partir del sitio web del consorcio en www.opencard.org.

La capa final indicada como Dispositivos Físicos 140 incluye la interfaz de dispositivo de testigo local 70 que acopla el testigo de seguridad 75 al sistema de ordenador 105. La capa de dispositivo físico 140 incluye además un

controlador de dispositivo de seguridad remoto basado en software 180. Este controlador de dispositivo de testigo remoto 180 está incluido en la capa de dispositivos físicos 140 para simplificar la comprensión de la invención únicamente. En realidad, el controlador de dispositivo de testigo remoto 180 está instalado en la capa de Controladores de Dispositivos 135. Por último, un dispositivo de interfaz de red 60 proporciona la conexión física entre el sistema de ordenador 105 y la red 65.

Haciendo referencia a la figura 1B-2, se muestra un diagrama de capas funcional del dispositivo remoto inteligente 110. Tal como se ha descrito anteriormente, las diversas capas mostradas se basan aproximadamente en el modelo de Interconexión de Sistemas Abiertos (OSI). El dispositivo remoto inteligente 110 incorpora esencialmente las mismas capas funcionales incluidas en el ordenador habilitado para testigos de seguridad descrito en la figura 1B-1 y estas no se repetirán en el caso que nos ocupa. Se muestra un emulador de testigo 182 como una aplicación de soporte intermedio 120' que permite que el dispositivo remoto inteligente 110 emule un dispositivo periférico de testigo de seguridad conectado localmente al sistema de ordenador habilitado para testigos de seguridad 105 a través de una red inalámbrica 65.

El emulador de testigos 182 incluye interfaces lógicas que facilitan el intercambio transparente de información entre el testigo de seguridad 75' y el sistema de ordenador habilitado para testigos de seguridad 105 en un protocolo nativo del testigo de seguridad 75', y recibe y encamina un parámetro de seguridad crítico 85' introducido localmente en el dispositivo remoto inteligente 110 ó recibido desde la red inalámbrica 65' al testigo de seguridad 75'. Aunque el emulador de testigos 182 se muestra como una aplicación de soporte intermedio 125', los expertos en la materia apreciarán que el mismo también se puede proporcionar como una subrutina, un control ActiveX, una función, un método invocable de manera remota asociado a la API de Testigos 145 o agente 160 instalado en el sistema de ordenador habilitado para testigos de seguridad 105, o una miniaplicación de navegador local.

El protocolo nativo tiene en general el formato de una unidad de datos de protocolo de aplicación (APDU) según se especifica en la ISO 7816-4. Tal como se describe en la presente, el emulador de testigos facilita el intercambio transparente de órdenes y respuestas APDU entre el sistema de ordenador habilitado para testigos de seguridad 105 y el dispositivo remoto inteligente 110. Se proporcionan varias formas de realización de comunicaciones de la invención que se describen en las argumentaciones incluidas con las figuras 2A a 2D las cuales se ofrecen a continuación.

Haciendo referencia a la figura 1C, se muestra un diagrama de bloques detallado que ilustra la interacción del dispositivo remoto inteligente 110 con el sistema de ordenador 105. En la presente descripción se omiten detalles relacionados con consideraciones de seguridad para información intercambiada a través de la red 65 con el fin de simplificar la explicación y comprensión de esta parte de la invención. Se incluyen consideraciones de seguridad en la descripción correspondiente a las figuras 2A a 2D que se ofrece a continuación.

Para iniciar el proceso en una forma de realización de la invención, un usuario en posesión del dispositivo remoto inteligente 110 selecciona una aplicación de autenticación remota compatible con testigos 175'. La aplicación de autenticación remota 175' provoca que la aplicación de emulación de testigos 182 ejecute un método de autenticación alternativo que implementa una política o guión de instrucciones de seguridad preestablecido asociado a la extensión EXT 155' con respecto a la aplicación de inicio de sesión 150'. La invocación de la aplicación de inicio de sesión 150' provoca que la aplicación de autenticación remota 175' invite al usuario a introducir su parámetro de seguridad crítico (CSP) 188. En una forma de realización relacionada de la invención, la aplicación de emulador de testigos 182 genera un mensaje de solicitud de acceso AR 190 el cual se envía a través de la red 65 al sistema de ordenador 105.

El mensaje de solicitud de acceso incluye información sobre el dispositivo remoto inteligente, tal como un identificador exclusivo, información sobre el testigo de seguridad acoplado operativamente 75', tal como un número de serie exclusivo, e información sobre la dirección de red asignada. El mensaje de solicitud de acceso se usa para transitar por un punto de acceso inalámbrico en disposiciones de redes inalámbricas.

En una forma de realización de la invención, un usuario introduce su CSP 188 el cual se encamina por medio de la aplicación de inicio de sesión 150', a través del gestor de recursos 165', a la interfaz de APDU 170' con vistas a la conversión de protocolos. A continuación, el CSP 188 incorporado en formato de APDU se encamina a través de la interfaz de dispositivo de testigo de seguridad 70 y hacia el testigo de seguridad 75'. El testigo de seguridad lleva a cabo una transacción de autenticación la cual autentica al usuario con respecto al testigo de seguridad. La autenticación del usuario se lleva a cabo mediante comparación del CSP introducido 188 con un CSP de referencia almacenado dentro del testigo de seguridad 75'.

En la invención, el CSP 188 se introduce desde una ubicación remota y se envía de forma segura a través de otra conexión inalámbrica al testigo de seguridad 75' por medio del dispositivo remoto inteligente 110. Esta invención resulta particularmente adecuada para la autenticación biométrica que requiere en general un mayor poder de procesado que el que puede estar disponible a partir del dispositivo remoto inteligente.

En el sistema de ordenador 105, la recepción del mensaje de solicitud de acceso AR 190 es detectada por el agente

160 el cual provoca la invocación del método alternativo de autenticación de usuario. Tal como se ha descrito previamente, la invocación del método alternativo de autenticación de usuario mediante la detección de un mensaje de solicitud de acceso por parte del agente 160 provoca que el gestor de recursos 165 conmute los controladores de dispositivos de testigo de seguridad desde el dispositivo de interfaz de testigo local 70 al controlador de dispositivo de testigo remoto 180. La API de testigos 145 es invocada al mismo tiempo por la extensión EXT 155 que provoca el inicio de la transacción de autenticación. El control de las aplicaciones equivalentes instaladas en el sistema de ordenador habilitado para testigos de seguridad 105 y el dispositivo remoto inteligente se puede llevar a cabo usando invocación remota de métodos, subrutinas y métodos invocables. Los expertos en la materia apreciarán que en la técnica correspondiente hay disponibles muchos mecanismos alternativos para lograr la invocación y control de las aplicaciones y módulos equivalentes.

Haciendo referencia a la figura 1D, una segunda parte de la transacción de autenticación se lleva a cabo bajo el control de la API de testigos 145. La segunda parte de la transacción de autenticación utiliza una política o guión de instrucciones de seguridad preestablecido, asociado a la aplicación de inicio de sesión 125. La política de seguridad puede incluir desafío/respuesta, intercambio de certificados digitales, contraseñas dinámicas, etcétera. Se intercambian datos de autenticación por medio de la interfaz de APDU 170 y el gestor de recursos 165 usando la interfaz de dispositivo de testigo de seguridad remoto 180 y la interfaz de red 60, y los mismos se intercambian a través de la red 65 con el dispositivo remoto inteligente 110. Los datos de autenticación recibidos en la interfaz de red 60' del dispositivo remoto inteligente son encaminados por el emulador de testigos 182, por medio del gestor de recursos 165' y la interfaz de APDU 170', a través de la interfaz de dispositivos de testigo de seguridad 70' y hacia el testigo de seguridad 75'.

Haciendo referencia a la figura 2A, se muestra una disposición de mensajería segura en la que se usa un par de claves simétricas Ksys'[ID] 205', Ksys[ID] 205 que tiene un identificador de sesión exclusivo asignado por el testigo de seguridad 75', para proporcionar una protección criptográfica de extremo-a-extremo de la información intercambiada entre el testigo de seguridad ST 75' por medio del dispositivo remoto inteligente IRD 110 y el sistema de ordenador CS 105 a través de la red 65. La red 65 incluye una pasarela de red NG 255 que proporciona una conexión segura ad hoc 230 entre la pasarela de red y el dispositivo remoto inteligente IRD 110. El par de claves simétricas Ksys'[ID] 205', Ksys[ID] 205 se incorpora en una disposición criptográfica simétrica que se describe en la solicitud US, en trámite con la presente, de cesión conjunta, n.º de serie 10/424.783, presentada por primera vez el 29/04/2003, titulada "Universal Secure Messaging For Cryptographic Modules", y que se incorpora a la presente a título de referencia.

En relación con la figura 2B, se muestra una disposición alternativa de mensajería segura en la que dos conjuntos de pares de claves simétricas Ksys'[ID] 205', Ksys[ID] 205, Ksys'[Idx] 210', Ksys[Idx] 210, que presenta cada uno de ellos un identificador de sesión exclusivo asignado por el testigo de seguridad 75', se usan para proporcionar una protección criptográfica de extremo-a-extremo de información intercambiada entre el testigo de seguridad ST 75' por medio del dispositivo remoto inteligente IRD 110 y el sistema de ordenador CS 105 a través de la red 65. El primer conjunto de par de claves simétricas Ksys'[ID] 205', Ksys[ID] 205 se usa para proporcionar un trayecto de confianza entre el testigo de seguridad 75' y el dispositivo remoto inteligente IRD 110. El trayecto de confianza permite usar el dispositivo remoto inteligente 110 en entornos operativos de alta seguridad, tales como los niveles de seguridad FIPS 3 y 4, que requieren la introducción de parámetros de seguridad críticos en o su salida desde un módulo criptográfico en un formato cifrado para evitar la interceptación de parámetros de seguridad críticos.

El segundo conjunto de par de claves Ksys'[Idx] 210', Ksys[Idx] 210 proporciona la conexión de comunicaciones segura entre el dispositivo remoto inteligente IRD 110 y el sistema de ordenador 105. Otros aspectos de esta segunda forma de realización de comunicaciones seguras se describen de modo similar en la solicitud US en trámite con la presente, n.º de serie 10/424.783.

Haciendo referencia a la figura 2C, se muestra otra forma de realización de comunicaciones seguras en la que se establece un conducto APDU entre el dispositivo remoto inteligente IRD 110 y el sistema de ordenador CS 105. En esta forma de realización de la invención, una aplicación de servidor de conductos 240 se instala en el sistema de ordenador CS 105. La aplicación de servidor de conductos 240 se usa para encapsular órdenes APDU en paquetes de comunicaciones, en general TCP/IP, para su transmisión a través de la red 65 al dispositivo remoto inteligente. Las APDU's se pueden cifrar antes o después de su encapsulamiento en un paquete de comunicaciones de red. La aplicación de servidor de conductos 240 se usa también para separar respuestas APDU entrantes con respecto a los paquetes de comunicaciones de red, y convertir las respuestas APDU resultantes en un protocolo legible por otras aplicaciones instaladas en el sistema de ordenador CS 110.

El dispositivo remoto inteligente IRD 110 incluye una aplicación de cliente de conductos 245 que se usa para separar órdenes APDU entrantes con respecto a los paquetes de comunicaciones de red, y encaminar las órdenes APDU resultantes al testigo de seguridad 75'. Alternativamente, la aplicación de cliente de conductos 245 empaqueta respuestas APDU generadas por el testigo de seguridad 75' en los paquetes de comunicaciones de red para su transmisión a través de la red 65 hacia el sistema de ordenador.

La disposición de comunicaciones de conductos de APDU se describe en la solicitud US en tramitación con la

presente, de cesión conjunta, n.º de serie 09/844.246, presentada por primera vez el 30 de abril de 2001, titulada "Method and System for Establishing a Remote Connection to a Personal Security Device", y que se incorpora a la presente memoria como referencia.

En relación con la figura 2D, se muestra otra forma de realización de la invención en la que se establece una primera conexión de comunicaciones segura entre el testigo de seguridad y un primer sistema de ordenador CS 105 usando un primer conjunto de par de claves simétricas Ksys'[ID] 205', Ksys[ID], y se establece una segunda conexión segura entre el testigo de seguridad y un segundo sistema de ordenador CS' 105' usando un segundo conjunto de par de claves simétricas Ksys'[Idx] 210', Ksys[Idx] 210 a través de la red. Esta forma de realización ilustra que se pueden autenticar múltiples sistemas de ordenador usando el dispositivo remoto inteligente IRD 110. Adicionalmente, se pueden obtener privilegios de acceso a la red enviando un mensaje de autenticación AM 270 desde el primer sistema de ordenador CS 105 a un servidor de autenticación AS 250 tras completar satisfactoriamente la transacción de autenticación de dos factores.

La invención permite que el usuario envíe su CSP en forma de una muestra biométrica al testigo de seguridad 75' por medio de la conexión de comunicaciones segura. Se proporciona un escáner biométrico 280 en el segundo sistema de ordenador CS' 105' que está conectado de forma segura e inalámbrica al testigo de seguridad a través de la red 65'. El escáner biométrico 280 está asociado a otro sistema de ordenador.

Tras completarse satisfactoriamente la transacción de autenticación de dos factores, al usuario se le proporciona un retorno sonoro 260 o visual 255. El retorno sonoro 260 o visual 255 se puede proporcionar en uno de entre los sistemas de ordenador CS 105, CS' 105 y el dispositivo remoto inteligente IRD 110, o en ambos elementos.

Por último, en la figura 3 se muestra un diagrama de flujo de las etapas principales implicadas en la implementación de esta invención. El proceso es iniciado 300 por un usuario en posesión de un dispositivo remoto inteligente equipado con un testigo de seguridad. El dispositivo remoto inteligente establece una conexión de comunicaciones ad hoc con un sistema de ordenador habilitado para testigos de seguridad 305. El usuario ejecuta una aplicación de autenticación remota instalada en el dispositivo remoto inteligente, que provoca el envío de un mensaje de solicitud de acceso al sistema de ordenador 310 si fuera necesario para transitar por una pasarela de red o un punto de acceso, e invoca un método alternativo de autenticación que permite que el dispositivo remoto inteligente emule un dispositivo periférico de seguridad local conectado al sistema de ordenador.

Al mismo tiempo o después de esto, la aplicación de autenticación remota invita al usuario a que proporcione su parámetro de seguridad crítico (CSP) 315. El parámetro de seguridad crítico se introduce desde otro sistema de ordenador en el procesado de comunicaciones con el dispositivo remoto inteligente. A continuación, se lleva a cabo una transacción de autenticación en la cual el usuario se autentica con respecto al testigo de seguridad usando el CSP 320 proporcionado.

Si la transacción de autenticación no resulta satisfactoria 325, el procesado finaliza 340. Si la transacción de autenticación resulta satisfactoria 325, al usuario se le permite acceder a por lo menos un recurso seguro 335. Opcionalmente, al usuario se le proporciona un retorno sensorial 330 que le informa sobre la transacción de autenticación satisfactoria. Además, en las formas de realización de la invención que utilizan claves simétricas que tienen identificadores de sesión exclusivos asignados por el testigo de seguridad, las claves simétricas se pueden establecer como sustitutos temporales de CSPs autenticados. El procesado de la transacción de autenticación remota finaliza tras completarse satisfactoriamente 340.

Las formas de realización descritas anteriormente de la invención se proporcionan como ilustraciones y descripciones. No pretenden limitar la invención a la forma precisa descrita. En particular, se contempla que la implementación funcional de la invención descrita en la presente se pueda implementar de manera equivalente en hardware, software, microprogramas, y/u otros componentes funcionales o bloques constructivos disponibles. No se pretende imponer ninguna limitación específica a un entorno operativo de módulo criptográfico particular. A la luz de las enseñanzas anteriores son posibles otras variantes y formas de realización, y no se pretende que esta Descripción Detallada limite el alcance de la invención, sino que, por el contrario, se consideren las reivindicaciones que se presentan a continuación en la presente memoria.

REIVINDICACIONES

1. Método para acceder a un sistema de ordenador habilitado para testigos de seguridad (105) usando un dispositivo remoto inteligente (110) como interfaz de comunicaciones para un testigo de seguridad (75'), que comprende las etapas de:

a. establecer una conexión de comunicaciones inalámbricas entre dicho dispositivo remoto inteligente (110) y dicho sistema de ordenador habilitado para testigos de seguridad (105),

b. ejecutar una aplicación de autenticación remota (175') instalada en el dispositivo remoto inteligente (110), que invoca un método de autenticación que permite que el dispositivo remoto inteligente emule un dispositivo periférico de seguridad local conectado localmente al sistema de ordenador habilitado para testigos de seguridad (105) que permite que un usuario se autentique remotamente con respecto al sistema de ordenador habilitado para testigos de seguridad (105) como si el usuario fuera local con respecto al sistema de ordenador habilitado para testigos de seguridad (105), y

c. invitar al usuario a que proporcione un parámetro de seguridad crítico (188) que, a continuación, se envía a dicho testigo de seguridad (75') acoplado operativamente a dicho dispositivo remoto inteligente (110), en el que dicho parámetro de seguridad crítico se proporciona desde otro sistema de ordenador y se envía a dicho testigo de seguridad a través de otra conexión inalámbrica establecida entre dicho dispositivo remoto inteligente y dicho otro sistema de ordenador, y

d. autenticar dicho parámetro de seguridad crítico (188) mediante dicho testigo de seguridad (75') de manera que el usuario es autenticado con respecto al testigo de seguridad (75'), y

e. tras completarse satisfactoriamente la transacción de autenticación con respecto al testigo de seguridad (75'), permitir que el usuario acceda a por lo menos un recurso seguro asociado al sistema de ordenador habilitado para testigos de seguridad (105),

en el que se proporciona a dicho usuario un retorno sonoro o visual a continuación de una autenticación satisfactoria.

2. Método según la reivindicación 1, que incluye además la etapa de enviar un mensaje de solicitud de acceso desde dicho dispositivo remoto inteligente (110) a dicho sistema de ordenador habilitado para testigos de seguridad (105) con el fin de iniciar el establecimiento de dicha conexión de comunicaciones inalámbricas.

3. Método según cualquiera de las reivindicaciones anteriores, que incluye además la etapa de establecer múltiples conexiones lógicas con múltiples sistemas de ordenador con el fin de autenticar los múltiples sistemas de ordenador usando el dispositivo remoto inteligente (110).

4. Método según cualquiera de las reivindicaciones anteriores, en el que dicho mensaje de solicitud de acceso incluye por lo menos un primer identificador asociado a dicho dispositivo remoto inteligente (110), un segundo identificador asociado a dicho testigo de seguridad (75') o una dirección de red inalámbrica asociada a dicho dispositivo remoto inteligente.

5. Método según cualquiera de las reivindicaciones anteriores, en el que la etapa de establecer una conexión de comunicaciones inalámbricas incluye además la etapa de autenticar por lo menos dicho testigo de seguridad (75') con respecto a dicho sistema de ordenador habilitado para testigos de seguridad (105).

6. Método según cualquiera de las reivindicaciones anteriores, en el que dicha conexión de comunicaciones inalámbricas entre dicho dispositivo remoto inteligente (110) y dicho sistema de ordenador habilitado para testigos de seguridad (105), incluye por lo menos un protocolo de comunicaciones seguras que comprende la capa de conexión segura, la seguridad de capa de transporte, la seguridad del protocolo de internet o una sesión de mensajería segura.

7. Método según cualquiera de las reivindicaciones anteriores, en el que dicha conexión de comunicaciones inalámbricas entre dicho dispositivo remoto inteligente (110) y dicho sistema de ordenador habilitado para testigos de seguridad (105) comprende una conexión inalámbrica óptica, una conexión inalámbrica de radiofrecuencia, o una combinación de las mismas.

8. Método según cualquiera de las reivindicaciones anteriores, en el que dicha conexión de comunicaciones inalámbricas se puede iniciar o bien desde dicho dispositivo remoto inteligente (110) o bien desde dicho sistema de ordenador habilitado para testigos de seguridad (105).

9. Método según cualquiera de las reivindicaciones anteriores, en el que, a través de dicho dispositivo remoto inteligente (110) por medio de una primera interfaz, se intercambia información entre dicho testigo de seguridad (75')

y dicho sistema de ordenador habilitado para testigos de seguridad remoto (105), y se recibe y se encamina un parámetro de seguridad crítico hacia dicho testigo de seguridad (75') mediante dicho dispositivo remoto inteligente (110) por medio de una segunda interfaz.

10. Método según cualquiera de las reivindicaciones anteriores, en el que dicho parámetro de seguridad crítico se proporciona desde dicho sistema de ordenador habilitado para testigos de seguridad (105) y se envía a través de dicha conexión de comunicaciones inalámbricas a dicho testigo de seguridad.

11. Método según cualquiera de las reivindicaciones anteriores 1 a 10, en el que dicho parámetro de seguridad crítico se proporciona desde dicho dispositivo remoto inteligente (110) y se envía directamente a dicho testigo de seguridad (75').

12. Sistema para acceder a un sistema de ordenador habilitado para testigos de seguridad (105) usando un dispositivo remoto inteligente (110) como interfaz de comunicaciones para un testigo de seguridad (75'), que comprende dicho sistema de ordenador habilitado para testigos de seguridad (105), dicho dispositivo remoto inteligente (110), dicho testigo de seguridad (75') y otro sistema de ordenador, incluyendo el dispositivo remoto inteligente (110) unos medios para:

- comunicarse con el sistema de ordenador habilitado para testigos de seguridad (105) a través de una conexión de comunicaciones inalámbricas,
- acoplar operativamente dicho testigo de seguridad (75') a dicho dispositivo remoto inteligente (110),
- recibir un parámetro de seguridad crítico proporcionado por un usuario; y
- estando equipado dicho dispositivo remoto inteligente (110) para invocar un método alternativo de autenticación que permite que el dispositivo remoto inteligente emule un dispositivo periférico de seguridad local conectado localmente a dicho sistema de ordenador habilitado para testigos de seguridad (105);

incluyendo dicho testigo de seguridad (75') unos medios para:

- recibir un parámetro de seguridad crítico (188) asociado a dicho usuario,
- autenticar dicho parámetro de seguridad crítico (188); e

incluyendo dicho sistema de ordenador habilitado para testigos de seguridad (105) unos medios para:

- utilizar dicho dispositivo remoto inteligente (110) como dicho dispositivo periférico de testigo de seguridad;
- permitir a dicho usuario acceder a por lo menos un recurso seguro tras una autenticación satisfactoria de dicho parámetro de seguridad crítico (188) y la autenticación remota del usuario con respecto al sistema de ordenador habilitado para testigos de seguridad (105) como si el usuario fuera local con respecto al sistema de ordenador habilitado para testigos de seguridad (105); y
- proporcionar a dicho usuario un retorno sonoro o visual a continuación de una autenticación satisfactoria;

proporcionando dicho otro sistema de ordenador dicho parámetro de seguridad crítico y enviándolo a dicho testigo de seguridad a través de otra conexión inalámbrica establecida entre dicho dispositivo remoto inteligente y dicho otro sistema de ordenador.

13. Sistema según la reivindicación 12, en el que dicho dispositivo remoto inteligente (110) incluye además unos medios para enviar un mensaje de solicitud de acceso a dicho sistema de ordenador habilitado para testigos de seguridad (105).

14. Sistema según la reivindicación 13, en el que dicho sistema de ordenador habilitado para testigos de seguridad (105) incluye además un agente de comunicaciones (160) que puede detectar un mensaje entrante de solicitud de acceso e invocar un método alternativo de autenticación de usuario.

15. Sistema según cualquiera de las reivindicaciones anteriores 13 a 14, en el que dicho mensaje de solicitud de acceso incluye por lo menos un primer identificador asociado a dicho dispositivo remoto inteligente, un segundo identificador asociado a dicho testigo de seguridad (75') o una dirección de red inalámbrica asociada a dicho dispositivo remoto inteligente (110).

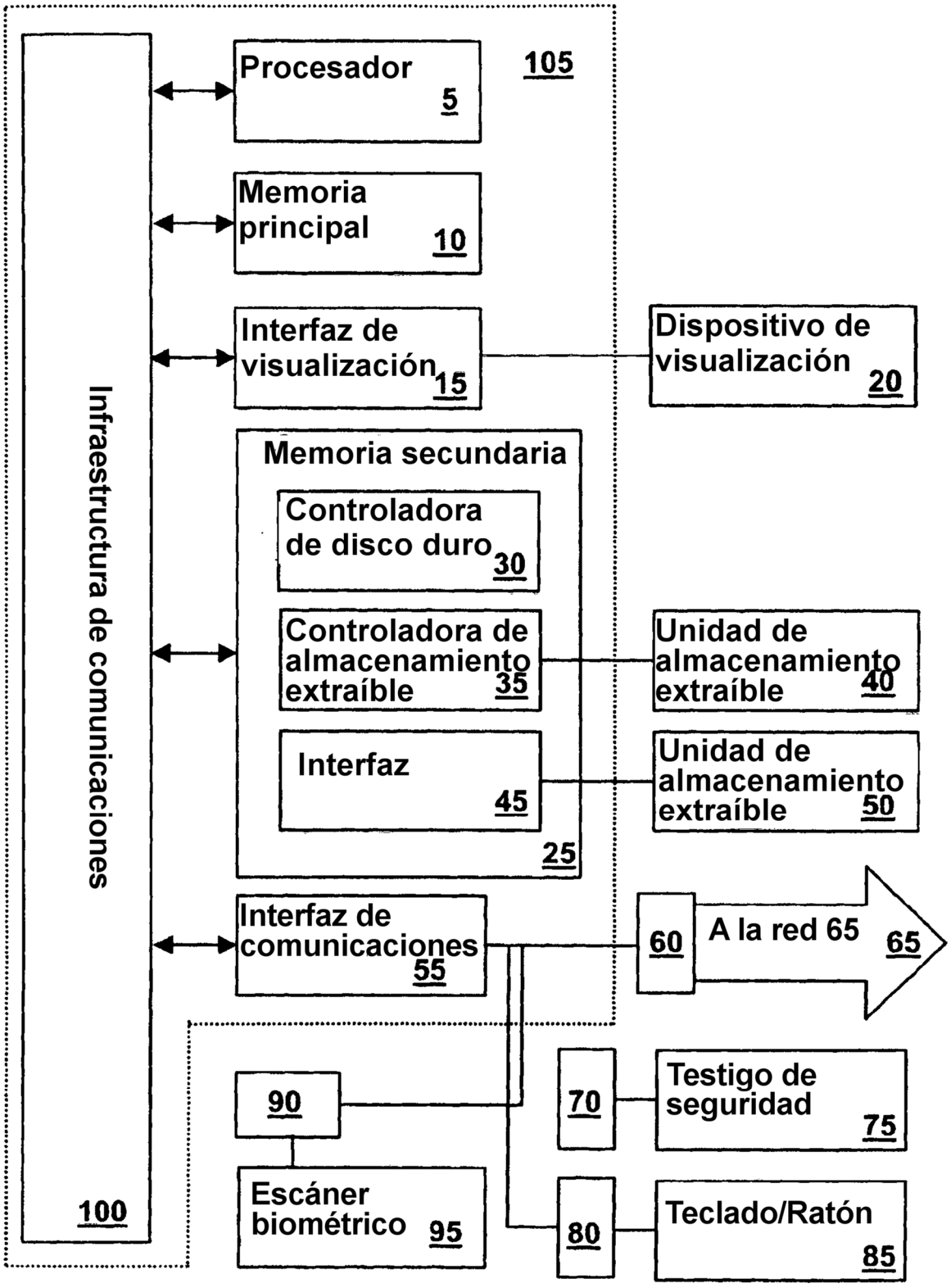
Procesador
5
105
Memoria principal
10
Interfaz de visualización
15
Dispositivo de visualización
20
Memoria secundaria
Controladora de disco duro
30
Controladora de almacenamiento extraíble
35
Unidad de almacenamiento extraíble
40
Interfaz
45
Unidad de almacenamiento extraíble
50
25
Infraestructura de comunicaciones
Interfaz de comunicaciones
55
60
A la red 65
65
90
70
Testigo de seguridad
75
Escáner biométrico
95
80
Teclado/Ratón
85
100

FIG. 1

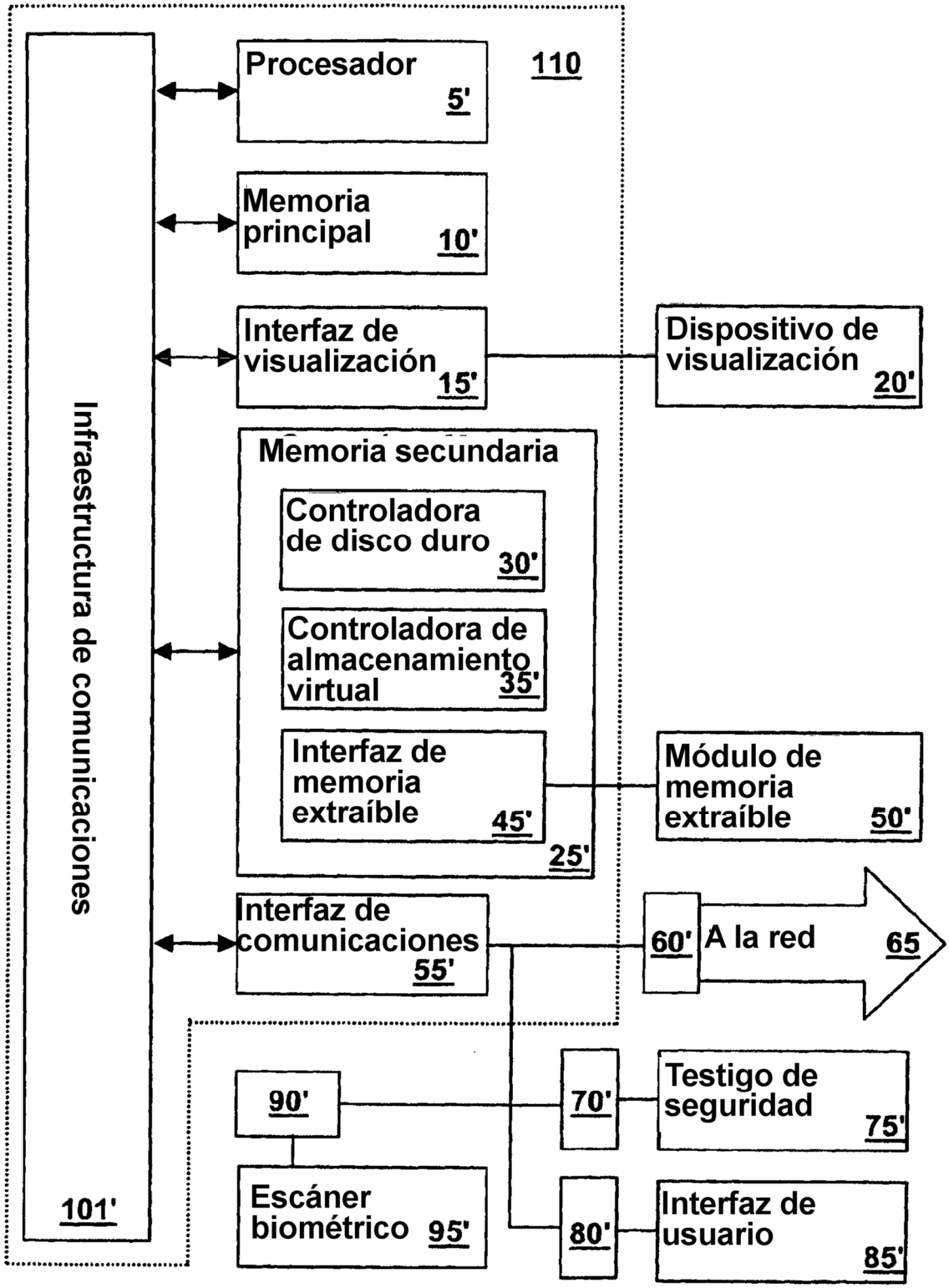
Procesador
5'
110
Memoria principal
10'
Interfaz de visualización
15'
Dispositivo de visualización
20'
Memoria secundaria
Controladora de disco duro
30'
Controladora de almacenamiento virtual
35'
Interfaz de memoria extraíble
45'
25'
Módulo de memoria extraíble
50'
Interfaz de comunicaciones
55'
60'
A la red
65
Infraestructura de comunicaciones
101'
90'
70'
Testigo de seguridad
75'
Escáner biométrico
95'
80'
Interfaz de usuario
85'

FIG. 1A

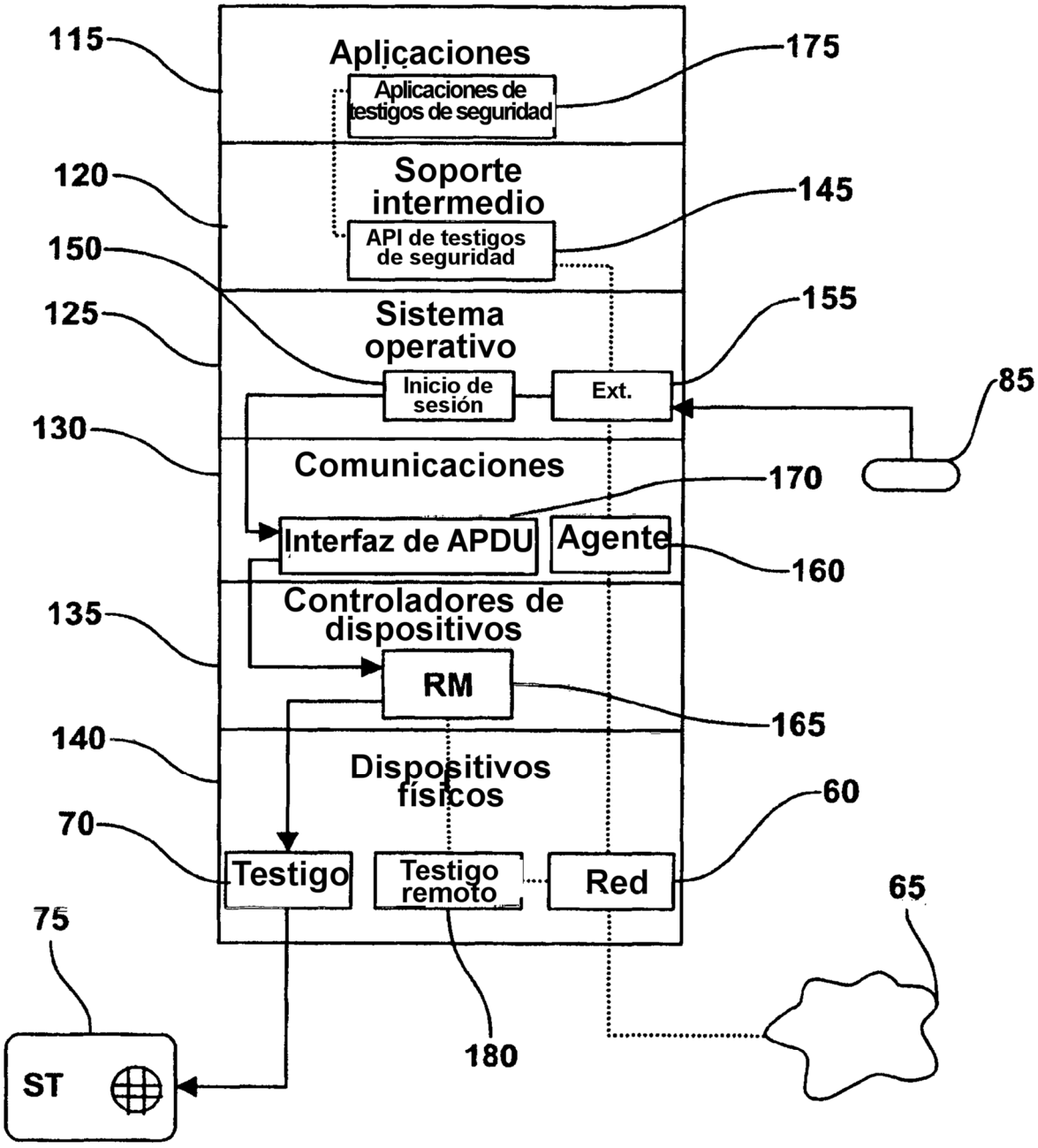
115
Aplicaciones
175
Aplicaciones de testigos de seguridad
120
Soporte intermedio
145
API de testigos de seguridad
150
125
Sistema operativo
155
Inicio de sesión
Ext.
85
130
Comunicaciones
170
Interfaz de APDU
Agente
160
135
Controladores de dispositivos
RM
165
140
Dispositivos físicos
60
70
Testigo
Testigo remoto
Red
65
75
ST
180

FIG.1B-1

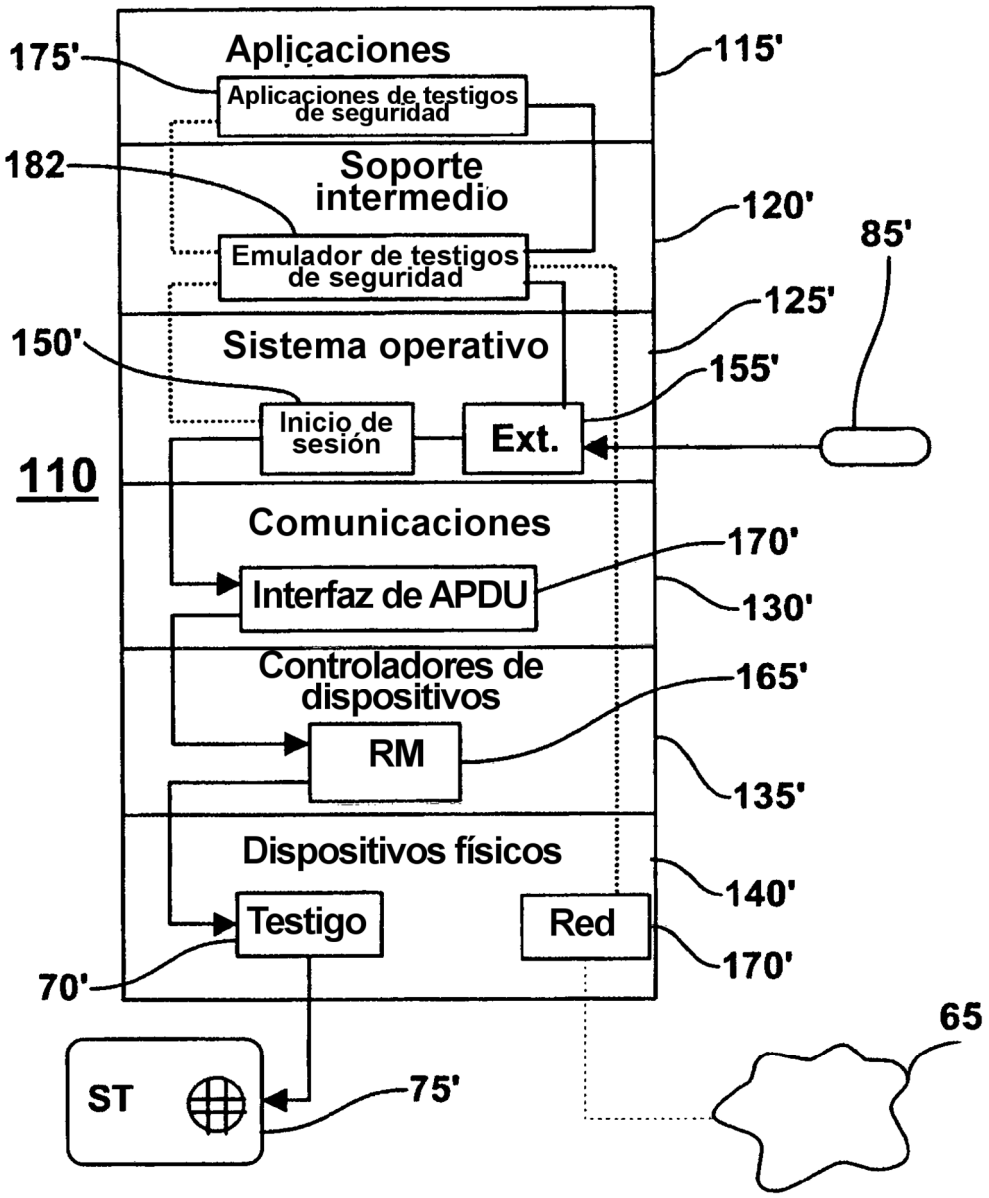
175'
Aplicaciones
115'
Aplicaciones de testigos de seguridad
182
Soporte intermedio
120'
85'
Emulador de testigos de seguridad
125'
150'
Sistema operativo
155'
Inicio de sesión
Ext.
110
Comunicaciones
170'
Interfaz de APDU
130'
Controladores de dispositivos
165'
RM
135'
Dispositivos físicos
140'
Testigo
Red
170'
70'
65
ST
75'

FIG.1B-2

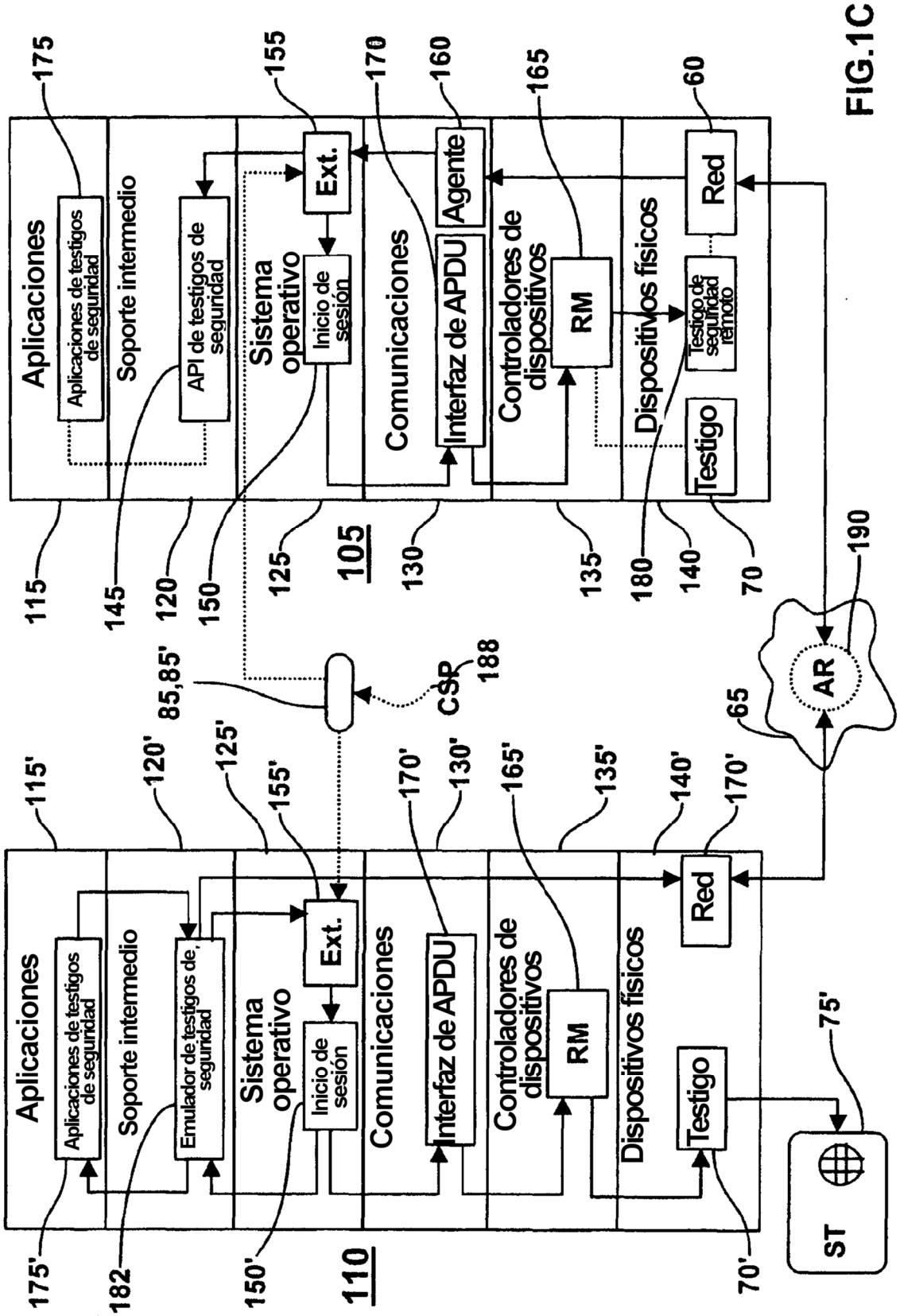
Aplicaciones
Aplicaciones de testigos de seguridad
Soporte intermedio
API de testigos de seguridad
Sistema operativo
Inicio de sesión
Ext.
Comunicaciones
Interfaz de APDU
Agente
Controladores de dispositivos
RM
Dispositivos físicos
Testigo
Testigo de seguridad remoto
Red
105
110
Emulador de testigos de seguridad
CSP
AR
ST
115
120
125
130
135
140
145
150
155
160
165
170
175
180
182
188
190
65
70
75'
85,85'
115'
120'
125'
130'
135'
140'
150'
155'
165'
170'
175'

FIG.1C

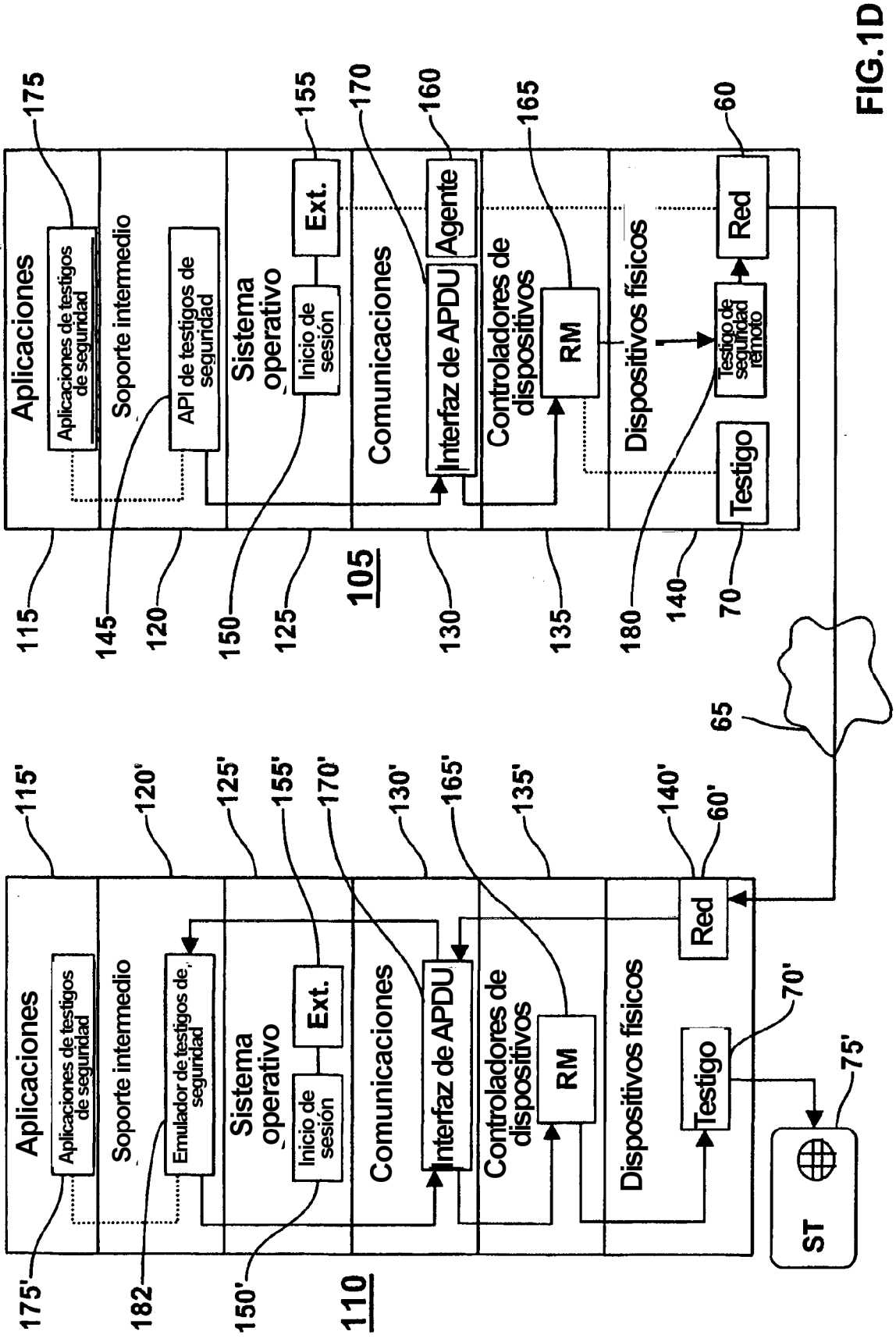
Aplicaciones
Aplicaciones de testigos de seguridad
Soporte intermedio
API de testigos de seguridad
Sistema operativo
Inicio de sesión
Ext.
Comunicaciones
Interfaz de APDU
Agente
Controladores de dispositivos
RM
Dispositivos físicos
Testigo
Testigo de seguridad remoto
Red
105
115
145
120
150
125
130
135
180
140
70
175
155
170
160
165
60
65
110
115'
120'
125'
155'
170'
130'
165'
135'
140'
60'
175'
182
150'
Emulador de testigos de seguridad
70'
75'
ST

FIG.1D

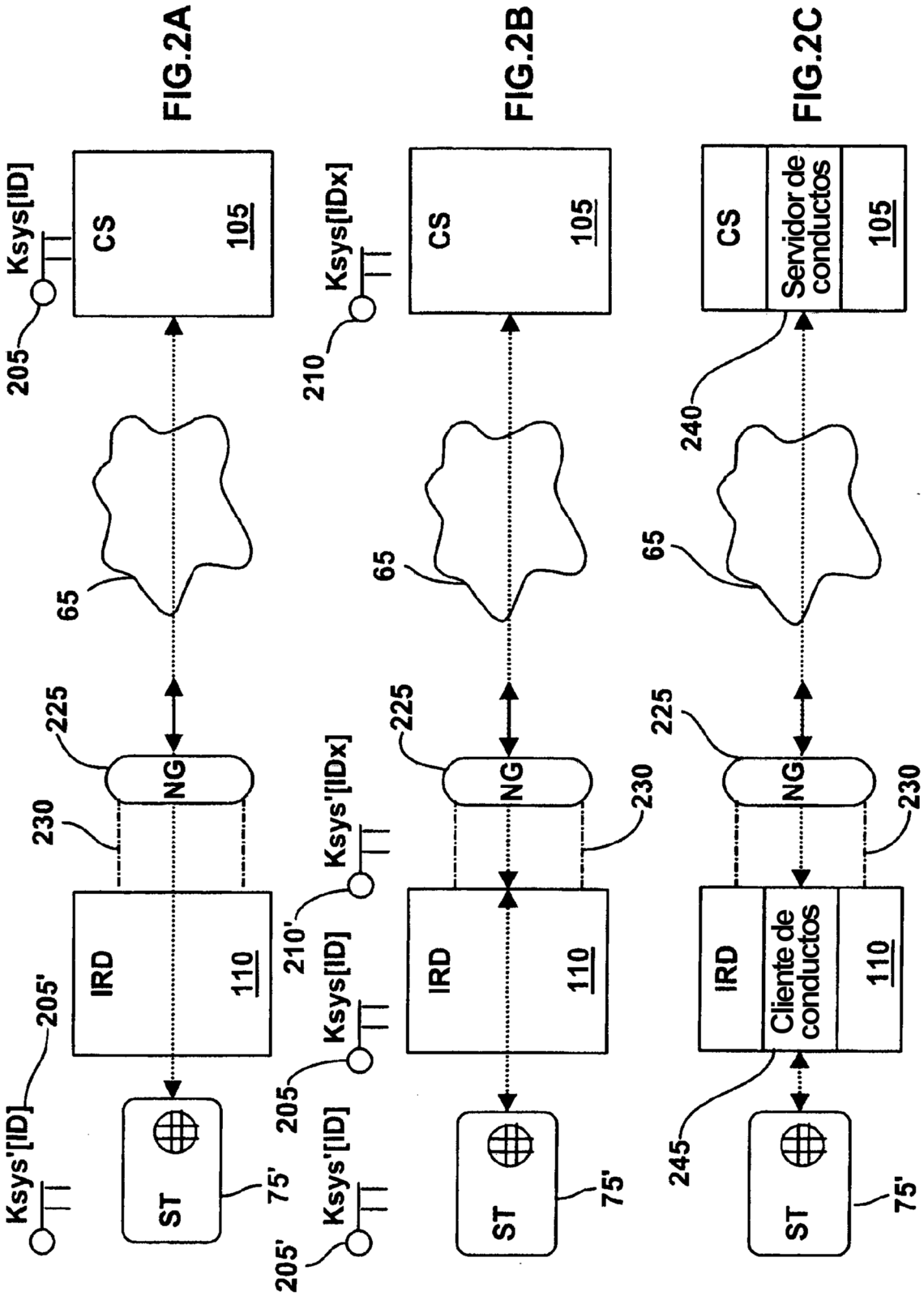
FIG.2A
Ksys[ID]
205
CS
105
65
225
NG
230
IRD
110
205'
Ksys'[ID]
ST
75'
205'
Ksys'[ID]
FIG.2B
Ksys[IDx]
210
CS
105
65
225
NG
230
210'
Ksys'[IDx]
IRD
110
205
Ksys[ID]
ST
75'
FIG.2C
CS
Servidor de conductos
105
240
65
225
NG
230
IRD
Cliente de conductos
110
245
ST
75'

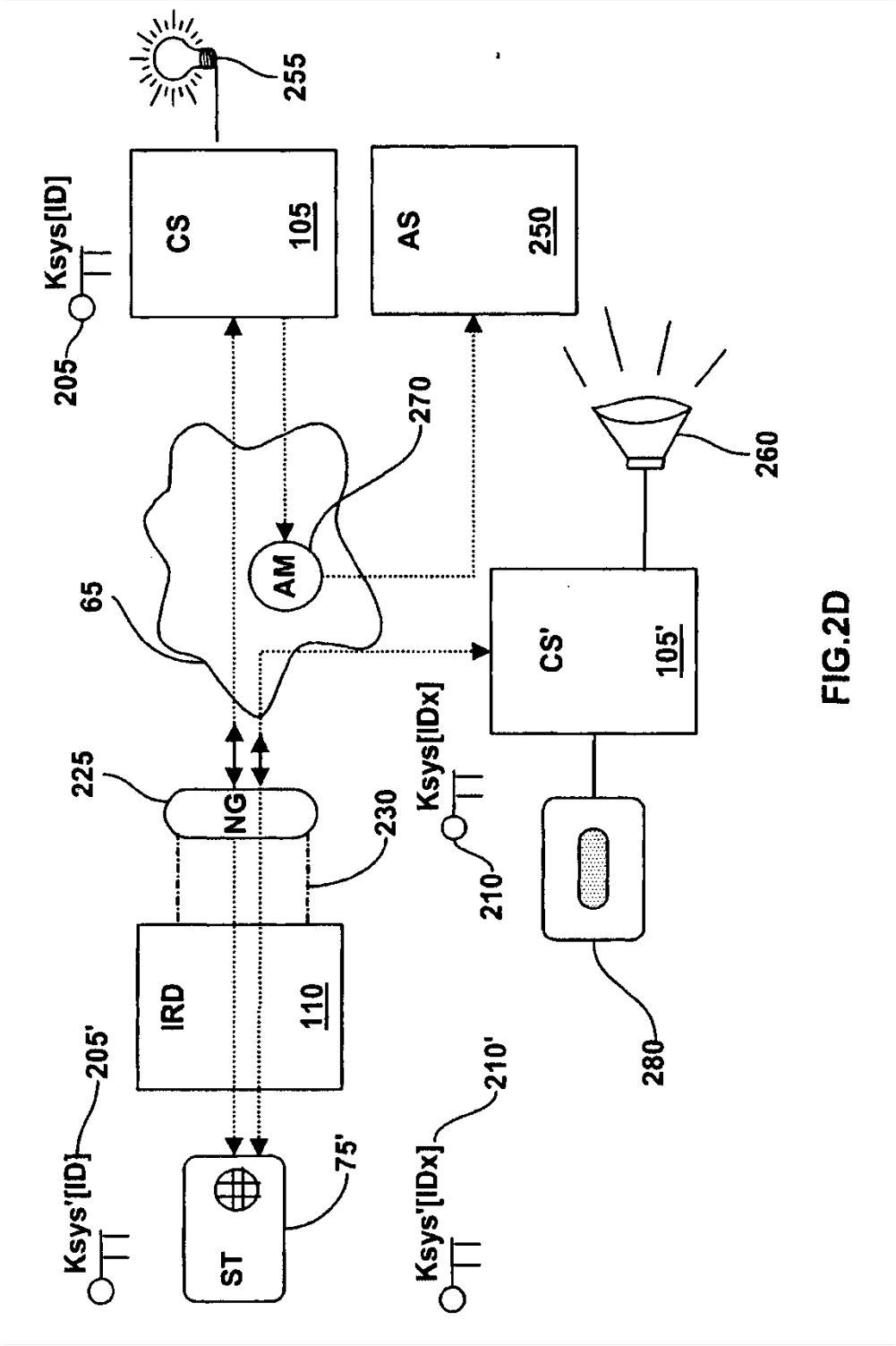
255
CS
105
AS
250
Ksys[ID]
205
270
260
AM
65
CS'
105'
Ksys[IDx]
225
NG
230
210
IRD
110
205'
280
Ksys'[ID]
75'
ST
210'
Ksys'[IDx]

FIG.2D

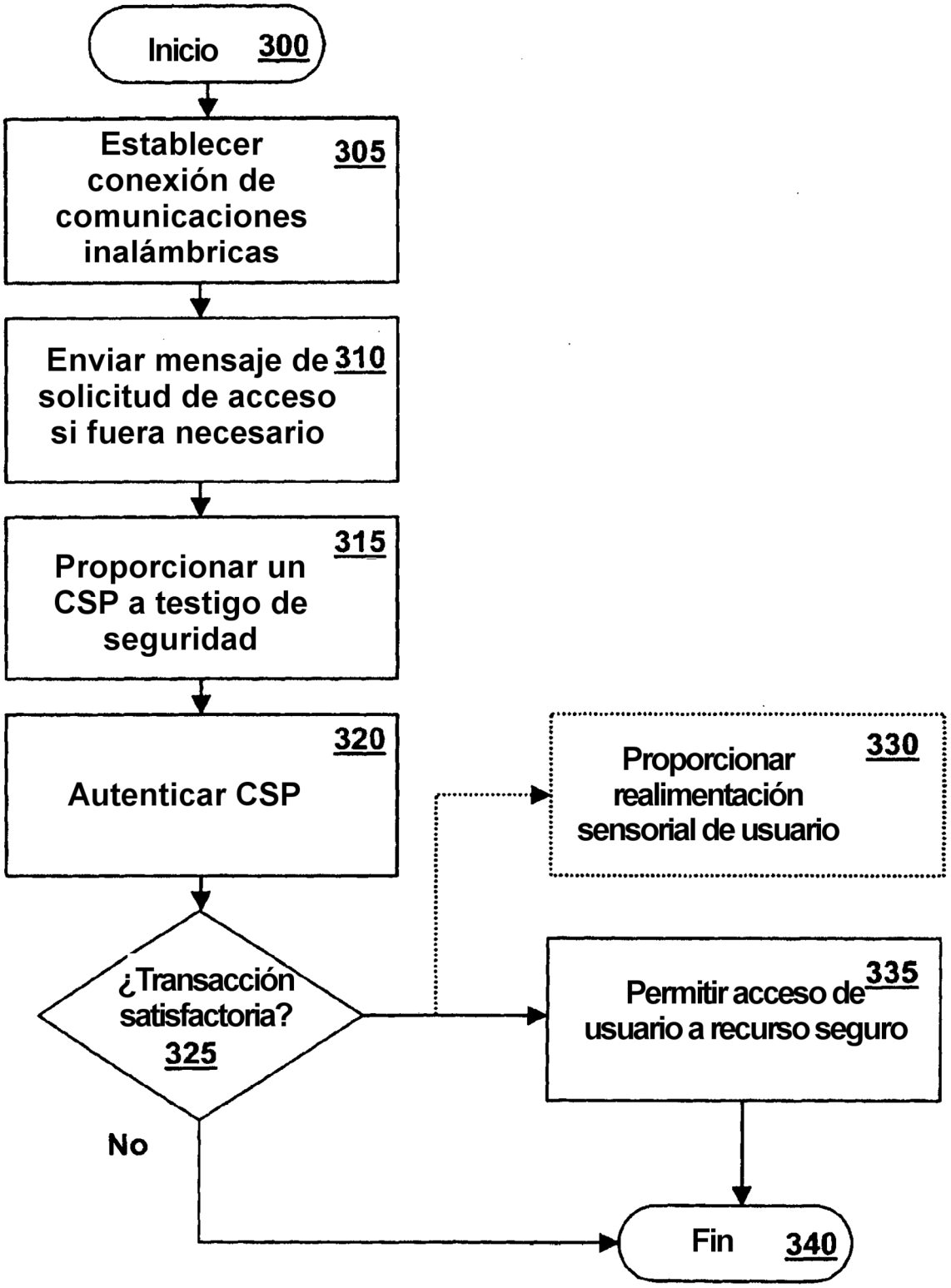
Inicio 300
Establecer conexión de comunicaciones inalámbricas 305
Enviar mensaje de solicitud de acceso si fuera necesario 310
Proporcionar un CSP a testigo de seguridad 315
Autenticar CSP 320
Proporcionar realimentación sensorial de usuario 330
¿Transacción satisfactoria? 325
Permitir acceso de usuario a recurso seguro 335
No
Fin 340

FIG. 3