(19) OFICINA ESPAÑOLA DE PATENTES Y MARCAS

ESPAÑA

(11) Número de publicación: **2 681 919**

(51) Int. CI.:

H04L 29/06 (2006.01)
G06F 21/33 (2013.01)

(12) TRADUCCIÓN DE PATENTE EUROPEA T3

(86) Fecha de presentación y número de la solicitud internacional: **22.06.2006 PCT/US2006/024364**

(87) Fecha y número de publicación internacional: **15.02.2007 WO07018768**

(96) Fecha de presentación y número de la solicitud europea: **22.06.2006 E 06785372 (1)**

(97) Fecha y número de publicación de la concesión europea: **02.05.2018 EP 1917616**

(54) Título: **Gestión del certificado de seguridad**

(30) Prioridad:

28.07.2005 US 191622

(45) Fecha de publicación y mención en BOPI de la traducción de la patente:
17.09.2018

(73) Titular/es:

THE BOEING COMPANY (100.0%)
100 North Riverside Plaza
Chicago, IL 60606-1596, US

(72) Inventor/es:

ALLEN, DAVID, L.;
SAVAGE, DAVID, E.;
LOVING, KENT;
POLLOCK, BRUCE, K.;
CLOUTIER, JOHN, M. y
SMITH, DENISE, M.

(74) Agente/Representante:

CARVAJAL Y URQUIJO, Isabel

DESCRIPCIÓN

Gestión del certificado de seguridad

Campo de la invención

La invención se relaciona en general con la comunicación entre una plataforma móvil y un centro de operaciones central de la plataforma móvil. Más particularmente, la invención se relaciona con establecer un enlace de comunicaciones seguro entre un sistema informático a bordo de la plataforma móvil y un sistema informático en un centro de operaciones central del proveedor de la plataforma móvil.

Antecedente de la invención

La evolución de las comunicaciones del Protocolo de Internet (IP) inalámbricas para plataformas móviles, tales como aeronaves, autobuses, trenes y barcos, ha introducido desafíos significativos. Aunque dicha comunicación proporciona una interfaz de datos flexible y de banda ancha, plantea problemas de seguridad informática. Por ejemplo, las aeronaves históricamente han utilizado el sistema de reporte/direccionamiento de las comunicaciones de la aeronave (ACARS) para comunicarse entre las aeronaves y entre las aeronaves y el sistema terrestre. Sin embargo, normalmente ha habido poca o ninguna seguridad asociada con este método de comunicación. Además, la tecnología de comunicación IP introduce el potencial de acceso no autorizado a datos confidenciales almacenados en sistemas de plataforma móvil, tales como una bolsa de vuelo electrónica de una aeronave, y/o sistemas centrales de proveedor de plataforma móvil, tales como un sistema central para una aerolínea. Tradicionalmente, para los sistemas con base en protocolos de internet, el problema del uso no autorizado se ha resuelto mediante la administración de certificados de seguridad que se intercambian entre "usuarios de confianza". En general, el extremo "móvil" del "entorno de confianza" es un ordenador con un usuario interactivo que puede participar en la aceptación de dichos certificados de seguridad. La actualización y el intercambio de dichos certificados se diseñaron inicialmente para usuarios de ordenadores dedicados e involucraron interacciones periódicas y específicas de un usuario a intervalos no planificados.

Sin embargo, en un entorno de plataforma móvil, el extremo "móvil" es a menudo un equipo informático o un sistema informático de la plataforma móvil. La tripulación de la plataforma móvil a menudo tiene un conocimiento limitado de la seguridad informática y los requisitos de carga de trabajo que hacen que la implementación de sistemas de certificados de seguridad "estándar" sea inviable a partir del punto de vista operativo. En muchos casos, el equipo informático de la plataforma móvil o los componentes del sistema informático pueden intercambiarse o reemplazarse. Por ejemplo, algunas aerolíneas utilizan la "agrupación de piezas de repuesto", lo cual permite a una aerolínea tomar prestado equipo informático de otra aerolínea. Las tripulaciones de vuelo y los equipos de mantenimiento realizan estos intercambios durante tiempos de respuesta cortos y, por lo general, no están autorizados para implementar un intercambio interactivo de certificados de seguridad entre el equipo informático recién instalado y el sistema informático central. El hardware criptográfico que podría usarse para intercambiar certificados de seguridad automáticamente entre los equipos informáticos recién instalados y el ordenador central implicaría "estacionar" la plataforma móvil durante períodos prolongados y requeriría considerables costes de mano de obra para instalar dicho hardware. Adicionalmente, una solicitud dinámica e interactiva del usuario para que una plataforma móvil acepte un nuevo certificado podría tener un gran tiempo de carga de trabajo y depender del conocimiento del usuario, que puede ser limitado, haciendo inviables dichas solicitudes dinámicas e interactivas.

El documento GB 2404126A se relaciona con enlaces de comunicaciones seguros en los que se usan técnicas criptográficas asimétricas para establecer un enlace seguro. El enlace seguro se establece entre el remitente y el destinatario mediante el envío de un mensaje que incluye un número secreto, que se utilizará para la criptografía simétrica, con el mensaje firmado digitalmente utilizando una clave privada del remitente.

La WO 2005/031545 A1 divulga un sistema para otorgar acceso a un objeto con base en ordenador. Se proporciona una tarjeta de memoria que tiene un procesador de código de programa, en el cual se almacenan al menos una clave pública y privada asignada a la tarjeta de memoria.

International Business Machines Corporation: "A strong client-server mutual authentication scheme", divulgación de la investigación, Publicaciones Mason, Hampshire, GB, vol. 417, no. 87, Enero de 1999 (1999-01), XP007123837, ISSN: 0374-4353 divulga un esquema de autenticación mutua entre el cliente y el servidor. Un cliente y un servidor se autentican mutuamente con base en un cripto-sistema simétrico con una clave generada por un algoritmo de generación de clave conocido por el cliente y el servidor.

Por lo tanto, es deseable implementar una solución de intercambio de certificados inalámbrica segura y automatizada que establezca un enlace seguro entre un sistema informático de plataforma móvil y un sistema informático remoto para garantizar que solo los usuarios autorizados puedan acceder a datos confidenciales almacenados en cualquiera de los sistemas.

Breve resumen de la invención

Una invención se define en las reivindicaciones independientes. Las características opcionales se definen en las reivindicaciones dependientes.

Diversas realizaciones de la presente invención proporcionan un sistema y método para establecer un enlace seguro autenticado mutuamente entre un sistema de plataforma móvil y un sistema remoto. Más particularmente, en diversas realizaciones, la invención proporciona un sistema y método para generar de forma remota y dinámica certificados de seguridad que se pueden usar para establecer un enlace seguro entre un sistema de plataforma móvil y un sistema remoto. Se crea una infraestructura de clave pública, donde el propietario o el proveedor de la plataforma móvil implementa una red segura, la cual incluye una autoridad de certificación segura y firmada por sí misma. Esta autoridad de certificación es explícitamente confiable en todos los sistemas informáticos a los cuales los dispositivos móviles deben comunicarse de forma segura.

En general, una red o sistema con base en ordenador de proveedor de plataforma móvil genera y firma digitalmente un certificado estático. El certificado estático se almacena al menos en un sistema informático central (CCS) que puede incluir el sistema informático del proveedor de la plataforma móvil o conectado comunicativamente al mismo. El certificado estático se emite al menos a un sistema de ordenador a bordo (OCS) de la plataforma móvil y el OCS utiliza el certificado estático para generar un certificado dinámico y firmar digitalmente el certificado dinámico con el certificado estático. Cuando se desea un enlace seguro entre el OCS y el CCS, el certificado dinámico se transmite al CCS a través de un enlace de comunicaciones inicial, en general abierto, entre el OCS y el CCS. Los protocolos criptográficos bien conocidos se utilizan para autenticar mutuamente los puntos finales y luego configurar una ruta segura para intercambiar información.

Al recibir el certificado dinámico, el CCS verifica que el certificado dinámico proviene de una fuente confiable, es decir, que el certificado dinámico está firmado con el certificado estático compartido. Si se verifica que el certificado dinámico fue enviado por una fuente confiable, el CCS envía un certificado dinámico de retorno firmado digitalmente con el certificado estático, también conocido como el certificado raíz, al OCS. Luego, el OCS verifica si el certificado dinámico de devolución procede del CCS, es decir, si el certificado dinámico de devolución está firmado con un certificado de confianza, por ejemplo el certificado estático. De ser así, se establece un enlace seguro mutuamente autenticado entre el OCS y el CCS que puede utilizarse como una red privada virtual (VPN) entre el OCS y el CCS.

Las características, funciones y ventajas de la presente invención se pueden lograr independientemente en diversas realizaciones de la presente invención o se pueden combinar en aún otras realizaciones.

Breve descripción de los dibujos

La presente invención se comprenderá más completamente a partir de la descripción detallada y los dibujos adjuntos, en donde;

La Figura 1 es un diagrama de bloques de un sistema de comunicaciones de plataforma móvil (MPCS), de acuerdo con diversas realizaciones de la presente invención; y

La Figura 2 es un diagrama de secuencia que ilustra un método para establecer un enlace seguro entre al menos un sistema informático a bordo y al menos un sistema informático central (que se muestra en la Figura 1), de acuerdo con la presente invención.

Los numerales de referencia correspondientes indican partes correspondientes a lo largo de las diversas vistas de los dibujos.

Descripción detallada de la invención

La siguiente descripción de las realizaciones preferidas es meramente de naturaleza de ejemplo y de ninguna manera pretende limitar la invención, su aplicación o usos. Adicionalmente, las ventajas proporcionadas por las realizaciones preferidas, como se describe a continuación, son de naturaleza de ejemplo y no todas las realizaciones preferidas proporcionan las mismas ventajas o el mismo grado de ventajas.

La Figura 1 es un diagrama de bloques de un sistema 10 de comunicaciones de plataforma móvil (MPCS), de acuerdo con diversas realizaciones de la presente invención. El MPCS 10 incluye al menos un sistema 14 de ordenador a bordo (OCS), a bordo de una o más plataformas 18 móviles y al menos un sistema 20 de ordenador central (CCS) ubicado remotamente a partir del OCS 14 y configurado para comunicarse con el OCS 14. Las comunicaciones entre el OCS 14 y el CCS 20 se pueden establecer utilizando cualquier enlace, protocolo o servicio adecuado de comunicaciones por cable o inalámbrico. Por ejemplo, en diversas realizaciones, se establece una conexión inalámbrica entre el OCS 14 y el CCS 20 usando GPRS (Servicio General de Radio por Paquetes), VHF, comunicación inalámbrica IEEE 802.11 y/o redes de satélite que implementan Internet o protocolos ACARS^{SM} (Sistema de

Comunicaciones y Grabación de la Aeronave). El ACARS[SM] puede ser provisto por ARINC, Inc. de Annapolis, MD o SITA de Ginebra, Suiza.

El OCS 14 puede ser un sistema autónomo o un subsistema de cualquier otro sistema, red o componente a bordo de la plataforma 18 móvil. Por ejemplo, en diversas realizaciones, el OCS 14 es una ayuda de viaje electrónica utilizada por un operador de la plataforma 18 móvil para mejorar la facilidad y eficiencia de diversas tareas que el operador debe realizar durante el funcionamiento de la plataforma 18 móvil. Por ejemplo, la ayuda de viaje electrónica podría ser una "bolsa de vuelo electrónica (EFB)" empleada por algunas aerolíneas para ayudar a los pilotos durante el vuelo. Alternativamente, el OCS 14 puede ser un subsistema de una LAN a bordo o un sistema de control de plataforma móvil a bordo. Aunque la plataforma 18 móvil se ilustra como una aeronave, la invención no se limita a las aplicaciones de aeronaves. Es decir, la plataforma 18 móvil podría ser cualquier plataforma móvil tal como una aeronave, autobús, tren o barco.

El OCS 14 incluye un procesador 22 para ejecutar todas las funciones del OCS 14 y un dispositivo 26 de almacenamiento electrónico (ESD) para almacenar electrónicamente una primera porción 28A de una aplicación 28 de software de autenticación (ASA), y otras aplicaciones, datos, información y algoritmos. La primera porción 28A de la aplicación 28 software ASA se denominará aquí simplemente ASA1 28A. El OCS ESD 26 puede ser cualquier dispositivo mediano legible por ordenador adecuado para almacenar electrónicamente cosas tales como datos, información, algoritmos y/o programas de software ejecutables por el procesador 22 OCS. Por ejemplo, el OCS ESD 26 puede ser un disco duro, una Zip, una unidad CDRW, una memoria USB o cualquier otro dispositivo de almacenamiento electrónico. El OCS 14 incluye adicionalmente una pantalla 30 para ilustrar datos gráficos y de texto, formularios y otra información, y un dispositivo 34 de entrada tal como un teclado, mouse, lápiz o joystick para ingresar datos e información al OCS 14 para ser almacenados en el OCS ESD 26. Se debe entender que el procesador OCS, ESD, pantalla y dispositivo 22, 26, 30 y 34 de entrada pueden ser componentes de un sistema independiente con base en ordenador, es decir, el OCS 14, o componentes de un sistema más grande, tales como como una LAN a bordo o un sistema de control de plataforma móvil a bordo que colectivamente comprende el OCS 14. Alternativamente, el OCS 14 puede ser un sistema autónomo que se puede conectar a un sistema más grande, por ejemplo una LAN a bordo, de modo que diversos de los dispositivos de procesador OCS, ESD, pantalla y dispositivo 22, 26, 30 y 34 de entrada están incluidos en el OCS 14 independiente y otros están incluidos en el sistema más grande.

En general, el procesador OCS 22 ejecuta el ASA1 28A para establecer automáticamente un enlace de comunicaciones seguro con el CCS 20, como se describe a continuación. Como se usa aquí, el término automáticamente debe entenderse como un evento automático que se inicia, ocurre y es controlado por el OCS 14 y/o el CCS 20 sin intervención manual, es decir, con interacción o entrada por parte de una persona, por ejemplo el personal de la plataforma móvil, el personal de mantenimiento y/o el proveedor de la plataforma móvil. El CCS 20 incluye al menos un procesador 38, al menos una base 42 de datos, al menos una pantalla 46, al menos un dispositivo 50 de almacenamiento electrónico (ESD) y al menos un dispositivo 54 de entrada. La pantalla 46 CCS puede ser cualquier pantalla adecuada para visualizar presentando gráficos, texto y datos a un usuario del MPCS 10. El dispositivo 54 de entrada CCS puede ser cualquier dispositivo adaptado para ingresar datos y/o información en el CCS 20, por ejemplo un teclado, un ratón, un joystick, un lápiz óptico, un escáner, un dispositivo de video y/o un dispositivo de audio. El CCS ESD 50 puede ser cualquier dispositivo medio legible por ordenador adecuado para almacenar electrónicamente una segunda porción 28B del ASA 28, y otras cosas como datos, información y algoritmos y/o programas de software ejecutables por el procesador CCS 38. Por ejemplo, el CCS ESD 50 puede ser un disco duro, una unidad Zip, una unidad CDRW, una memoria USB o cualquier otro dispositivo de almacenamiento electrónico. La segunda porción 28B del ASA 28 se denominará aquí simplemente como ASA2 28B.

La base 42 de datos CCS también es un dispositivo de memoria electrónico, es decir, un medio legible por ordenador, para almacenar grandes cantidades de datos organizados para acceder y utilizar durante diversas operaciones del sistema 10 MPCS. Por ejemplo, una pluralidad de tablas de búsqueda que contienen datos de mantenimiento, datos de fallas, procedimientos de mantenimiento y métricas de plataformas móviles pueden almacenarse electrónicamente en la base 42 de datos CCS para acceso y uso por el sistema 10 MPCS y usuarios del sistema 10 MPCS. El procesador 38 CCS controla todas las operaciones del CCS 20. Por ejemplo, el procesador 38 CCS controla las comunicaciones inalámbricas entre el OCS 14 y el CCS 20, transfiriendo datos e información entre el ASA1 28A y el CCS 20, mostrando gráficos y datos en la pantalla 46 CCS, información de interpretación y enrutamiento y entrada de datos mediante el dispositivo 54 de entrada CCS y la ejecución de diversos algoritmos almacenados en el CCS ESD 42. Además, el procesador 38 CCS ejecuta el ASA2 28B para establecer un enlace de comunicación segura con el CCS 20, como se describe a continuación.

Los datos y la información confidenciales, tales como las métricas de la plataforma móvil y los datos de fallas necesitan ser comunicados entre el OCS 14 y el CCS 20 a través de un enlace seguro para impedir el acceso no autorizado a dichos datos e información. Los datos y la información pueden almacenarse en el CCS ESD 50 o en la base 42 de datos CCS, o los datos pueden compartirse con otros sistemas informáticos o redes autorizadas por un operador del

CSS 20. Por ejemplo, los datos se pueden compartir con sistemas de monitorización y mantenimiento de rendimiento de la plataforma móvil que aseguran que se realice un mantenimiento programado regularmente y que la plataforma 18 móvil y todos los sistemas a bordo se mantengan en el orden operacional adecuado. Los sistemas de monitorización y mantenimiento de rendimiento de la plataforma móvil pueden ser aplicaciones de software almacenadas en el CCS ESD 50 o pueden ser sistemas informáticos separados vinculados de manera comunicativa con el CCS 20.

Con referencia ahora a las Figuras 1 y 2, la Figura 2 es un diagrama 200 de secuencia que ilustra un método para establecer un enlace seguro entre al menos un OCS 14 y al menos un CCS 20, de acuerdo con la presente invención. Como se indica en 202, un sistema proveedor de plataforma móvil ejecuta una rutina de administración de seguridad para generar y firmar digitalmente un certificado estático. En diversas realizaciones, el sistema proveedor de plataforma móvil es una red o sistema informático remoto conectado comunicativamente al CCS 20. Alternativamente, el sistema proveedor de plataforma móvil puede ser el CCS 20 o un subsistema del mismo. Como se indica en 204, el certificado estático se comunica al CCS ESD 50 para su posterior recuperación y uso durante la ejecución del ASA2 28B, que se describe a continuación. Además, como se indica en 206, el certificado estático se pasa a una función 62 de gestión de datos distribuidos del sistema proveedor de plataforma móvil que se ejecuta para emitir el certificado estático al(los) OCS(s) 14, como se indica en 208 y 210. Específicamente, el certificado estático está codificado en un archivo de configuración que se carga en cada OCS 14. El archivo de configuración que contiene el certificado estático se puede cargar en cada OCS 14 de cualquier manera de carga de software adecuada. Por ejemplo, el archivo de configuración que contiene el certificado estático se puede cargar a través de un terminal de mantenimiento portátil (PMAT) o a partir de una carga "por etapas" la cual está estacionada de manera inalámbrica en cada OCS 14.

Si el MPCS 10 incluye una pluralidad de OCS 14, cada OCS 14 se carga con el mismo archivo de configuración que contiene el mismo certificado estático. En general, el sistema proveedor de la plataforma móvil genera un único certificado estático que identifica el proveedor de la plataforma móvil y carga el archivo de configuración que contiene el certificado estático en el CCS 20 y todos los sistemas integrados, por ejemplo OCS(s) 14, que el proveedor de la plataforma móvil quiere que el CCS 20 reconozca como un sistema de confianza.

Típicamente, el OCS 14 se inicia después de cada vez que el OCS 14 se instala, mueve o reconfigura. Como se indica en 212, después del "arranque" del OCS 14, el procesador 22 OCS ejecuta el ASA1 28A. Como se indica en 214, la ejecución de ASA1 28A fluye, es decir, elimina, cualquier autorización pertinente preexistente, autenticación y datos de certificado estático que puedan almacenarse en el OCS ESD 26. Por ejemplo, si el OCS 14 se ha eliminado de una primera plataforma 18 móvil y posteriormente instalado en la segunda plataforma 18 móvil, la ejecución del ASA1 28A borrará todos los datos de autorización, autenticación y certificado estático pertinentes preexistentes. Como se indica adicionalmente en 214, la ejecución del ASA1 28A carga el certificado estático codificado en el archivo de configuración del OCS 14. La ejecución del ASA1 28A luego crea un certificado dinámico, como también se indica en 214. Para crear el certificado dinámico, el ASA1 28A obtiene información pertinente que identifica el OCS 14, tal como la identificación del proveedor de la plataforma móvil, un número de identificación de la plataforma 18 móvil en la cual está instalado el OCS 14, por ejemplo un número de registro de un avión, un número de identificación del OCS 14, la ubicación del OCS 14 en la plataforma 18 móvil y cualquier otra información crítica necesaria para especificar la identidad única del OCS 14. El ASA1 28A genera un certificado dinámico con base en la información de identificación pertinente y firma electrónicamente el certificado dinámico utilizando el certificado estático. Como también se indicó en 214, el dinámico recién creado se almacena en OCS ESD 26, por ejemplo, un registro dentro de OCS ESD 26 se actualiza con el certificado dinámico recién creado. Por lo tanto, el OCS 14 crea un par de claves criptográficas únicas que contienen la identidad precisa del OCS 14.

Cuando la plataforma móvil llega a un terminal de destino o en cualquier momento a la vez que la plataforma móvil está en camino al terminal de destino, el OCS 14 puede iniciar una conexión de comunicaciones con el CCS 20, por ejemplo una conexión de protocolo de control de transmisión (TCP), como se indica en 216. Una vez establecida la conexión de comunicación, el ASA1 28A transmite el certificado dinámico generado al CCS 20, como se indica en 220. Como se indicó en 221, el procesador 38 CCS ejecuta el ASA2 38B para leer la firma, es decir, el certificado estático, del certificado dinámico recibido. La ejecución del ASA 38B verifica si el certificado dinámico proviene de un usuario de confianza, como se indica en 222. Dado que el certificado dinámico se firmó digitalmente con el certificado estático, el CCS 20 reconocerá o validará que el certificado dinámico provenga de una fuente confiable.

Una vez verificado como una fuente confiable, el CCS 20 envía un mensaje de aceptación al OCS 14, como se indica en 224. En general, el ASA2 38B enviará un certificado dinámico de retorno que identifica el CCS 20 y firmado digitalmente con el mismo certificado estático al OCS 14. Debido a que el certificado dinámico de retorno está firmado por el mismo certificado estático, el OCS 14 reconocerá al CCS 20 como una fuente confiable y se establecerá el enlace autenticado mutuamente. Por lo tanto, se establece un enlace seguro, con base en clave pública, mutuamente autenticado entre el CCS 20 y el OCS 14 utilizando cualquier protocolo de seguridad adecuado.

El OCS 14 entonces inicia sesión en el CCS 20 y el ASA2 lee la información de identificación del OCS 14 pertinente, por ejemplo el número de identificación de la plataforma móvil, el número de serie del OCS 14 y/o posición del estante,

incluido en el certificado dinámico para configurarse como necesario para comunicarse con el OCS 14, como se indica en 226.

Adicionalmente, el CCS 20 incluye una primera porción o aplicación similar, 53A de la función de gestión de comunicaciones (CMF) almacenada en el CCS ESD 50. Una segunda porción, o aplicación 58B similar del CMF se almacena en el OCS ESD 26. La primera y segunda porciones 58A y 58B del CMF se denominarán respectivamente CMF1 58A y CMF2 58B y se denominarán colectivamente CMF 58. En general, el CMF 58 proporciona interfaces de programas de aplicación para permitir al ASA1 28A y al ASA2 28B comunicarse, como se describe más adelante. Si más de un OCS 14 ha establecido un enlace autenticado mutuamente con el CCS 20, la ejecución del CMF 58 coincide con la información de identificación del OCS 14 pertinente contra una lista incluida CMF2 58B de manera que el CCS 20 pueda rastrear qué OCS 14 están conectados y validar el usuario autorizado. Además, una vez que se establece el enlace seguro entre el CCS 20 y el OCS 14, utilice el enlace seguro como un túnel o canal seguro de una red privada virtual (VPN), como se indica en 230, 232, 234 y 236. Como se indica en 232 el OCS 14 utiliza el CCS 20 para iniciar sesión en el CCS 20. Esto permite al CCS 20 rastrear una pluralidad de plataformas 18 móviles incluidas en el MPCS 10, cada una de las cuales incluye uno o más OCS 14 que se comunican con el uno o más CCSs 20. El CMF 58 también agrega una segunda capa de protección para no permitir usuarios no autorizados.

Por ejemplo, el OCS 14 puede utilizar el certificado dinámico generado por el ASA1 38A, como se describe anteriormente, para establecer un enlace seguro con un segundo CCS 20 a través del canal seguro previamente establecido entre el OCS 14 y el primer CCS 20. O, un el segundo OCS 14 con el mismo certificado estático programado en sus archivos de configuración puede utilizar el canal seguro establecido para establecer un enlace seguro con el CCS 20 utilizando un certificado dinámico generado por, e incluye información de identificación pertinente del segundo OCS 14, de la misma manera que se describe anteriormente. Aún más, el segundo OCS 14 puede generar un certificado dinámico, como se describió anteriormente, para crear un enlace seguro con un segundo CCS 20, a través del canal seguro previamente establecido.

El proveedor de plataforma móvil puede actualizar el paradigma de seguridad emitiendo un nuevo certificado estático. Como este MPCS 10 trata el certificado estático como una parte configurada, se utilizan procedimientos de gestión de configuración establecidos que aíslan al operador de la plataforma móvil y al personal de mantenimiento de los procedimientos especializados.

El sistema 10 de comunicaciones de plataforma móvil utiliza los procesos de control de configuración de software estándar del proveedor de plataforma móvil, junto con el ASA 28 automatizado, para intercambiar los certificados de seguridad apropiados y establecer un enlace seguro entre el(los) OCS(s) 14 y el(los) CCS(s) 20. Esto se hace implementando el certificado estático como parte de la configuración estándar OCS 14 y generando automáticamente un certificado dinámico mediante la ejecución del ASA1 28A al encender el OCS 14 y la ejecución del ASA2 28B cuando el OCS 14 inicia una conexión de comunicación con el CCS 20.

Los expertos en la técnica ahora pueden apreciar a partir de la descripción anterior que las amplias enseñanzas de la presente invención se pueden implementar en una variedad de formas. Por lo tanto, aunque esta invención se ha descrito en conexión con ejemplos particulares de la misma, el verdadero alcance de la invención es como se define en las reivindicaciones.

REIVINDICACIONES

1. Un método para establecer un enlace seguro mutuamente autenticado entre un sistema (18) de plataforma móvil y un sistema remoto, comprendiendo dicho método:

generar (206) y firmar digitalmente un certificado estático;

ejecutar una segunda porción de una aplicación de software de autenticación "ASA2" (28B) para almacenar el certificado estático en un dispositivo (50) de almacenamiento electrónico "ESD" de al menos un sistema (20) informático central "CCS" ubicado remotamente a partir de la plataforma móvil;

emitir (210) el certificado estático a al menos un sistema (14) informático a bordo "OCS" de la plataforma móvil;

ejecutar una primera porción de la aplicación de software de autenticación "ASA1" (28A) para generar (214) automáticamente un certificado dinámico que utiliza el OCS y firmar digitalmente el certificado dinámico con el certificado estático;

transmitir (220) el certificado dinámico al CCS a través de un enlace de comunicaciones iniciado (216) entre el OCS y el CCS;

verificar (222), utilizando el CCS, que el certificado dinámico proviene de una fuente confiable;

enviar (224) un certificado dinámico de retorno firmado electrónicamente con el certificado estático del CCS al OCS; y

ejecutar el ASA1 (28A) para verificar (232), utilizando el OCS, que el certificado dinámico de retorno proviene del CCS, estableciendo así un enlace mutuamente autenticado entre el OCS y el CCS.

2. El método de la reivindicación 1, en donde emitir (210) el certificado estático comprende: codificar el certificado estático en un archivo de configuración; y

cargar el archivo de configuración que incluye el certificado estático en el OCS (14).

3. El método de la reivindicación 2, en donde cargar el archivo de configuración comprende ejecutar el ASA1 (28A) para eliminar la autorización pertinente preexistente, autenticación y datos de certificado estático almacenados en el OCS, y cargar el archivo de configuración en el OCS al encender el OCS.

4. El método de la reivindicación 1, en donde la generación (214) del certificado dinámico comprende:

obtener automáticamente la información pertinente de identificación OCS e incluir la información de identificación OCS en el certificado dinámico; y

almacenar el certificado dinámico en el OCS.

5. El método de la reivindicación 1, en donde verificar que el certificado dinámico proviene de una fuente confiable comprende la ejecución del ASA2 (28B) almacenado en el CCS para verificar que el certificado dinámico haya sido firmado digitalmente con el certificado estático.

6. Un sistema para establecer un enlace de comunicaciones seguro mutuamente autenticado entre una plataforma (18) móvil y una red informática remota, comprendiendo dicho sistema:

al menos un sistema informático a bordo "OCS" (14) de la plataforma móvil que incluye un procesador OCS (22) adaptado para ejecutar una primera porción de una aplicación de software de autenticación "ASA1" (28A) almacenada en el OCS; y

al menos un sistema informático central "CCS" (20) ubicado remotamente a partir de la plataforma móvil adaptada para comunicarse inalámbricamente con el OCS, que incluye el CCS un procesador (38) CCS adaptado para ejecutar una segunda porción de la aplicación de software de autenticación "ASA2" (28B) almacenado en el CCS;

en donde la ejecución del ASA1 está adaptada a:

generar (214) automáticamente y firmar digitalmente un certificado dinámico con un certificado estático emitido por el CCS (20); y

transmitir (220) automáticamente el certificado dinámico al CCS a través de un enlace de comunicación inalámbrica entre el OCS y el CCS; y

en donde la ejecución del ASA2 (28B) se adapta a:

después de que el certificado estático ha sido generado (206) y firmado digitalmente, almacenar el certificado estático en un dispositivo de almacenamiento electrónico "ESD" (50) del CCS;

emitir (210) el certificado estático al OCS; verificar (222) que el certificado dinámico está firmado con el certificado estático; y

enviar (224) un certificado dinámico de retorno firmado electrónicamente con el certificado estático al OCS;

en donde la ejecución del ASA1 se adapta adicionalmente a:

verificar (232) que el certificado dinámico de retorno está firmado con el certificado estático, para establecer un enlace autenticado mutuamente entre el OCS y el CCS.

7. El sistema de la reivindicación 6, en donde la ejecución del ASA2 (28B) está adaptada además para codificar el certificado estático en un archivo de configuración.

8. El sistema de la reivindicación 7, en donde la ejecución del ASA1 está adaptada además para eliminar (214) automáticamente la autorización pertinente preexistente, autenticación y datos de certificado estático almacenados en el OCS, y cargar el archivo de configuración en el OCS al encender el OCS.

9. El sistema de la reivindicación 6, en donde la ejecución del ASA1 (28A) está adaptada además para:

enviar (224) automáticamente un certificado dinámico de retorno firmado electrónicamente con el certificado estático al OCS, en donde el enlace seguro mutuamente autenticado proporciona una red privada virtual "VPN" para la comunicación entre la plataforma móvil y el CCS.

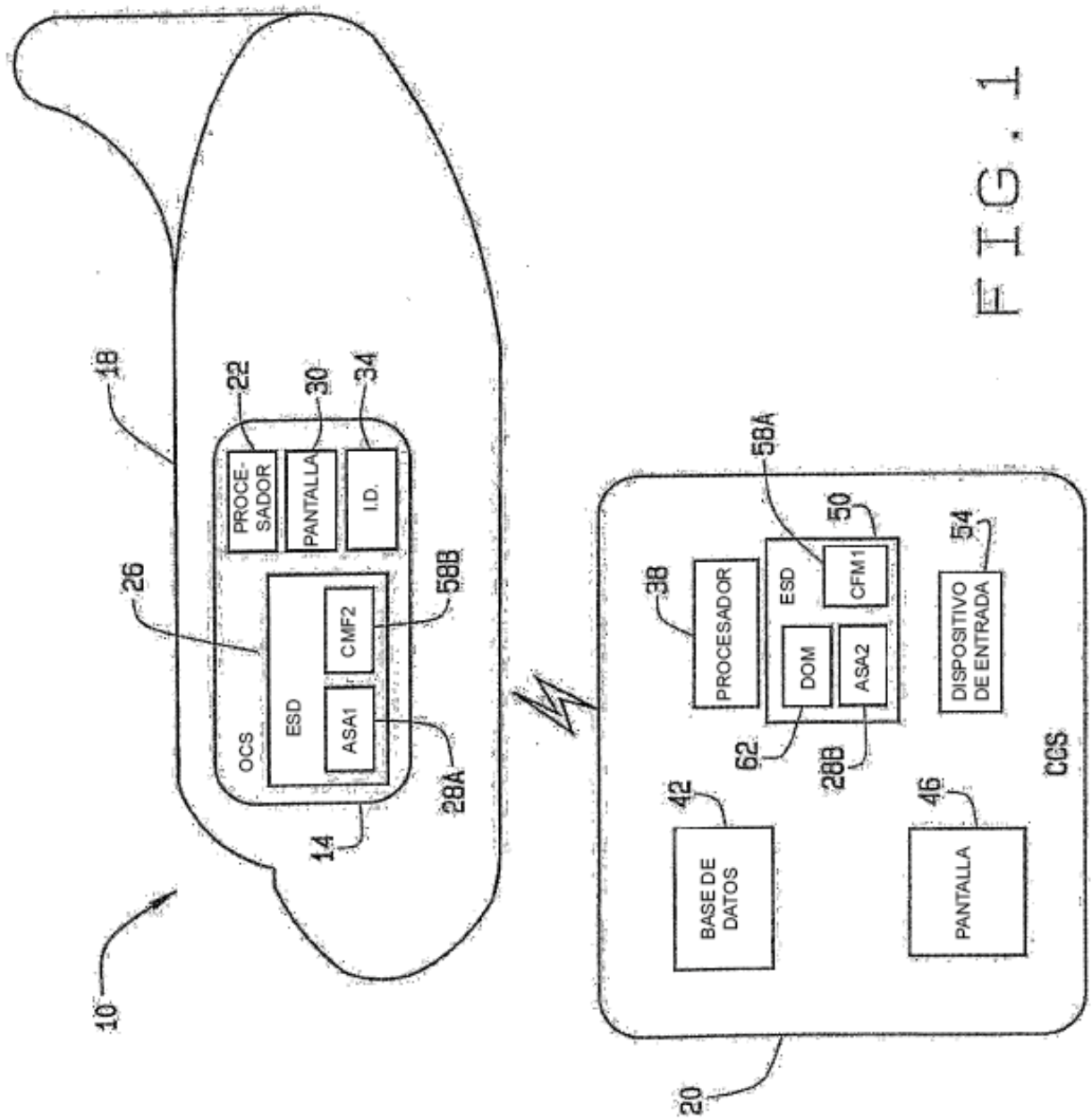
10
18
22
30
34
PROCE-SADOR
PANTALLA
I.D.
26
58B
CMF2
ESD
ASA1
OCS
28A
14
58A
50
38
PROCESADOR
ESD
CFM1
DOM
ASA2
62
28B
54
DISPOSITIVO DE ENTRADA
CGS
42
BASE DE DATOS
46
PANTALLA
20

FIG. 1

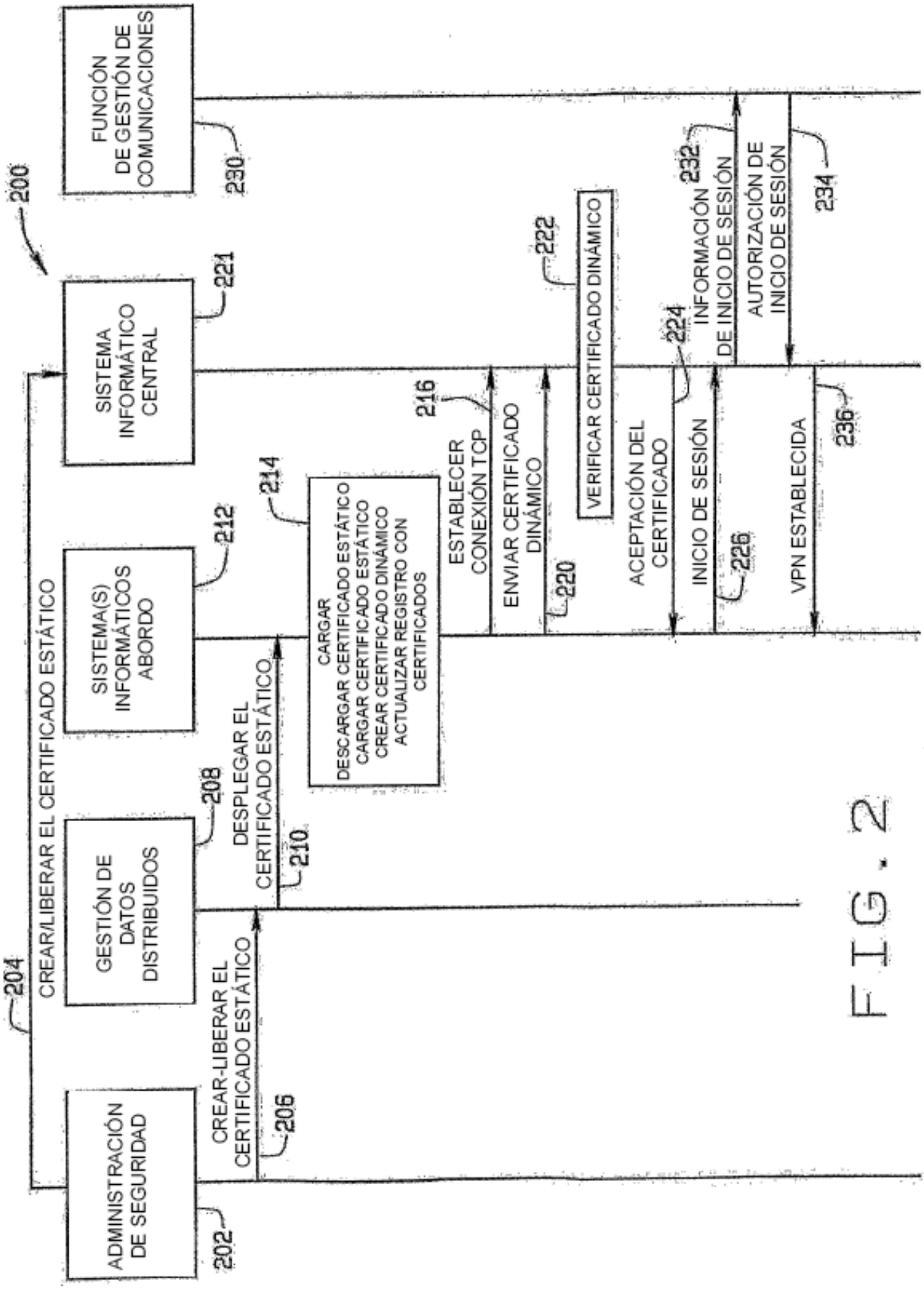
200
FUNCIÓN DE GESTIÓN DE COMUNICACIONES
230
SISTEMA INFORMÁTICO CENTRAL
221
SISTEMA(S) INFORMÁTICOS ABORDO
212
GESTIÓN DE DATOS DISTRIBUIDOS
208
ADMINISTRACIÓN DE SEGURIDAD
202
204
CREAR/LIBERAR EL CERTIFICADO ESTÁTICO
CREAR-LIBERAR EL CERTIFICADO ESTÁTICO
206
DESPLEGAR EL CERTIFICADO ESTÁTICO
210
CARGAR
DESCARGAR CERTIFICADO ESTÁTICO
CARGAR CERTIFICADO ESTÁTICO
CREAR CERTIFICADO DINÁMICO
ACTUALIZAR REGISTRO CON CERTIFICADOS
214
ESTABLECER CONEXIÓN TCP
216
ENVIAR CERTIFICADO DINÁMICO
220
VERIFICAR CERTIFICADO DINÁMICO
222
ACEPTACIÓN DEL CERTIFICADO
224
INICIO DE SESIÓN
226
INFORMACIÓN DE INICIO DE SESIÓN
232
AUTORIZACIÓN DE INICIO DE SESIÓN
234
VPN ESTABLECIDA
236

FIG. 2