(19) OFICINA ESPAÑOLA DE PATENTES Y MARCAS

ESPAÑA

(11) Número de publicación: **2 619 690**

(51) Int. CI.:

G06F 21/00 (2013.01)
H04L 29/06 (2006.01)
H04L 9/32 (2006.01)
H04L 12/24 (2006.01)

(12) TRADUCCIÓN DE PATENTE EUROPEA T3

(86) Fecha de presentación y número de la solicitud internacional: **14.11.2008 PCT/CN2008/073059**

(87) Fecha y número de publicación internacional: **28.05.2009 WO09065345**

(96) Fecha de presentación y número de la solicitud europea: **14.11.2008 E 08851105 (0)**

(97) Fecha y número de publicación de la concesión europea: **04.01.2017 EP 2211570**

(54) Título: **Método de control de acceso a una red confiable basado en autenticación entre pares de tres elementos**

(30) Prioridad:

16.11.2007 CN 200710019093

(45) Fecha de publicación y mención en BOPI de la traducción de la patente:
26.06.2017

(73) Titular/es:

CHINA IWNCOMM CO., LTD (100.0%)
A201, Qinfeng Ge Xi'an Software Park No. 68 Keji 2nd Road Xi'an High-Tech Industry Dev. Zone Xi'an
Shaanxi 710075, CN

(72) Inventor/es:

XIAO, YUELEI;
CAO, JUN;
LAI, XIAOLONG y
HUANG, ZHENHAI

(74) Agente/Representante:

ZEA CHECA, Bernabé

DESCRIPCIÓN

Método de control de acceso a una red confiable basado en autenticación entre pares de tres elementos

Esta solicitud reivindica prioridad a la Solicitud de Patente China nº 200710019093.2, titulada "Método de control de acceso a una red confiable basado en autenticación entre pares de tres elementos", presentada en la Oficina de Patentes China el 16 de noviembre de 2007, la cual se incorpora aquí por referencia en su totalidad.

CAMPO DE LA INVENCIÓN

La presente invención se refiere al campo de la seguridad de redes y, en particular, a un método para el control de acceso a una red confiable basado en autenticación entre pares de tres elementos.

ANTECEDENTES DE LA INVENCIÓN

El problema del software malicioso, por ejemplo, virus, gusanos, etc., se ha vuelto muy importante junto con el desarrollo de la informatización. Ha habido más de treinta y cinco mil tipos de software malicioso en la actualidad, y más de cuarenta millones de ordenadores son infectados anualmente. Para la inhibición de tales ataques se requiere no sólo dirigir un transporte seguro y una comprobación para la entrada de datos, sino también defender desde el origen, es decir, cada terminal conectado a una red. Sin embargo, los enfoques tradicionales de defensa de la seguridad no han podido defenderse contra numerosos ataques maliciosos.

El *Trusted Computing Group* Internacional (TCG) ha establecido específicamente para este problema una especificación de conexión de red basada en la computación confiable - Conexión de Red Confiable (TNC) - simplemente TCG-TNC, que incluye una arquitectura de integridad terminal abierta y un conjunto de normas para garantizar interoperaciones seguras. Este conjunto de normas puede proteger una red tal como se exige para un usuario en la medida de una protección autodefinida por el usuario. El TCG-TNC está destinado esencialmente a establecer una conexión partiendo de la integridad de un terminal. En la arquitectura TCG-TNC es necesario crear un conjunto de políticas para la condición de operación de un sistema en la red confiable, de manera que solamente pueda acceder a la red un terminal que cumpla con una política establecida para la red, la red puede aislar y localizar aquellos dispositivos que no cumplan con la política. Un ataque de sistemas raíz puede bloquearse también debido a un Módulo de Plataforma Confiable (TPM) en uso. Los sistemas raíz son un tipo de script de ataque, un programa de sistema modificado o un conjunto de scripts y sistemas de ataque, que está pensado en un sistema de destino para adquirir ilegalmente el privilegio de control más alto del sistema.

En la arquitectura TCG-TNC existente, la transmisión de información completa en una conexión de red confiable es tal como se ilustra en la figura 1. Un TNC cliente preparará y presentará la información de integridad de la plataforma necesaria a un Colector de Medición de Integridad (IMC) antes de establecer una conexión de red. En un terminal provisto de un Módulo de Plataforma Confiable (TPM), el proceso anterior también significa que la información de la plataforma requerida para una política de red es cifrada y luego almacenada en respectivos Registros de Configuración de la Plataforma (PCRs) y un servidor TNC debe preestablecer y presentar una petición de verificación de integridad de la plataforma a un Verificador de Medición de Integridad IMV. Un proceso específico de este método es el siguiente:

(1) Un solicitante de acceso a la red inicia una solicitud de acceso a un ejecutor de políticas.

(2) El ejecutor de políticas transmite una descripción de la solicitud de acceso a un autorizador de acceso a la red.

(3) El autorizador de acceso a la red ejecuta un protocolo de autenticación de usuario con el solicitante de acceso a la red tras la recepción de la descripción de la solicitud de acceso desde el solicitante de acceso a la red. El autorizador de acceso a la red transmite la solicitud de acceso e información de éxito de autenticación del usuario a un servidor TNC tras la autenticación satisfactoria del usuario.

(4) El servidor TNC inicia la ejecución de autenticación de credenciales de plataforma bidireccional con un TNC cliente, por ejemplo, verificando una clave de identidad de certificación (AIK) de una plataforma, tras la recepción tanto de la solicitud de acceso como de la información de éxito de autenticación de usuario transmitida desde el autorizador de acceso a la red.

(5) El TNC cliente notifica a un Colector de Medición de Integridad (IMC) acerca tanto del inicio de una nueva conexión de red como de la necesidad de ejecutar un protocolo de acuerdo de integridad tras una autenticación de credenciales de plataforma satisfactoria. El Colector de Medición de Integridad (IMC) devuelve la información necesaria sobre la integridad de la plataforma a través de una interfaz

del colector de medición de integridad IF-IMC. El servidor TNC envía la información de integridad de la plataforma a un Verificador de Medición de Integridad (IMV) a través de una Interfaz de Verificación de Medición de Integridad IF-IMV.

(6) El TNC cliente y el TNC servidor realizan uno o más intercambios de datos durante la ejecución del protocolo de acuerdo de integridad hasta que el TNC servidor ya no necesita más.

(7) El servidor TNC completa la ejecución del protocolo de acuerdo de integridad en el TNC cliente y transmite una recomendación al autorizador de acceso a la red para solicitar que se permita un acceso. Tal como puede apreciarse, si existe una consideración de seguridad adicional, el punto de decisión de políticas todavía puede no permitir ningún acceso del Solicitante de Acceso.

(8) El autorizador de acceso a la red pasa una decisión de acceso al ejecutor de políticas, y el ejecutor de políticas ejecuta finalmente la decisión para controlar el acceso del solicitante de acceso.

En la actualidad, no se ha puesto en el mercado ningún producto de arquitectura TCG-TNC desarrollada. Algunas técnicas importantes de la arquitectura TCG-TNC se encuentran todavía en fase de investigación y estandarización. Tal como puede apreciarse en el método de la técnica anterior, puesto que un canal seguro predefinido está presente entre el punto de aplicación de políticas y el punto de decisión de políticas, y el punto de decisión de políticas posiblemente gestiona un gran número de puntos de aplicación de políticas, el punto de decisión de políticas tiene que configurar un gran número de canales seguros, lo que provoca una gestión complicada y consecuentemente una mala capacidad de expansión. Además, los datos en una capa de acceso a la red tienen que estar protegidos por seguridad, por lo que debe establecerse un canal seguro entre el solicitante de acceso y el punto de decisión de políticas, es decir, debe realizarse una negociación de claves de sesión. Sin embargo, también es necesaria la protección de datos entre el solicitante de acceso y el punto de aplicación de políticas, de modo que debe realizarse de nuevo la negociación de claves de sesión entre el Solicitante de Acceso AR y el punto de ejecución de políticas, complicando de este modo la negociación de claves de sesión. También se pasa una clave primaria resultante de la negociación entre el solicitante de acceso y el punto de decisión de políticas desde el punto de decisión de políticas al punto de aplicación de políticas. El paso de la clave a través de la red puede introducir un nuevo punto de ataque de seguridad para reducir la seguridad. Además, la negociación de claves de sesión dual utiliza la misma clave primaria, lo que también puede reducir la seguridad en toda la arquitectura de conexión de red confiable. Además, el solicitante de acceso puede ser incapaz de verificar un certificado AIK del punto de decisión de políticas para su validez. Durante el proceso de autenticación de credenciales de la plataforma, el solicitante de acceso y el punto de decisión de políticas utilizan claves privadas AIK y certificados para la autenticación de credenciales de plataforma bidireccional y ambos verificarán la validez de los certificados AIK. Si el punto de decisión de políticas es un proveedor de acceso de red del solicitante de acceso, el solicitante de acceso no puede acceder a ninguna red sin una conexión de red confiable, es decir, el certificado AIK del punto de decisión de políticas no puede verificarse para su validez, lo cual sería inseguro. Por último, la evaluación de la integridad de la plataforma no es punto a punto. En la arquitectura TCG-TNC, el punto de decisión de políticas realiza una evaluación de la integridad de la plataforma sobre el solicitante de acceso y el punto de aplicación de políticas puede conocer una decisión de aplicación del punto de decisión de políticas si una plataforma del solicitante de acceso es confiable, pero el solicitante de acceso no realizará una evaluación de la integridad de la plataforma en el punto de decisión de políticas. Si la plataforma del punto de decisión de políticas no es confiable, por ejemplo, debido a software malicioso, etc., puede ser inseguro que la red de acceso esté conectada a un dispositivo no confiable y un enlace confiable desde el solicitante de acceso a la red confiable puede romperse en el punto de aplicación de políticas, pero es necesaria una confianza punto a punto en una red Ad Hoc.

DESCRIPCIÓN DE LA INVENCIÓN

Un objetivo de la invención es un método de control de acceso a una red confiable basado en autenticación entre pares de tres elementos (TePA), que pueda solucionar los problemas técnicos de una red confiable conectada en la técnica anterior, incluyendo una mala expansibilidad, un complejo proceso de negociación de claves, baja seguridad, sin que el solicitante de acceso pueda verificar un certificado AIK para su validez y sin que la evaluación de la confiabilidad de la plataforma sea punto a punto.

Las soluciones técnicas de la invención son las siguientes:

Un método de control de acceso a una red confiable basado en la autenticación entre pares de tres elementos incluye las etapas de:

Inicializar, mediante un solicitante de acceso y un controlador de acceso, unos Colectores de Medición de la confiabilidad, TMCs, en una capa de medición de la confiabilidad para recopilar información de la confiabilidad requerida para cada uno; e inicializar, por medio de un gestor de políticas, un verificador

de medición de la confiabilidad, TMV, en la capa de medición de la confiabilidad para verificar la información confiable del solicitante de acceso y el controlador de acceso;

ejecutar un protocolo de autenticación entre pares de tres elementos basado en un gestor de políticas que actúa como tercero por el solicitante de acceso, el controlador de acceso y el gestor de directivas en una capa de control de acceso a la red para realizar la autenticación de usuario bidireccional entre el solicitante de acceso y el controlador de acceso;

cuando los resultados de la autenticación de usuario indican una autenticación satisfactoria o que se requiere un proceso de evaluación de la confiabilidad de plataforma en una política local, ejecutar el protocolo de autenticación entre pares de tres elementos basado en el gestor de políticas que actúa como tercero por el solicitante de acceso, el controlador de acceso y el gestor de políticas en una capa de evaluación de plataforma confiable para realizar una evaluación de la confiabilidad de la plataforma bidireccional entre el solicitante de acceso y el controlador de acceso; generar, a través de un TNAC cliente del solicitante de acceso y un TNAC servidor del controlador de acceso de acuerdo con resultados de la evaluación de la confiabilidad de la plataforma en el proceso de evaluación de la confiabilidad de la plataforma y transmitir correspondientes recomendaciones respectivamente al solicitante de acceso y al controlador de acceso, de manera que el solicitante de acceso de red y el controlador de acceso de red controlan mutuos puertos de acceso respectivamente, de acuerdo con las recomendaciones.

En particular, el control de puertos se lleva a cabo de la siguiente manera:

un puerto no controlado del solicitante de acceso controla el transporte de datos de autenticación de usuario y protocolos de negociación de claves de sesión, datos de protocolo de evaluación de la confiabilidad de plataforma y datos de servicio de corrección de la plataforma, y un puerto controlado del solicitante de acceso controla el transporte de datos de servicios de aplicación; y

un puerto no controlado del controlador de acceso controla el transporte de los datos de autenticación de usuario y de protocolos de negociación de claves de sesión, y un puerto controlado del controlador de acceso controla el transporte de los datos de protocolo de evaluación de la confiabilidad de la plataforma, datos de servicio de corrección de la plataforma y datos de servicio de aplicación.

En particular, el control de puertos se lleva a cabo tal como sigue:

(a) una entidad solicitante de acceso en el solicitante de acceso y una entidad de autenticación de usuario en el controlador de acceso realizan autenticación de usuario bidireccional y negociación de claves de sesión a través de los puertos no controlados; y la entidad de autenticación de usuario en el controlador de acceso y una entidad de políticas de servicio de autenticación en el gestor de políticas intercambian información directamente; y tras una autenticación de usuario bidireccional satisfactoria, el puerto controlado del controlador de acceso cambia a un estado autenticado para permitir el transporte de los datos del protocolo de evaluación de la confiabilidad de la plataforma; y

(b) la entidad solicitante de acceso en el solicitante de acceso, una entidad de evaluación de la confiabilidad de la plataforma en el controlador de acceso y una entidad de servicio de políticas de evaluación en el gestor de políticas ejecutan el protocolo de autenticación entre pares de tres elementos para realizar una evaluación de la confiabilidad de la plataforma bidireccional entre el solicitante de acceso y el controlador de acceso; y en el proceso de evaluación de la confiabilidad de la plataforma, la entidad solicitante de acceso en el solicitante de acceso se comunica a través del puerto no controlado, la entidad de evaluación de la confiabilidad de la plataforma en el controlador de acceso se comunica a través del puerto controlado autenticado y la entidad de evaluación de la confiabilidad de la plataforma en el controlador de acceso y la entidad de servicio de políticas de evaluación en el gestor de políticas intercambian información directamente.

En particular, el control de puertos del solicitante de acceso y el controlador de acceso se realiza siguiendo cuatro casos después de que se realiza un proceso de evaluación de la confiabilidad de la plataforma:

si ambas plataformas del solicitante de acceso y el controlador de acceso son confiables, tanto los puertos controlados en el solicitante de acceso como el controlador de acceso están en un estado confiable de modo que se permite el transporte de datos de servicio de aplicación entre el solicitante de acceso y el controlador de acceso.

O si la plataforma del solicitante de acceso es confiable y la plataforma del controlador de acceso no es confiable, los puertos no controlados y controlados del solicitante de acceso y el controlador de acceso están en un estado original y el controlador de acceso recupera información de corrección de configuración de la plataforma de un dominio aislado conectado para la corrección de la plataforma. El controlador de acceso está conectado tanto al dominio aislado como a un dominio seguro.

O, si la plataforma del solicitante de acceso no es confiable y la plataforma del controlador de acceso es confiable, se cambia el puerto controlado para el cual se deshabilita la corrección del controlador de acceso a un estado en el que se ha habilitado la corrección para que el solicitante de acceso pueda acceder a un dominio aislado a través del controlador de acceso para recuperar la información de corrección de la configuración de la plataforma para la corrección de la plataforma.

O, si ninguna de las plataformas del solicitante de acceso y del controlador de acceso es confiable, el puerto controlado para el cual está desactivada la corrección del controlador de acceso se cambia a un estado en el que se ha habilitado la corrección para que el solicitante de acceso pueda acceder a un dominio aislado a través del controlador de acceso para recuperar la información de corrección de la configuración de la plataforma para la corrección de la plataforma.

En particular, las recomendaciones incluyen información de permisos de acceso, información de prohibición de acceso o información de aislamiento y corrección.

En particular, cuando las recomendaciones recibidas por el controlador de acceso a la red y el solicitante de acceso a la red son información de aislamiento y corrección, el solicitante de acceso y el controlador de acceso realizan la corrección de la plataforma mediante la información de corrección de la configuración de la plataforma y realizan el proceso de evaluación confiable de la plataforma entre el solicitante de acceso y el controlador de acceso.

En particular, la evaluación de la confiabilidad de plataforma se realiza tal como sigue:

se realiza una autenticación de credenciales de la plataforma: el gestor de políticas verifica los certificados AIK del solicitante de acceso y del controlador de acceso para su validez; y se realiza una verificación de la confiabilidad de la plataforma: el gestor de políticas verifica la confiabilidad de la plataforma del solicitante de acceso y del controlador de acceso.

En particular, el proceso de evaluación de la confiabilidad de plataforma entre el solicitante de acceso y el controlador de acceso incluye:

transmitir información que identifica la configuración de la plataforma del solicitante de acceso entre el solicitante de acceso y el gestor de políticas e información que identifica la configuración de la plataforma del controlador de acceso entre el controlador de acceso y el gestor de políticas a través de una transmisión encriptada;

transmitir información intercambiada entre el TNAC cliente y el TNAC servidor utilizando una clave de sesión; y

generar y transmitir, mediante el gestor de políticas, los resultados de la evaluación de la confiabilidad de la plataforma del solicitante de acceso y del controlador de acceso al TNAC cliente y al TNAC servidor.

En particular, un proceso de autenticación de usuario entre el solicitante de acceso y el controlador de acceso incluye:

iniciar una solicitud de acceso desde el solicitante de acceso al controlador de acceso;

iniciar, mediante el controlador de acceso, el proceso de autenticación de usuario al recibir la solicitud de acceso y generar resultados de autenticación de usuario del solicitante de acceso y el controlador de acceso;

generar, mediante el solicitante de acceso y el controlador de acceso, una clave primaria entre ellos al realizar una autenticación de usuario satisfactoria; y

negociar, mediante el solicitante de acceso y el controlador de acceso, acerca de una clave de sesión utilizando la clave primaria y transmitir la información de éxito de autenticación de usuario, respectivamente, al TNAC cliente y al TNAC servidor.

En particular, la inicialización de los Colectores de Medida de la Confiabilidad, TMCs y el Verificador de Medición de la confiabilidad, TMV, en la capa de medición de la confiabilidad incluye:

inicializar, mediante el TNAC cliente del solicitante de acceso y el TNAC servidor del controlador de acceso, los Colectores de Medición de la confiabilidad, en la capa de medición de la confiabilidad;

inicializar, mediante un Servidor de Políticas de Evaluación, EPS, del gestor de políticas, el Verificador de Medición de la confiabilidad, TMV, en la capa de medición confiable;

almacenar, mediante unos Módulos de Plataforma Confiable, TPMs, del solicitante de acceso y el controlador de acceso, la información de la confiabilidad de la plataforma requerida para cada uno en unos Registros de Configuración de la Plataforma, PCRs;

preparar, mediante el TNAC cliente del solicitante de acceso y el TNAC servidor del controlador de acceso, información de la confiabilidad de la plataforma requerida para el controlador de acceso y el solicitante de acceso, respectivamente, a través de los Colectores de Medida de la Confiabilidad, TMCs; y

establecer y distribuir, mediante el gestor de políticas, políticas de control de acceso que incluyen una política del solicitante de acceso para unirse a una red conectada y una política de control de acceso a la red del controlador de acceso para el solicitante de acceso.

La invención presenta las siguientes ventajas sobre la técnica anterior:

Con el método de acuerdo con la invención, puede ampliarse una descripción de la confiabilidad de la plataforma y puede definirse la confiabilidad como un atributo de estado de la plataforma que mide y evalúa la confiabilidad de la plataforma, por ejemplo, la integridad, para aumentar de este modo la capacidad de expansión del control de acceso a la red confiable. En una aplicación práctica, un gestor de políticas tiene que gestionar un gran número de controladores de acceso, y la invención puede eliminar la necesidad de una fuerte asociación de seguridad entre el controlador de acceso y el gestor de directivas, aumentando así la capacidad de extensión del control de acceso de red confiable. Además, la invención puede simplificar aún más un proceso de negociación de claves y mejorar la seguridad del control de acceso de red confiable. La negociación de claves puede realizarse entre el solicitante de acceso y el controlador de acceso para asegurar directamente los datos de un proceso de evaluación de la confiabilidad de la plataforma y datos de servicio después de un control de acceso de red confiable sin negociación de claves de sesión dual para simplificar un proceso de negociación de claves y mejorar la seguridad del control de acceso de red confiable. La seguridad de una clave puede garantizarse ya que no es necesario transmitir una clave primaria generada en un proceso de autenticación a través de una red para garantizar así la seguridad de la clave. La invención puede mejorar aún más la seguridad del proceso de evaluación de la confiabilidad de la plataforma y simplificar un mecanismo de gestión de claves de verificación de la confiabilidad de un control de acceso a una red confiable. Puesto que, de acuerdo con la invención, se adopta un método de autenticación entre pares de tres elementos en la capa de evaluación de plataforma confiable, es decir, la autenticación y la verificación centralizadas de certificados AIK y la confiabilidad de la plataforma del solicitante de acceso y el controlador de acceso se realizan, respectivamente, en un método de autenticación bidireccional basado en terceros para mejorar así la seguridad del proceso de evaluación de la confiabilidad de la plataforma y simplificar el mecanismo de verificación de la gestión de claves y la confiabilidad de una arquitectura de control de acceso de red confiable. Además, la invención puede mejorar la seguridad del control de acceso global a la red confiable. La invención adopta el método de autenticación entre pares de tres elementos para la autenticación bidireccional del usuario en la capa de control de acceso a la red y la evaluación bidireccional de la confiabilidad de la plataforma en la capa de evaluación de la plataforma confiable. De este modo, la invención mejora la seguridad de la arquitectura global de control de acceso de la red confiable.

De este modo, la invención puede eliminar, además, el problema de que pueda romperse una cadena confiable en un dispositivo de acceso. Dado que la evaluación bidireccional de la confiabilidad de la plataforma se realiza entre el solicitante de acceso y el controlador de acceso, la invención elimina el problema de que se rompa una cadena confiable en el controlador de acceso de un dispositivo de acceso.

Por último, el procedimiento de acuerdo con la invención adopta un control de puertos de múltiples niveles. El controlador de acceso realiza un control de múltiples niveles en un puerto controlado para controlar estrictamente de este modo un privilegio de acceso del solicitante de acceso y mejorar la seguridad y el rendimiento de la arquitectura de control de acceso a la red confiable. La invención amplía una descripción de un módulo de plataforma confiable. En la arquitectura TCG-TNC, un Módulo de Plataforma Confiable (TPM) es un chip de seguridad en una placa principal. De acuerdo con la invención, el Módulo de Plataforma Confiable (TPM) puede ser un módulo de software

abstracto responsable de la evaluación de la plataforma confiable. Por ejemplo, un Módulo de Plataforma Confiable (TPM) implementado en el software explora componentes respectivos de la plataforma y, a continuación, genera y transmite los resultados del análisis de seguridad a una plataforma opuesta. La plataforma opuesta evalúa entonces estos resultados de la exploración de seguridad para realizar de este modo la evaluación de la plataforma confiable.

BREVE DESCRIPCIÓN DE LOS DIBUJOS

La figura 1 es un diagrama esquemático de la transmisión de información completa para un control de acceso a una red confiable en una arquitectura TCG-TNC existente;
La figura 2 es un diagrama esquemático de un sistema de control de puertos en una arquitectura TNAC de acuerdo con la invención;
La figura 3 es un diagrama esquemático de transmisión de información completa para control de acceso a una red confiable en una arquitectura TNAC de acuerdo con la invención; y
La figura 4 es un diagrama esquemático de un proceso de evaluación de la confiabilidad de la plataforma en la arquitectura TNAC de acuerdo con la invención.

A continuación, se enumeran los números de referencia:

N_S: número aleatorio generado por un controlador de acceso; $Cert_{AC\text{-}AIK}$: un certificado AIK de un controlador de acceso; $PCRsList_{AR}$: una lista de parámetros PCRs solicitados por el controlador de acceso desde el solicitante de acceso; N_{AR}: un número aleatorio generado por el solicitante de acceso; $Cert_{AR\text{-}AIK}$: un certificado AIK del solicitante de acceso; $PCRsList_{AC}$: una lista de parámetros PCRs solicitados por peticiones del solicitante de acceso desde el controlador de acceso; Log_{AR}: un registro de medida correspondiente a los valores de PCR solicitados por el controlador de acceso; $PCRs_{AR}$: los valores de PCR solicitados por el controlador de acceso; $[N_S, PCRs_{AR}]_{Sig}$: una firma del solicitante de acceso sobre el número aleatorio generado por el controlador de acceso N_S y sobre los valores correspondientes de los PCRs solicitados por el controlador de acceso; N_{AC}: un número aleatorio generado por un usuario del controlador de acceso; Log_{AC}: un registro de medida correspondiente a valores de PCRs solicitados por el solicitante de acceso; $PCRs_{AC}$: los valores de PCRs solicitados por el solicitante de acceso; $[N_{AR}, PCRs_{AC}]_{Sig}$: una firma del controlador de acceso sobre el número aleatorio generado por el solicitante de acceso NAR y sobre los valores correspondientes de los PCRs solicitados por el solicitante de acceso; $Result_{AIK\text{-}PCRs}$: resultados de autenticación de certificados AIK y verificación de la confiabilidad del solicitante de acceso y del controlador de acceso; $[Result_{AIK\text{-}PCRs}]_{Sig}$: una firma de un gestor de políticas sobre los resultados de la autenticación de certificados AIK y la verificación de la confiabilidad del solicitante de acceso y el controlador de acceso; Re_{AC}: el resultado de la verificación de la confiabilidad de la plataforma del controlador de acceso; Re_{AR}: el resultado de la verificación de la confiabilidad del solicitante de acceso; $Re_{AR\text{-}AIK}$: el resultado de la verificación del certificado AIK del solicitante de acceso; $Re_{AC\text{-}AIK}$: el resultado de la verificación del certificado AIK del controlador de acceso; Re_{Access}: un resultado de acceso confiable; Rem_{AR}: información de corrección de la configuración de plataforma del solicitante de acceso; y Rem_{AC}: información de corrección de la configuración de la plataforma del controlador de acceso.

DESCRIPCIÓN DETALLADA DE LA INVENCIÓN

La invención se refiere a una conexión de red basada en una técnica informática confiable y un método para el control de acceso a una red confiable (TNAC) basado en autenticación entre pares de tres elementos (TePA), que se ha propuesto principalmente para los inconvenientes de la arquitectura TNC en el sistema TCG existente.

La invención consiste principalmente en una capa de control de acceso a la red, una capa de evaluación de plataforma confiable y una capa de medición de la confiabilidad. Un solicitante de acceso, un controlador de acceso y un gestor de políticas, que son tres entidades lógicas de la invención, pueden distribuirse en cualquier lugar a través de una red. El solicitante de acceso también se denomina solicitante, estación de usuario, etc., el controlador de acceso también se conoce como controlador de acceso de autenticación, estación base, unidad de servicio de acceso, etc., y el gestor de políticas también se denomina servidor de autenticación, servidor confiable, servidor en segundo plano, etc.

La capa de control de acceso a la red es responsable de la autenticación direccional del usuario y la negociación de claves entre el solicitante de acceso y el controlador de acceso, así como el control de acceso mutuo del solicitante de acceso y el controlador de acceso de acuerdo con un resultado de autenticación de usuario de red y un resultado de la confiabilidad de plataforma evaluación. La capa de control de acceso a la red puede adoptar un método para el control de acceso basado en autenticación entre pares de tres elementos, es decir, una técnica de control de acceso a la red ya adoptada en el estándar WLAN chino. La confiabilidad de la invención se refiere a un atributo de estado de la plataforma que mide y evalúa la confiabilidad de una plataforma, por ejemplo, la integridad.

Un Módulo de Plataforma Confiable (TPM) en la invención puede ser un Módulo de Plataforma Confiable (TPM) de una arquitectura TNC en un sistema TCG o un módulo de software abstracto responsable de la evaluación de la

plataforma confiable. Por ejemplo, un Módulo de Plataforma Confiable (TPM) implementado en el software explora los componentes respectivos de la plataforma y, a continuación, genera y transmite los resultados del análisis de seguridad a una plataforma opuesta. La plataforma opuesta evalúa estos resultados de exploración de seguridad para realizar, de este modo, la evaluación de la plataforma confiable.

La capa de evaluación de la plataforma confiable es responsable de la evaluación de la confiabilidad de la plataforma, incluyendo la autenticación de credenciales de la plataforma y la verificación de la confiabilidad de la plataforma entre el solicitante de acceso y el controlador de acceso. En la capa de evaluación de la plataforma confiable se ejecuta un protocolo de autenticación entre pares de tres elementos, es decir, un protocolo de autenticación bidireccional basado en terceros, entre el solicitante de acceso, el controlador de acceso y el gestor de políticas, y el gestor de políticas verifica los certificados AIK del solicitante de acceso y el controlador de acceso para la validez y es responsable de verificar la confiabilidad de la plataforma del solicitante de acceso y del controlador de acceso.

La capa de medición de la confiabilidad es responsable de recopilar y verificar la información relacionada con la confiabilidad de la plataforma del solicitante de acceso y del controlador de acceso.

La figura 3 ilustra un diagrama de interacción estructural de un proceso de transmisión de información completa para un control de acceso de red confiable de acuerdo con la invención. Las etapas específicas de implementación de la invención son tal como sigue:

(1) Se lleva a cabo la inicialización. Unos Colectores de Medición de la confiabilidad (TMC) y un Verificador de Medición de la confiabilidad (TMV) en la capa de medición de la confiabilidad se inicializan antes de que se establezca la conexión de una red confiable;
En particular, la inicialización puede incluir las siguientes etapas:

(1.1) Un TNAC cliente del solicitante de acceso y un TNAC servidor del controlador de acceso inicializan los Colectores de Medición de la confiabilidad (TMC) en la capa de medición de la confiabilidad para recopilar información de la confiabilidad requerida para cada uno. Un Servidor de Políticas de Evaluación (EPS) del gestor de políticas inicializa el Verificador de Medición de la confiabilidad (TMV) en la capa de medición de la confiabilidad para verificar la confiabilidad de la plataforma del solicitante de acceso y el controlador de acceso.

(1.2) Los Módulos de Plataforma Confiable (TPMs) del solicitante de acceso y el controlador de acceso almacenan la información de la confiabilidad requerida para cada uno en unos Registros de Configuración de la Plataforma (PCRs). La información de la confiabilidad relativa a la integridad será cifrada y almacenada en los Registros de Configuración de la Plataforma (PCRs).

(1.3) El TNAC cliente del solicitante de acceso y el TNAC servidor del controlador de acceso preparan información de la confiabilidad de la plataforma requerida para el controlador de acceso y el solicitante de acceso, respectivamente, a través de los Colectores de Medición de la confiabilidad (TMCs).

(1.4) El gestor de políticas establece y distribuye políticas de control de acceso a la red incluyendo una política de si el solicitante de acceso se une a una red conectada y una directiva de control de acceso a la red del controlador de acceso para el solicitante de acceso. El gestor de políticas puede establecer y distribuir las políticas de control de acceso a la red del solicitante de acceso y el controlador de acceso de acuerdo con la especificación nacional de protección de múltiples niveles de seguridad de la información.

(1.5) El TNAC cliente y el TNAC servidor preparan unas listas de parámetros de PCRs que son solicitados por el solicitante de acceso y el controlador de acceso respectivamente para la verificación de cada uno de acuerdo con políticas de control de acceso a la red distribuidas por el gestor de políticas

(2) El solicitante de acceso, el controlador de acceso y el gestor de políticas ejecutan un protocolo de autenticación entre pares de tres elementos basado en el gestor de políticas que actúa como tercero en la capa de control de acceso a la red para realizar la autenticación de usuario bidireccional entre el solicitante de acceso y el controlador de acceso.
En particular, la etapa (2) puede incluir las siguientes etapas:

(2.1) El solicitante de acceso inicia una petición de acceso al controlador de acceso.

(2.2) Al recibir la solicitud de acceso, el controlador de acceso inicia un proceso de autenticación de usuario y el solicitante de acceso a la red, el controlador de acceso a la red y el servidor de políticas de autenticación en la capa de control de acceso a la red comienzan a ejecutar el protocolo de autenticación entre pares de tres elementos, es decir, un protocolo de autenticación bidireccional basado en terceros, donde el servidor de políticas de autenticación actúa como tercero, para realizar de este modo la autenticación de usuario bidireccional entre el solicitante de acceso y el controlador de acceso y generar resultados de autenticación de usuario entre el solicitante de acceso y el controlador de acceso. Si la autenticación bidireccional del usuario es satisfactoria, el solicitante de acceso y el controlador de acceso generan una clave primaria entre ellos durante la autenticación del usuario.

(2.3) Tras la autenticación de usuario bidireccional satisfactoria, el solicitante de acceso y el controlador de acceso negocian acerca de una clave de sesión utilizando la clave primaria generada durante la autenticación de usuario y luego transmiten información de autenticación de usuario satisfactoria respectivamente al TNAC cliente y al TNAC servidor y tienen puertos del solicitante de acceso a la red y el controlador de acceso a la red controlados respectivamente de acuerdo con los resultados de la autenticación del usuario del controlador de acceso y el solicitante de acceso para permitir de este modo el paso de los datos de un proceso de evaluación de confiabilidad.

(3.) Cuando los resultados de la autenticación de usuario bidireccional indican una autenticación satisfactoria o que se requiere un proceso de evaluación de la confiabilidad de la plataforma en una política local, el solicitante de acceso, el controlador de acceso y el gestor de políticas ejecutan el protocolo de autenticación de tres elementos basado en el gestor de políticas que actúa como tercero en la capa de evaluación de plataforma confiable para realizar la evaluación de la confiabilidad de plataforma bidireccional entre el solicitante de acceso y el controlador de acceso.

En particular, la etapa (3) puede realizarse en el siguiente proceso:

Cuando el TNAC servidor del controlador de acceso recibe la información de autenticación de usuario satisfactoria transmitida desde el controlador de acceso de la red o información del proceso de evaluación de la confiabilidad de plataforma requerida en la política local, el TNAC cliente, el TNAC servidor y un servidor de políticas de evaluación en la capa de evaluación de plataforma confiable realizan la evaluación de la confiabilidad de la plataforma bidireccional del solicitante de acceso y del controlador de acceso utilizando el protocolo de autenticación entre pares de tres elementos. En el proceso de evaluación de la confiabilidad de la plataforma, la información intercambiada entre el TNAC cliente se transmite bajo la protección de la clave de sesión negociada en la etapa (2.3).

En el proceso de evaluación de la confiabilidad, la información que identifica la configuración de la plataforma del solicitante de acceso se transmitirá entre el solicitante de acceso y el gestor de políticas, por ejemplo, un registro de medición correspondiente a valores de los Registros de Configuración de Plataforma (PCRs), información de corrección de la configuración de la plataforma, etc., que se transmitirán mientras se cifran para evitar de este modo que el controlador de acceso o un atacante conozcan la información. También, entre el controlador de acceso y el gestor de directivas se transmitirá información que identifica la configuración de la plataforma del controlador de acceso mientras ésta se cifra para evitar así que el solicitante de acceso o un atacante conozca la información. Las técnicas de transmisión cifradas que pueden adoptarse aquí pueden incluir encriptación de clave simétrica y asimétrica. En el proceso de evaluación de la confiabilidad de la plataforma, el servidor de políticas de evaluación desempeña el papel de una tercera paridad y el TNAC servidor, el TNAC cliente y el servidor de políticas de evaluación también intercambian información con unos colectores de medición de la confiabilidad y un verificador de medición de la confiabilidad en la capa superior.

En particular, en una aplicación práctica, la evaluación de la sensibilidad de la plataforma se lleva a cabo tal como sigue:

Se lleva a cabo una autenticación de credenciales de la plataforma: el gestor de políticas verifica los certificados AIK del solicitante de acceso y el controlador de acceso para su validez; y
(2) se lleva a cabo una verificación de la confiabilidad de la plataforma: el gestor de políticas verifica la confiabilidad de la plataforma del solicitante de acceso y del controlador de acceso.

Haciendo referencia a la figura 3, una implementación específica de la evaluación de la confiabilidad de la plataforma de acuerdo con la invención puede ser tal como sigue:

(3.1) Cuando el TNAC servidor del controlador de acceso recibe la información de autenticación de usuario satisfactoria transmitida desde el controlador de acceso a la red o ha confirmado la autenticación de usuario satisfactoria, el controlador de acceso transmite un número aleatorio generado por el controlador de acceso N_S, un certificado del controlador de acceso $Cert_{AC-AIK}$, y una lista de parámetros PCRs solicitada por el controlador de acceso desde el solicitante de acceso, $PCRsLiSt_{AR}$, al solicitante de acceso.

(3.2) Al recibir la información transmitida desde el controlador de acceso en la etapa (3.1.1), el solicitante de acceso extrae en primer lugar los valores correspondientes de PCRs $PCRs_{AR}$, al Módulo de Plataforma Confiable (TPM) de la lista de parámetros PCRs solicitados por el controlador de acceso y, a continuación, firma con una clave privada AIK los valores de PCRs $PCRs_{AR}$, extraídos al Módulo de Plataforma Confiable (TPM) y al número aleatorio generado por el controlador de acceso N_S en el Módulo de Plataforma Confiable (TPM). Finalmente, el solicitante de acceso transmite al controlador de acceso el número aleatorio generado por el controlador de acceso N_S, un número aleatorio generado por el solicitante de acceso N_{AR}, un certificado AIK del solicitante de acceso $Cert_{AR-AIK}$, una lista de parámetros PCRs solicitados por el solicitante de acceso desde el controlador de acceso $PCRsList_{AC}$, los valores de PCRs solicitados por el controlador de acceso $PCRs_{AR}$, un registro de medición correspondiente a los valores de PCRs solicitados por el controlador de acceso Log_{AR}, y una firma del solicitante de acceso con la clave privada AIK en el Módulo de Plataforma Confiable (TPM) en los valores de PCRs, $PCRs_{AR}$, extraídos al Módulo de Plataforma Confiable (TPM) y el número aleatorio generado por el controlador de acceso N_S, $[N_S, PCRs_{AR}]_{Sig}$.

(3.3) Al recibir la información transmitida desde el solicitante de acceso en la etapa (3.2), el controlador de acceso comprueba primero el número aleatorio generado por el controlador de acceso N_S por consistencia y verifica la firma AIK $[N_S, PCRs_{AR}]_{Sig}$ del solicitante de acceso con una clave pública en el certificado AIK del solicitante de acceso para la validez, y extrae luego los valores correspondientes de PCRs $PCRs_{AC}$, al Módulo de Plataforma Confiable (TPM) de la lista de parámetros PCRs solicitados por el solicitante de acceso. A continuación, el controlador de acceso firma con una clave privada AIK los valores de PCRs $PCRs_{AC}$, extraídos al Módulo de Plataforma Confiable (TPM) y el número aleatorio N_{AR} generado por el solicitante de acceso en el Módulo de Plataforma Confiable (TPM). Finalmente, el controlador de acceso transmite al gestor de políticas el número aleatorio N_S y un número aleatorio N_{AC} generado por el controlador de acceso, el número aleatorio generado por el solicitante de acceso N_{AR}, el certificado AIK del solicitante de acceso $Cert_{AR-AIK}$, Solicitado por el controlador de acceso $PCRs_{AR}$, el registro de medición correspondiente a los valores de PCRs solicitados por el controlador de acceso Log_{AR}, el certificado AIK del controlador de acceso $Cert_{AC-AIK}$, los valores de PCRs solicitados por el solicitante de acceso $PCRs_{AC}$ y un registro de medida correspondiente a los valores de PCRs solicitados por el solicitante de acceso Log_{AC}.

(3.4) Al recibir la información transmitida desde el controlador de acceso en la etapa (3.3), el gestor de políticas verifica en primer lugar los certificados AIK del solicitante de acceso y el controlador de acceso para su validez; después recalcula valores correspondientes de PCRs de acuerdo con los registros de medida Log_{AR} y Log_{AC} de los valores correspondientes de PCRs extraídos a los respectivos Módulos de Plataforma Confiable (TPMs) del solicitante de acceso y el controlador de acceso y los compara con $PCRs_{AR}$ y $PCRs_{AC}$ para verificar de este modo los registros de medición Log_{AR} y Log_{AC} para integridad; a continuación, compara los valores de medición confiable de los componentes de plataforma respectivos en los registros de medición Log_{AR} y Log_{AC} con los valores de medición de confiabilidad estándar correspondientes de los componentes de plataforma respectivos de una base de datos para finalmente generar resultados de autenticación de certificado AIK y verificación de la confiabilidad de plataforma con una clave privada que corresponde a un certificado de identidad del gestor de políticas; y finalmente transmite al controlador de acceso los resultados de autenticación del certificado AIK y verificación de la confiabilidad de la plataforma del solicitante de acceso y el controlador de acceso $Result_{AIK-PCRs}$, y una firma del gestor de políticas en los resultados de autenticación del certificado AIK y verificación de la confiabilidad de la plataforma del solicitante de acceso y el controlador de acceso $[Result_{AIK-PCRs}]_{Sig}$. Los resultados de autenticación del certificado AIK y verificación de la confiabilidad de la plataforma del solicitante de acceso y el controlador de acceso $[Result_{AIK-PCRs}]$ generados en la etapa (3.4) incluyen el número aleatorio N_{AC} y el número aleatorio N_S generados por el controlador de acceso, el certificado AIK del solicitante de acceso $Cert_{AR-AIK}$, un resultado de la verificación del certificado AIK del solicitante de acceso Re_{AR-AIK}, los valores de PCRs solicitados por el controlador de acceso $PCRs_{AR}$, un resultado de la verificación de la confiabilidad de la plataforma del solicitante de acceso Re_{AR}, información de corrección de la

configuración de la plataforma del solicitante de acceso Rem_{AR}, el número aleatorio generado por el solicitante de acceso N_{AR}, el certificado AIK del controlador de acceso $Cert_{AC-AIK}$, un resultado de la verificación del certificado AIK del controlador de acceso Re_{AC-AIK}, los valores de PCRs solicitados por el solicitante de acceso $PCRs_{AC}$, un resultado de la verificación de la confiabilidad de la plataforma del controlador de acceso RE_{AC}, información de corrección de la configuración de la plataforma del controlador de acceso Rem_{AC}.

(3.5) Al recibir la información transmitida desde el gestor de políticas en la etapa (3.4), el controlador de acceso verifica primero si el número aleatorio N_{AC} y el número aleatorio N_S generados por el controlador de acceso, el certificado AIK del solicitante de acceso $Cert_{AR-AIK}$, los valores PCRs solicitados al controlador de acceso $PCRs_{AR}$, el número aleatorio generado por el solicitante de acceso N_{AR}, el certificado AIK del controlador de acceso $Cert_{AC-AIK}$ y los valores PCRs solicitados por el solicitante de acceso $PCRs_{AC}$ son consistentes con elementos correspondientes en la información transmitida desde el controlador de acceso en la etapa (3.1.3); a continuación verifica la firma $[Result_{AIK-PCRs}]$ del gestor de políticas para la validez con una clave pública correspondiente al certificado de identidad del gestor de políticas; después genera un resultado de acceso confiable Re_{Access} y un resultado de evaluación de la confiabilidad de la plataforma del solicitante de acceso de acuerdo con el resultado de la verificación del certificado AIK Re_{AR-AIK} del solicitante de acceso y el resultado de la verificación de la confiabilidad de la plataforma Re_{AR} del solicitante de acceso. Finalmente, el controlador de acceso transmite al solicitante de acceso la información transmitida en la etapa (3.4), el número aleatorio generado por el solicitante de acceso N_{AR}, el resultado del acceso confiable Re_{Access} y una firma del controlador de acceso, con la clave privada AIK en el Módulo de Plataforma Confiable (TPM), en los valores de PCRs extraídos al Módulo de Plataforma Confiable (TPM) y el número aleatorio generado por el solicitante de acceso N_{AR}, $[N_{AR}, PCRs_{AC}]_{Sig}$. En el proceso de generar el resultado de la evaluación de la confiabilidad de plataforma del solicitante de acceso en la etapa (3.5), el controlador de acceso repetirá la etapa (3.1) a la etapa (3.6) para intercambiar y verificar la información de la confiabilidad de nuevo con el solicitante de acceso si el controlador de acceso no está satisfecho con el resultado o con la demanda de otra política de red, donde el proceso de verificación del certificado AIK para la validez y un proceso adicional de verificación de la confiabilidad de la plataforma realizado por el solicitante de acceso en el controlador de acceso puede ser opcional si es necesario.

(3.6) Al recibir la información transmitida desde el controlador de acceso en la etapa (3.5), el solicitante de acceso verifica primero si el número aleatorio generado por el controlador de acceso N_S, el certificado AIK del solicitante de acceso $Cert_{AR-AIK}$, los valores de PCRs solicitados por el controlador de acceso $PCRs_{AR}$ y el número aleatorio generado por el solicitante de acceso N_{AR} son consistentes con elementos correspondientes en la información transmitida desde el solicitante de acceso en la etapa (3.2) y verifica la firma AIK del controlador de acceso $[N_{AR}, PCRs_{AC}]_{Sig}$ para la validez con una clave pública en el certificado AIK del controlador de acceso; entonces verifica la validez de la firma del gestor de políticas $[Result_{AIK-PCRs}]$ con la clave pública correspondiente al certificado de identidad del gestor de políticas; y finalmente genera un resultado de la verificación de la confiabilidad de la plataforma del controlador de acceso de acuerdo con el resultado de la verificación del certificado AIK del controlador de acceso Re_{AC-AIK} y el resultado de la verificación de la confiabilidad de la plataforma del controlador de acceso Re_{AC}. En el proceso de generar el resultado de la evaluación de la confiabilidad de plataforma del solicitante de acceso en la etapa (3.6), el solicitante de acceso repetirá la etapa (3.2) a la etapa (3.6) para intercambiar y verificar información de la confiabilidad de nuevo con el controlador de acceso si el solicitante de acceso no está satisfecho con el resultado o bajo demanda de otra política de red, donde el proceso de verificación del certificado AIK para su validez y un proceso adicional de verificación de la confiabilidad de plataforma realizado por el controlador de acceso en el solicitante de acceso puede ser opcional si es necesario.

En una implementación específica de la evaluación de la confiabilidad de plataforma anterior, el registro de medición correspondiente a los valores de los registros de configuración de plataforma (PCRs) del solicitante de acceso se transmitirán al gestor de políticas mientras se cifra y la información de corrección de la configuración de la plataforma del solicitante de acceso generado por el gestor de políticas también se transmitirá al solicitante de acceso mientras se cifra; y la información de corrección de la configuración de la plataforma también se transmitirá al solicitante de acceso mientras de cifra; e igualmente el registro de medición correspondiente a los valores de los registros de configuración de plataforma (PCRs) del controlador de acceso se transmitirá al gestor de políticas mientras se cifra y la información de corrección de la configuración de plataforma del controlador de acceso generada por el gestor de políticas también se transmitirá al controlador de acceso mientras se cifra. Las técnicas de transmisión cifrada que pueden adoptarse aquí pueden incluir encriptación de clave simétrica y asimétrica.

(4.) El TNAC cliente y el TNAC servidor se generan de acuerdo con los resultados de la evaluación de la confiabilidad de la plataforma en el proceso de evaluación de la confiabilidad de la plataforma y transmiten las recomendaciones correspondientes respectivamente al solicitante de acceso y al controlador de acceso de modo que el solicitante de acceso y el controlador de acceso controlan puertos de acceso mutuo, respectivamente, de acuerdo con las recomendaciones.

En particular, la etapa (4) puede incluir las siguientes etapas:

El servidor de políticas de plataforma se genera en el proceso de evaluación de la confiabilidad de la plataforma y después transmite resultados de evaluación de la confiabilidad de la plataforma del solicitante de acceso y el controlador de acceso al TNAC cliente y el TNAC servidor.

El TNAC cliente y el TNAC servidor se generan de acuerdo con los resultados de la evaluación de la confiabilidad de plataforma generados por el servidor de políticas de plataforma y transmiten recomendaciones correspondientes respectivamente al solicitante de acceso a la red y al controlador de acceso a la red.

Las recomendaciones transmitidas desde el TNAC servidor y el TNA cliente al controlador de acceso a la red y al solicitante de acceso a la red pueden incluir permiso, prohibición o aislamiento.

El solicitante de acceso a la red y el controlador de acceso a la red controlan puertos, respectivamente, de acuerdo con las recomendaciones recibidas respectivamente para realizar de este modo el control de acceso mutuo del solicitante de acceso y el controlador de acceso.

Se observará que, si las recomendaciones recibidas por el solicitante de acceso a la red y el controlador de acceso a la red son aisladas, el solicitante de acceso a la red y el controlador de acceso a la red realizan la corrección de acuerdo con la información de corrección de la configuración de la plataforma recuperada respectivamente en el proceso de evaluación de la confiabilidad de la plataforma y después realizan de nuevo el proceso de evaluación de la confiabilidad de la plataforma. Tal como puede apreciarse, la invención puede realizar un control de múltiples niveles en un puerto controlado para mejorar, de este modo, la seguridad del control de acceso a la red confiable global.

Haciendo referencia a la figura 2, el control de puertos de acuerdo con la invención puede realizarse tal como sigue en una aplicación práctica:

Se definen dos tipos de puertos lógicos tanto para el solicitante de acceso como para el controlador de acceso: puertos no controlados y controlados. Un puerto no controlado del solicitante de acceso puede transportar los datos de autenticación de usuario y de protocolos de negociación de claves, datos de protocolo de evaluación de la confiabilidad de la plataforma y datos de servicio de corrección de la plataforma, y un puerto controlado del solicitante de acceso puede transportar solamente datos de servicio de aplicación. Un puerto no controlado del controlador de acceso puede transportar solamente los datos de autenticación de usuario y datos de protocolos de negociación de claves, y un puerto controlado del controlador de acceso puede realizar un control del transporte de los datos del protocolo de evaluación de la confiabilidad de la plataforma, datos de servicio de corrección de la plataforma y datos de servicio de aplicación en forma de control de múltiples niveles. El solicitante de acceso y el controlador de acceso controlan los puertos controlados de acuerdo con los resultados de la autenticación del usuario y los resultados de la evaluación de la confiabilidad de la plataforma.

Con referencia a la figura 2, puede llevarse a cabo un proceso específico de control de puertos de acuerdo con la invención tal como sigue:

(a) La entidad del solicitante de acceso en el sistema solicitante de acceso y la entidad de autenticación de usuario en el sistema controlador de acceso realizan una autenticación de usuario bidireccional y una negociación de claves a través de los puertos no controlados, y la entidad de autenticación de usuario en el sistema de controlador de acceso y la entidad de política de servicio de autenticación en el sistema de gestión de políticas intercambian información directamente. Tras la autenticación de usuario bidireccional satisfactoria, el puerto controlado no autenticado en el sistema controlador de acceso se cambia a un estado autenticado para que el puerto controlado del controlador de acceso pueda transportar los datos del protocolo de evaluación de la confiabilidad de la plataforma.

(b) La entidad del solicitante de acceso en el sistema solicitante de acceso, la entidad de evaluación de la confiabilidad de la plataforma en el sistema controlador de acceso y la entidad de servicio de políticas de evaluación en el sistema gestor de directivas ejecutan el protocolo de autenticación entre pares de tres elementos para realizar una evaluación de la confiabilidad bidireccional de la plataforma

entre el solicitante de acceso y el controlador de acceso. En el proceso de evaluación de la confiabilidad de la plataforma, la entidad solicitante de acceso en el sistema solicitante de acceso se comunica a través del puerto no controlado, la entidad de evaluación de la confiabilidad de la plataforma en el sistema controlador de acceso se comunica a través del puerto controlado autenticado, y la entidad de evaluación de la confiabilidad de la plataforma en el sistema controlador de acceso y la entidad de servicio de políticas de evaluación en el sistema de gestor de políticas intercambian información directamente.

Se observará que los siguientes cuatro casos pueden darse para el control de puertos del solicitante de acceso y el controlador de acceso después de que se realice la evaluación de la confiabilidad de la plataforma bidireccional. En un primer caso, si ambas plataformas del solicitante de acceso y el controlador de acceso son confiables, los puertos controlados no confiables tanto en el sistema solicitante de acceso como en el sistema controlador de acceso se cambian a un estado confiable para que los datos del servicio de aplicación puedan ser transportados entre el solicitante de acceso y el controlador de acceso. En un segundo caso, si la plataforma del solicitante de acceso es confiable y la plataforma del controlador de acceso es no confiable, no se cambian los estados de los puertos en el sistema solicitante de acceso y el sistema controlador de acceso, y el controlador de acceso recupera información de corrección de la plataforma de un dominio aislado conectado para la corrección de la plataforma. En un tercer caso, si la plataforma del solicitante de acceso no es confiable y la plataforma del controlador de acceso es confiable, el puerto controlado para el cual se ha desactivado la corrección en el sistema controlador de acceso se cambia a un estado en el que se ha activado la corrección para que el solicitante de acceso pueda acceder a un dominio aislado a través del sistema controlador de acceso para la corrección de la plataforma. En un cuarto caso, si ninguna de las plataformas del solicitante de acceso y del controlador de acceso es confiable, el puerto controlado para el cual se ha desactivado la corrección en el sistema de controlador de acceso se cambia a un estado en el cual se ha activado la corrección para que el solicitante de acceso pueda acceder a un dominio aislado a través del sistema controlador de acceso para la corrección de la plataforma y el controlador de acceso también recupere su información de corrección de la plataforma desde un dominio aislado conectado a la misma para la corrección de la plataforma.

REIVINDICACIONES

1. Método de control de acceso a una red confiable basado en autenticación entre pares de tres elementos, que comprende:

inicializar unos Colectores de Medición de la confiabilidad, TMCs, en una capa de medición de la confiabilidad,
ejecutar un protocolo de autenticación entre pares de tres elementos en base a un gestor de políticas que actúa como tercero mediante por un solicitante de acceso, un controlador de acceso y el gestor de políticas en una capa de control de acceso a la red para realizar una autenticación de usuario bidireccional entre el solicitante de acceso y el controlador de acceso;
cuando los resultados de la autenticación de usuario indican una autenticación satisfactoria, ejecutar el protocolo de autenticación entre pares de tres elementos en base al gestor de políticas que actúa como tercero por el solicitante de acceso, el controlador de acceso y el gestor de políticas en una capa de evaluación de la plataforma confiable para realizar una evaluación de la confiabilidad de la plataforma bidireccional entre el solicitante de acceso y el controlador de acceso;
generar, mediante un TNAC cliente del solicitante de acceso y un TNAC servidor del controlador de acceso, de acuerdo con resultados de evaluación de la confiabilidad de plataforma en el proceso de evaluación de la confiabilidad de la plataforma, y transmitir recomendaciones correspondientes respectivamente al solicitante de acceso y el controlador de acceso, de manera que el solicitante de acceso a la red y el controlador de acceso a la red controlan puertos de acceso mutuo respectivamente de acuerdo con las recomendaciones;

en el que el control de puertos se realiza tal como sigue:

un puerto no controlado del solicitante de acceso controla el transporte de datos de autenticación de usuario y de protocolos negociación de claves de sesión, datos de protocolo de evaluación de la confiabilidad de la plataforma y datos de servidor de corrección de la plataforma, y un puerto controlado del solicitante de acceso controla el transporte de datos de servicio de aplicación; y un puerto no controlado del controlador de acceso controla el transporte de datos de autenticación de usuario y de protocolos negociación de claves de sesión, y un puerto controlado del controlador de acceso controla el transporte de los datos de protocolo de evaluación de la confiabilidad de la plataforma, datos de servicio de corrección de la plataforma y datos de servicio de aplicación.

2. Método de control de acceso a una red confiable basado en autenticación entre pares de tres elementos de acuerdo con la reivindicación 1, caracterizado por el hecho de que el control de puertos se lleva a cabo tal como sigue:

(a) una entidad solicitante de acceso en el solicitante de acceso y una entidad de autenticación de usuario en el controlador de acceso realizan autenticación de usuario bidireccional y una negociación de claves de sesión a través de los puertos no controlados; y la entidad de autenticación de usuario en el controlador de acceso y una entidad de políticas de servicio de autenticación en el gestor de políticas intercambian información directamente; y tras una autenticación de usuario bidireccional satisfactoria, el puerto controlado del controlador de acceso cambia a un estado autenticado para permitir el transporte de los datos del protocolo de evaluación de la confiabilidad de la plataforma; y

(b) la entidad solicitante de acceso en el solicitante de acceso, una entidad de evaluación de la confiabilidad de la plataforma en el controlador de acceso y una entidad de servicio de políticas de evaluación en el gestor de políticas ejecutan el protocolo de autenticación entre pares de tres elementos para realizar una evaluación de la confiabilidad de la plataforma bidireccional entre el solicitante de acceso y el controlador de acceso; y en el proceso de evaluación de la confiabilidad de la plataforma, la entidad solicitante de acceso en el solicitante de acceso se comunica a través del puerto no controlado, la entidad de evaluación de la confiabilidad de la plataforma en el controlador de acceso se comunica a través del puerto controlado autenticado y la entidad de evaluación de la confiabilidad de la plataforma en el controlador de acceso y la entidad de servicio de políticas de evaluación en el gestor de políticas intercambian información directamente.

3. Método de control de acceso a una red confiable basado en autenticación entre pares de tres elementos de acuerdo con la reivindicación 2, caracterizado por el hecho de que el control de puertos del solicitante de acceso y el controlador de acceso se lleva a cabo tal como sigue después de que se lleve a cabo el proceso de evaluación de la confiabilidad de plataforma:

si ambas plataformas del solicitante de acceso y el controlador de acceso son confiables, tanto los puertos controlados en el solicitante de acceso como el controlador de acceso están en un estado confiable de modo que se permite el transporte de datos de servicio de aplicación entre el solicitante de acceso y el controlador de acceso; o

si la plataforma del solicitante de acceso es confiable y la plataforma del controlador de acceso no es confiable, los puertos no controlados y controlados del solicitante de acceso y el controlador de acceso están en un estado original y el controlador de acceso recupera información de corrección de configuración de la plataforma de un dominio aislado conectado para la corrección de la plataforma; o

si la plataforma del solicitante de acceso no es confiable y la plataforma del controlador de acceso es confiable, se cambia el puerto controlado para el cual se deshabilita la corrección del controlador de acceso a un estado en el que se ha habilitado la corrección para que el solicitante de acceso pueda acceder a un dominio aislado a través del controlador de acceso para recuperar la información de corrección de la configuración de la plataforma para la corrección de la plataforma; o

si ninguna de las plataformas del solicitante de acceso y del controlador de acceso es confiable, el puerto controlado para el cual está desactivada la corrección del controlador de acceso se cambia a un estado en el que se ha habilitado la corrección para que el solicitante de acceso pueda acceder a un dominio aislado a través del controlador de acceso para recuperar la información de corrección de la configuración de la plataforma para la corrección de la plataforma.

4. Método de control de acceso a una red confiable basado en autenticación entre pares de tres elementos de acuerdo con una cualquiera de las reivindicaciones 1 a 3, caracterizado por el hecho de que las recomendaciones comprenden información de permiso de acceso, información de prohibición de acceso o información de aislamiento y corrección.

5. Método de control de acceso a una red confiable basado en autenticación entre pares de tres elementos de acuerdo con la reivindicación 4, caracterizado por el hecho de que cuando las recomendaciones recibidas por el controlador de acceso a la red y el solicitante de acceso a la red son información de aislamiento y corrección, el solicitante de acceso y el controlador de acceso realizan una corrección de la plataforma a través de información de corrección de la configuración de la plataforma y realizan el proceso de evaluación de la confiabilidad de la plataforma entre el solicitante de acceso y el controlador de acceso.

6. Método de control de acceso a una red confiable basado en autenticación entre pares de tres elementos de acuerdo con la reivindicación 3, caracterizado por el hecho de que la evaluación de la confiabilidad de la plataforma se lleva a cabo tal como sigue:

se realiza una autenticación de credenciales de la plataforma:
el gestor de políticas verifica certificados AIK del solicitante de acceso y el controlador de acceso para la validez; y
se realiza una verificación de la confiabilidad de la plataforma: el gestor de políticas verifica la confiabilidad de la plataforma del solicitante de acceso y del controlador de acceso.

7. Método de control de acceso a una red confiable basado en autenticación entre pares de tres elementos de acuerdo con la reivindicación 6, caracterizado por el hecho de que el proceso de evaluación de la confiabilidad de plataforma entre el solicitante de acceso y el controlador de acceso comprende:

transmitir información que identifica la configuración de la plataforma del solicitante de acceso entre el solicitante de acceso y el gestor de políticas e información que identifica la configuración de la plataforma del controlador de acceso entre el controlador de acceso y el gestor de políticas a través de transmisión cifrada;
transmitir información intercambiada entre el TNAC cliente y el TNAC servidor utilizando una clave de sesión; y
generar y transmitir, por el gestor de políticas, los resultados de la evaluación de la confiabilidad de la plataforma del solicitante de acceso y el controlador de acceso al TNAC cliente y al TNAC servidor.

8. Método de control de acceso a una red confiable basado en autenticación entre pares de tres elementos de acuerdo con la reivindicación 1, caracterizado por el hecho de que un proceso de autenticación de usuario entre el solicitante de acceso y el controlador de acceso comprende:

iniciar una petición de acceso desde el solicitante de acceso al controlador de acceso;
iniciar, mediante el controlador de acceso, el proceso de autenticación de usuario tras la recepción de la petición de acceso y generar resultados de autenticación de usuario del solicitante de acceso y el controlador de acceso;

generar, mediante el solicitante de acceso y el controlador de acceso, una clave primaria entre ellos tras una autenticación de usuario satisfactoria; y
negociar, mediante el solicitante de acceso y el controlador de acceso, una clave de sesión utilizando la clave primaria y transmitir información de autenticación de usuario satisfactoria, respectivamente, al TNAC cliente y al TNAC servidor.

9. Método de control de acceso a una red confiable basado en autenticación entre pares de tres elementos de acuerdo con la reivindicación 8, caracterizado por el hecho de que inicializar los Colectores de Medición de Confiabilidad, TMCs, en la capa de medición de la confiabilidad, comprende:

inicializar, mediante el TNAC cliente del solicitante de acceso y el TNAC servidor del controlador de acceso, los Colectores de Medición de la Confiabilidad, TMCs, en la capa de medición de la confiabilidad para recoger información de la confiabilidad requerida para cada uno;
almacenar, mediante unos Módulos de Plataforma Confiable, TPMs, del solicitante de acceso y el controlador de acceso, la información de la confiabilidad requerida para cada uno en unos Registros de Configuración de la Plataforma, PCRs;
preparar, mediante el TNAC cliente del solicitante de acceso y el TNAC servidor del controlador de acceso, información de la confiabilidad de la plataforma requerida para el controlador de acceso y el solicitante de acceso, respectivamente, a través de los Colectores de Medición de la Confiabilidad, TMCs; y establecer y distribuir, mediante el gestor de políticas, políticas de control de acceso que comprenden una política del solicitante de acceso para unirse a una red conectada y una política de control de acceso a la red del controlador de acceso para el solicitante de acceso.

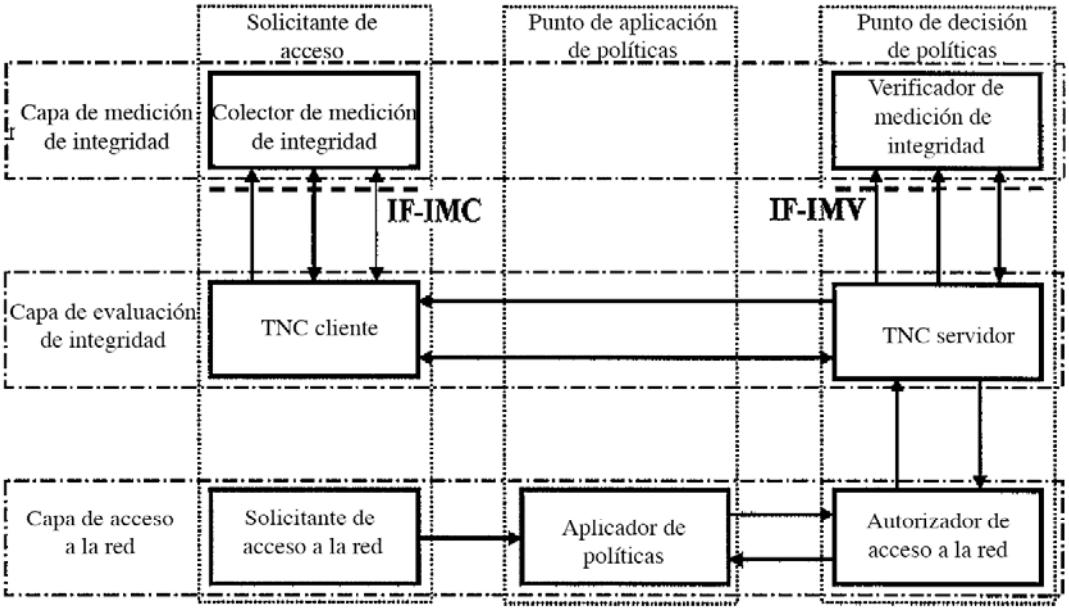
Solicitante de acceso
Punto de aplicación de políticas
Punto de decisión de políticas
Capa de medición de integridad
Colector de medición de integridad
Verificador de medición de integridad
IF-IMC
IF-IMV
Capa de evaluación de integridad
TNC cliente
TNC servidor
Capa de acceso a la red
Solicitante de acceso a la red
Aplicador de políticas
Autorizador de acceso a la red

Fig.1

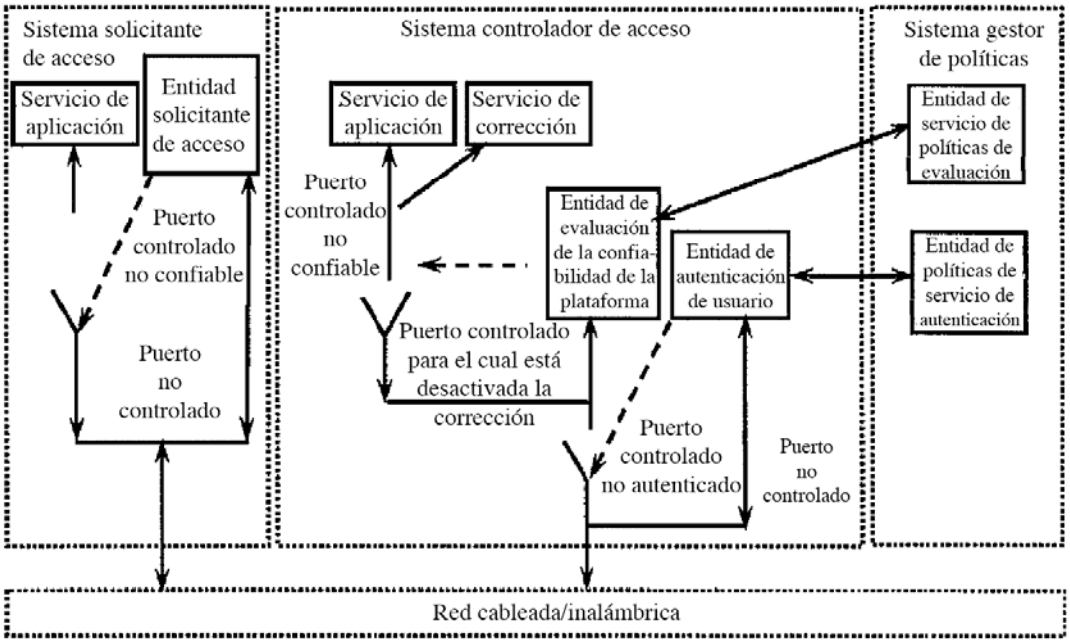
Sistema solicitante de acceso
Servicio de aplicación
Entidad solicitante de acceso
Puerto controlado no confiable
Puerto no controlado
Sistema controlador de acceso
Servicio de aplicación
Servicio de corrección
Puerto controlado no confiable
Entidad de evaluación de la confiabilidad de la plataforma
Entidad de autenticación de usuario
Puerto controlado para el cual está desactivada la corrección
Puerto controlado no autenticado
Puerto no controlado
Sistema gestor de políticas
Entidad de servicio de políticas de evaluación
Entidad de políticas de servicio de autenticación
Red cableada/inalámbrica

Fig.2

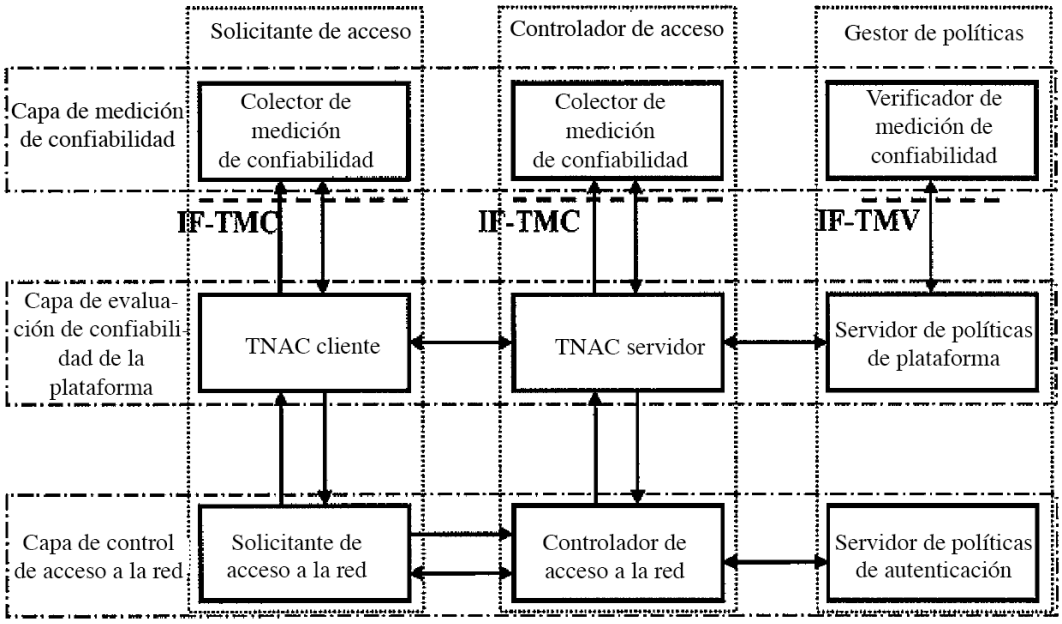
Solicitante de acceso
Controlador de acceso
Gestor de políticas
Capa de medición de confiabilidad
Colector de medición de confiabilidad
Colector de medición de confiabilidad
Verificador de medición de confiabilidad
IF-TMC
IF-TMC
IF-TMV
Capa de evaluación de confiabilidad de la plataforma
TNAC cliente
TNAC servidor
Servidor de políticas de plataforma
Capa de control de acceso a la red
Solicitante de acceso a la red
Controlador de acceso a la red
Servidor de políticas de autenticación

Fig.3

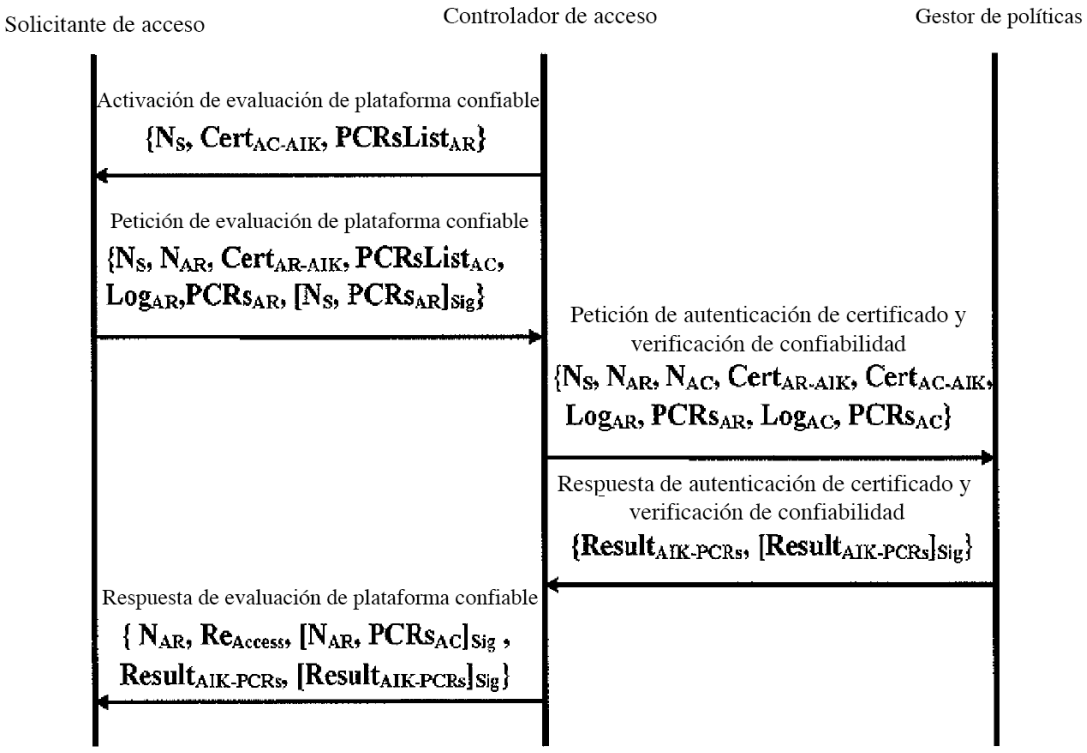
Solicitante de acceso
Controlador de acceso
Gestor de políticas
Activación de evaluación de plataforma confiable
{NS, CertAC-AIK, PCRsListAR}
Petición de evaluación de plataforma confiable
{NS, NAR, CertAR-AIK, PCRsListAC, LogAR,PCRsAR, [NS, PCRsAR]Sig}
Petición de autenticación de certificado y verificación de confiabilidad
{NS, NAR, NAC, CertAR-AIK, CertAC-AIK, LogAR, PCRsAR, LogAC, PCRsAC}
Respuesta de autenticación de certificado y verificación de confiabilidad
{ResultAIK-PCRs, [ResultAIK-PCRs]Sig}
Respuesta de evaluación de plataforma confiable
{ NAR, ReAccess, [NAR, PCRsAC]Sig , ResultAIK-PCRs, [ResultAIK-PCRs]Sig}

Fig.4

REFERENCIAS CITADAS EN LA DESCRIPCIÓN

Esta lista de referencias citadas por el solicitante es únicamente para la comodidad del lector. No forma parte del documento de la patente europea. A pesar del cuidado tenido en la recopilación de las referencias, no se pueden excluir errores u omisiones y la EPO niega toda responsabilidad en este sentido.

Documentos de patentes citados en la descripción

• CN 200710019093 **[0001]**