(19) OFICINA ESPAÑOLA DE PATENTES Y MARCAS

ESPAÑA

(11) Número de publicación: **2 378 816**

(51) Int. CI.:
H04L 29/06 (2006.01)
H04L 29/08 (2006.01)

(12) TRADUCCIÓN DE PATENTE EUROPEA T3

(96) Número de solicitud europea: **03756482 .0**
(96) Fecha de presentación: **20.10.2003**
(97) Número de publicación de la solicitud: **1676409**
(97) Fecha de publicación de la solicitud: **05.07.2006**

(54) Título: **Red y nodo para proporcionar una transmisión segura de mensajes de parte de aplicación móvil**

(45) Fecha de publicación de la mención BOPI:
18.04.2012

(45) Fecha de la publicación del folleto de la patente:
18.04.2012

(73) Titular/es:
Telefonaktiebolaget LM Ericsson (publ)
164 83 Stockholm , SE

(72) Inventor/es:
PEKKALA, Reijo;
SÄÄSKILAHTI, Juha y
WIREN, Karl-Johan

(74) Agente/Representante:
de Elzaburu Márquez, Alberto

Aviso: En el plazo de nueve meses a contar desde la fecha de publicación en el Boletín europeo de patentes, de la mención de concesión de la patente europea, cualquier persona podrá oponerse ante la Oficina Europea de Patentes a la patente concedida. La oposición deberá formularse por escrito y estar motivada; sólo se considerará como formulada una vez que se haya realizado el pago de la tasa de oposición (art. 99.1 del Convenio sobre concesión de Patentes Europeas).

DESCRIPCIÓN

Red y nodo para proporcionar una transmisión segura de mensajes de parte de aplicación móvil

Campo de la invención

La invención se refiere a una red y un nodo para proporcionar una transmisión segura de mensajes de parte de aplicación móvil.

Descripción del la técnica anterior

La invención se refiere a una capa de protocolo para cifrar y descifrar mensajes de acuerdo con el protocolo de parte de aplicación móvil (MAP). El protocolo MAP es un protocolo de aplicaciones en la pila de protocolos de acuerdo con el sistema de señalización número 7 (SS7). El protocolo MAP que ha sido desarrollado para redes móviles de acuerdo con el estándar del Sistema Global para Comunicaciones Móviles (GSM). El protocolo MAP se usa para consultar bases de datos en redes GSM, tal como un Registro de Posición de Visitante (VLR) o un Registro de Ubicación Local (HLR). La transmisión de mensajes MAP se puede asegurar por un cifrado de un mensaje MAP en un nodo de envío y un descifrado de un mensaje MAP en un nodo de recepción. El cifrado y descifrado de mensajes MAP es parte de una seguridad de la capa de aplicaciones MAP que se describe en la especificación técnica (TS) 33.200 del proyecto de cooperación de tercera generación (3GPP).

Actualmente la necesidad de asegurar la transmisión de mensajes MAP ha llegado a ser destacada en redes que se usan comúnmente por operadores entre los cuales no se ha desarrollado aún una relación de confianza con una plena extensión.

De acuerdo con el estado de la técnica se implementan una unidad para cifrar y descifrar mensajes MAP y una petición de protocolo MAP en un nodo físico común. Esto no es flexible y esto se relaciona con costes de implementación grandes si la seguridad de la capa de aplicaciones MAP se introduce en una red que comprende un gran número de nodos de red diferentes.

La WO0211395 revela un método y un sistema para establecer una conexión de señalización asegurada, en el que una primera entidad de red obtiene parámetros de seguridad de una segunda red y usa estos para asegurar la información a ser transmitida a una segunda entidad de red.

Objeto de la invención

Por lo tanto es un objeto de la invención superar las desventajas del estado de la técnica y proporcionar una implementación flexible y rentable de la seguridad de la capa de aplicaciones MAP.

Resumen de la invención

Este objeto se resuelve mediante la red de la reivindicación 1. La invención también se realiza en un nodo pasarela de acuerdo con la reivindicación 6. Las realizaciones ventajosas se describen en las reivindicaciones dependientes.

De acuerdo con la presente invención una red de telecomunicación con un primer dominio comprende al menos una petición de protocolo de parte de aplicación móvil conectado con un nodo pasarela el cual se adapta para enviar y recibir mensajes de la parte de aplicación móvil y el cual es conectable a un segundo dominio. La red de telecomunicación es notable porque el nodo pasarela está adaptado para recibir un mensaje de la parte de aplicación móvil desde el primer dominio, para convertir el mensaje de la parte de aplicación móvil recibido obteniendo un mensaje de la parte de aplicación móvil asegurado, y para enviar el mensaje obtenido hacia el segundo dominio. El nodo pasarela además se adapta para recibir un mensaje de la parte de aplicación móvil asegurado desde el segundo dominio, para extraer un mensaje de la parte de aplicación móvil no asegurado a partir del mensaje de la parte de aplicación móvil asegurado recibido y para enviar el mensaje extraído hacia el primer dominio.

Esto proporciona un método flexible para implementar seguridad de la capa de aplicaciones de la parte de aplicación móvil, ya que una petición adicional de protocolo de parte de aplicación móvil se puede añadir fácilmente al primer dominio. Además una implementación rentable de la seguridad de la capa de aplicaciones de la parte de aplicación móvil se proporciona a un primer dominio que comprende diferentes tipos de nodos de red en los cuales se implementa el protocolo de la parte de aplicación móvil.

En una realización adicional de la red de telecomunicación el nodo pasarela es conectable a un tercer dominio y el nodo pasarela realiza un descarte selectivo de mensajes de la parte de aplicación móvil recibidos desde el primer dominio y destinados al tercer dominio y un descarte selectivo de mensajes de la parte de aplicación móvil recibidos desde el tercer dominio y destinados al primer dominio.

Mediante esto se proporciona una comunicación asegurada por el nodo pasarela hacia diferentes dominios. También se puede proporcionar un nivel básico de seguridad por el nodo pasarela si se transmiten mensajes no cifrados en el tercer dominio.

En otra realización de la red de telecomunicación, el nodo pasarela funciona como un cortafuegos hacia el tercer dominio.

En una realización ventajosa de la red de telecomunicación el nodo pasarela es conectable a distintos dominios, y los niveles de seguridad son configurables para los distintos dominios. Mediante esto se puede proporcionar una comunicación segura por el nodo pasarela de una forma flexible.

En una realización ventajosa de la red de telecomunicación un nivel de seguridad es configurable para un dominio independientemente de una configuración de un nivel de seguridad para otro dominio. Mediante esto se puede proporcionar una comunicación segura por el nodo pasarela en una forma flexible.

En una realización ventajosa adicional de la red de telecomunicación para un dominio particular un repliegue a un nivel más bajo de seguridad que el nivel configurado de seguridad para el dominio particular es admisible y la admisión del repliegue al nivel más bajo de seguridad es configurable para un dominio independientemente de una configuración de una admisión de un repliegue respectivo a un nivel más bajo de nivel de seguridad para otro dominio.

Mediante esto se puede permitir un repliegue a un nivel más bajo de seguridad de acuerdo con un nivel de confianza hacia un dominio. Esto proporciona una forma flexible y segura para conectar el primer dominio a otros diferentes dominios de las redes de telecomunicación.

En otra realización de la invención un nodo pasarela comprende una interfaz a un primer dominio de una red de telecomunicación para enviar y recibir mensajes de la parte de aplicación móvil. El nodo pasarela es notable porque comprende una interfaz a un segundo dominio de la red de telecomunicación para enviar y recibir mensajes de la parte de aplicación móvil asegurada. El nodo pasarela además comprende una unidad de conversión que está adaptada para recibir un mensaje de la parte de aplicación móvil a través de la interfaz con el primer dominio, para convertir el mensaje de la parte de aplicación móvil recibido obteniendo un mensaje de la parte de aplicación móvil asegurado, y para enviar el mensaje obtenido a través de la interfaz hacia el segundo dominio. La unidad de conversión se adapta además para recibir un mensaje de la parte de aplicación móvil asegurado a través de la interfaz con el segundo dominio, para extraer un mensaje de la parte de aplicación móvil no asegurado a partir del mensaje de la parte de aplicación móvil asegurado recibido y para enviar el mensaje extractado a través de la interfaz hacia el primer dominio.

Esto proporciona un método flexible para implementar seguridad de capa de aplicaciones de la parte de aplicación móvil, ya que una petición de protocolo de la parte de aplicación móvil adicional se puede añadir fácilmente al primer dominio. Además una implementación rentable de la seguridad de la capa de aplicaciones de la parte de aplicación móvil se proporciona a un primer dominio que comprende diferentes tipos de nodos de red en los cuales se implementa el protocolo de la parte de aplicación móvil.

En una realización adicional del nodo pasarela, el nodo pasarela comprende una interfaz con un tercer dominio para enviar y recibir mensajes de la parte de aplicación móvil y una unidad de filtrado adaptada para realizar un descarte selectivo de los mensajes de la parte de aplicación móvil.

Mediante esto se proporciona una comunicación asegurada por el nodo pasarela hacia diferentes dominios. También se puede proporcionar un nivel básico de seguridad por el nodo pasarela si se transmiten mensajes no cifrados en el tercer dominio.

En otra realización ventajosa del nodo pasarela el nodo pasarela funciona como un cortafuegos hacia el tercer dominio.

En una realización ventajosa adicional del nodo pasarela, el nodo pasarela es conectable a diferentes dominios, y el nodo pasarela comprende una base de datos de seguridad para almacenar las indicaciones de los niveles de seguridad para los diferentes dominios. Mediante esto se puede proporcionar una comunicación segura por el nodo pasarela de una forma flexible.

En otra realización ventajosa del nodo pasarela, un nivel de seguridad es configurable para un dominio independientemente de una configuración de un nivel de seguridad para otro dominio. Mediante esto se puede proporcionar una comunicación segura por el nodo pasarela de una forma flexible.

En una realización ventajosa adicional del nodo pasarela, el nodo pasarela comprende un almacén de repliegue para almacenar para un dominio particular una indicación de que un repliegue a un nivel más bajo de seguridad que el nivel configurado de seguridad para el dominio particular es admisible y la admisión del repliegue al nivel más bajo de seguridad es configurable para un dominio independientemente de una admisión de un repliegue respectivo a un nivel más bajo de seguridad para otro dominio.

Mediante esto se puede permitir un repliegue a un nivel más bajo de seguridad de acuerdo con un nivel de confianza hacia un dominio. Esto proporciona una forma flexible y segura para conectar el primer dominio con otros diferentes dominios de la red de telecomunicación.

Breve descripción de los dibujos

Las siguientes figuras muestran:

La Figura 1 representa una red de comunicación de telecomunicación que proporciona una transmisión de mensajes de la parte de aplicación móvil entre un primer dominio y dominios adicionales, en que se proporcionan diferentes tipos de mecanismos de seguridad.

La Figura 2 representa una arquitectura de un nodo pasarela para convertir un mensaje MAP recibido obteniendo un mensaje MAP asegurado, y para extraer un mensaje MAP no cifrado a partir de un mensaje MAP asegurado.

La Figura 3 representa un diagrama de flujo que comprende los pasos de decisión y los pasos de procesamiento que se realizan durante la puesta en marcha de un canal de comunicación seguro.

Descripción detallada de realizaciones

A continuación la invención se describe en más detalle por medio de realizaciones y figuras. Signos de referencia iguales indican elementos iguales.

La Figura 1 representa una red de telecomunicación que comprende un primer dominio PLMN-A, un segundo dominio PLMN-B, un tercer dominio PLMN-E, un cuarto dominio PLMN-C, y un quinto dominio PLMN-D. Un dominio puede ser por ejemplo una subred y los diferentes dominios pueden ser subredes operadas por diferentes operadores de red.

Los dominios diferentes de la red de telecomunicación comprenden nodos de red en los que se implementan peticiones de protocolo del protocolo MAP (parte de aplicación móvil). Los canales de comunicación entre los nodos de red que están asegurados porque los mensajes MAP se transmiten como mensajes de seguridad MAP se representan como líneas gruesas continuas. Los canales de comunicación entre nodos de red a través de los cuales se transmiten los mensajes de la parte de aplicación móvil como mensajes no asegurados se representan como líneas finas continuas. Las conexiones para intercambiar claves para el cifrado o descifrado y otros tipos de información de seguridad usada para una seguridad de la capa de transporte de la parte de aplicación móvil se representa como flechas con puntas dobles discontinuas. Las conexiones para proporcionar información de seguridad por una base de datos de seguridad a un nodo de red en la cual se implementa una petición de protocolo de la parte de aplicación móvil se implementan como líneas de puntos.

El primer dominio PLMN-A comprende un primer y un segundo nodo de red NEA1 y NEA2 en los cuales se instalan peticiones de protocolo MAP. El primer dominio PLMN-A se considera como un dominio seguro de la red de telecomunicación. Por lo tanto no se aplica cifrado a los mensajes MAP y los mensajes MAP no cifrados se pueden intercambiar por las peticiones del protocolo MAP dentro del primer dominio PLMN-A.

Para proporcionar una conexión de las peticiones de protocolo MAP en el primer dominio PLMA-A con otras peticiones de protocolo MAP en los otros dominios de la red de telecomunicación, el primer y el segundo nodo de red NEA1 y NEA2 son conectables a otros nodos de red a través de un primer nodo pasarela MSEGA. Los mensajes MAP desde las peticiones de protocolo MAP en el primer dominio PLMN-A a las peticiones de protocolo MAP en los otros dominios se encaminan dentro del primer dominio PLMN-A hacia el primer nodo pasarela MSEGA. Por consiguiente los mensajes MAP cifrados y los mensajes MAP no cifrados desde otros dominios se encaminan hacia las peticiones de protocolo MAP en el primer dominio a través del primer nodo pasarela MSEGA.

El primer nodo pasarela MSEGA proporciona un cifrado de mensajes MAP recibidos desde las peticiones de protocolo dentro del primer dominio PLMN-A en el que el cifrado cumple con la seguridad de la capa de aplicaciones MAP. Los mensajes cifrados se obtienen cifrando dicho cumplimiento con la seguridad de la capa de aplicaciones MAP. Por consiguiente el primer nodo pasarela MSEGA proporciona un descifrado de los mensajes MAP asegurados el contenido de los cuales se destina a las peticiones de protocolo MAP en el primer dominio PLMN-A y que se reciben desde dominios de la red de telecomunicación distintos del primer dominio PLMN-A. Los mensajes descifrados obtenidos descifrando dicho cumplimiento con el protocolo MAP.

En una realización ventajosa del primer nodo pasarela MSEGA el primer nodo pasarela MSEGA comprende una base de datos de seguridad que almacena y proporciona información de seguridad usada para el cifrado de mensajes MAP y el descifrado de mensajes MAP asegurados. Tal información de seguridad comprende claves para cifrar los mensajes MAP, claves para descifrar los mensajes MAP asegurados y las políticas de seguridad a ser aplicadas. Para proporcionar un intercambio de dicha información de seguridad el primer nodo pasarela MSEGA se conecta con otras bases de datos que almacenan y proporcionan información de seguridad. En particular la base de datos de seguridad dentro del primer nodo pasarela MSEGA se conecta a una base de datos de seguridad en un segundo nodo pasarela MSEGB a través de una primera conexión de intercambio de información de seguridad IKEC_AB. Además la base de datos de seguridad dentro del primer nodo pasarela MSEGA se conecta con una primera base de datos de seguridad KACC en el cuarto dominio PLMN-C a través de una segunda conexión de intercambio de información de seguridad IKEC_AC y con una segunda base de datos de seguridad KACE en el tercer dominio PLMN-E a través de una tercera conexión de intercambio de información de seguridad IKEC_AE.

El segundo dominio PLMN-B comprende un tercer y un cuarto nodo de red NEB1 y NEB2, que están conectados con el primer y el segundo nodo de red NEA1 y NEA2 en el primer dominio PLMN-A a través del segundo nodo pasarela MSEGB. El tercer y el cuarto nodo de red NEB1 y NEB2 cada uno comprende peticiones de protocolo MAP. El segundo dominio PLMN-B se considera como un dominio seguro de la red de telecomunicación. Por lo tanto no se aplica cifrado a los mensajes MAP dentro del segundo dominio y los mensajes MAP no cifrados se pueden intercambiar por las peticiones de protocolo MAP dentro del segundo dominio PLMN-B. Una transmisión de mensajes MAP asegurados entre el primer nodo pasarela MSEGA y el segundo nodo pasarela MSEGB se proporciona por el primer canal de transmisión asegurado SC_AB.

Los mensajes MAP desde el segundo dominio PLMN-B a otros dominios se encamina a través del segundo nodo pasarela MSEGB y los mensajes MAP asegurados hacia el segundo dominio PLMN-B se encaminan en consecuencia a través del segundo nodo pasarela MSEGB. Ya que una transmisión de mensajes no cifrados entre el primer y el segundo dominio PLMN-A y PLMN-B no se considera como segura, los mensajes MAP entre el primer y el segundo dominio PLMN-A y PLMN-B se transmiten como mensajes MAP cifrados a través del primer canal de transmisión asegurado SC_AB. Por lo tanto un mensaje MAP desde una petición de protocolo en el primer dominio PLMN-A a una petición de protocolo en el segundo dominio PLMN-B se encamina en el primer dominio PLMN-A hacia el primer nodo pasarela MSEGA. El mensaje MAP se recibe en el primer nodo pasarela MSEGA, cifrado aplicando el cifrado que cumple con la seguridad de la capa de aplicaciones MAP y enviado como el mensaje MAP cifrado a través del primer canal de transmisión asegurado SC_AB al segundo nodo pasarela MSEGB dentro del segundo dominio PLMN-B. El mensaje MAP cifrado se descifra en el segundo nodo pasarela MSEGB obteniendo un mensaje MAP que comprende el contenido del mensaje MAP original enviado en el primer dominio PLMN-A. El mensaje MAP obtenido se encamina en el segundo dominio PLMN-B hacia una petición de protocolo MAP que termina el mensaje MAP.

Por consiguiente un mensaje MAP desde una petición de protocolo MAP en el segundo dominio PLMN-B y destinado a una petición de protocolo MAP en el primer dominio PLMN-A se encamina en el segundo dominio PLMN-B hacia el segundo nodo pasarela MSEGB, cifrado obteniendo un mensaje MAP asegurado que se transmite a través del primer canal de transmisión asegurado SC_AB al primer nodo pasarela MSEGA en el primer dominio PLMN-A. En el primer nodo pasarela MSEGA el mensaje MAP asegurado se descifra obteniendo un mensaje MAP que comprende el contenido del mensaje MAP original enviado en el segundo dominio PLMN-B. El mensaje MAP obtenido se encamina en el primer dominio PLMN-A hacia una petición de protocolo MAP destino que termina el mensaje MAP.

El cuarto dominio PLMN-C de la red de telecomunicación comprende un quinto y un sexto nodo de red NEC1 y NEC2, en cada uno de los cuales están instaladas una petición de protocolo MAP y una unidad de conversión para el cifrado y descifrado del mensaje MAP. La petición de protocolo MAP en el quinto y el sexto nodo de red NEC1 y NEC2 respectivamente están conectados con el primer nodo pasarela MSEGA a través de un segundo y un tercer canal de transmisión asegurado SC_AC1 y SC_AC2 respectivamente. El cuarto dominio PLMN-C además comprende una primera base de datos de seguridad KACC que almacena y que proporciona información de seguridad usada por el cifrado de mensajes MAP y la descripción de mensajes MAP asegurados. La primera base de datos de seguridad KACC proporciona información de seguridad a las unidades de conversión en el quinto y el sexto nodo de red NEC1 y NEC2. Para proporcionar un intercambio de información de seguridad la primera base de datos de seguridad KACC está conectada con la base de datos de seguridad en el primer nodo pasarela MSEGA a través de una segunda conexión de intercambio de información de seguridad IKEC_AC.

O bien la transmisión de mensajes MAP no cifrados en el cuarto dominio PLMN-C o bien la transmisión de mensajes MAP no cifrados desde el cuarto dominio PLMN-C a otros dominios por ejemplo al primer dominio PLMN-A no se considera segura. Los mensajes MAP entre las peticiones de protocolo MAP en el primer dominio PLMN-A y las peticiones de protocolo MAP en el cuarto dominio PLMN-C están por lo tanto cifradas y se transmiten como mensajes MAP asegurados. El cifrado y descifrado del mensaje para las peticiones de protocolo MAP en el quinto y el sexto nodo de red NEC1 y NEC2 se realiza por las unidades de conversión respectivas en el quinto y sexto nodo de red NEC1 y NEC2 respectivamente. La transmisión de mensajes MAP asegurados entre el primer y el cuarto dominio, PLMN-A y PLMN-C muestra que la solución inventada es compatible con la implementación de seguridad de capa de aplicaciones MAP de acuerdo con el estado de la técnica, en la que la unidad de conversión para el cifrado y descifrado del mensaje MAP se proporciona para cada petición de protocolo MAP.

A continuación el cifrado y descifrado de mensajes MAP entre el cuarto y el primer dominio PLMN-C y PLMN-A se describirán mediante el ejemplo de las peticiones de protocolo MAP en el primer y el quinto nodo de red NEA1 y NEC2. Un mensaje MAP desde la petición de protocolo MAP en el quinto nodo de red NEC1 destinado a la petición de protocolo MAP en el primer nodo de red NEA1 se reenvía en el quinto nodo de red NEC1 a la unidad de conversión en el quinto nodo de red NEC1 y se descifra obteniendo un mensaje MAP asegurado. El mensaje MAP asegurado obtenido se envía a través del segundo canal de transmisión asegurado SC_AC1 al primer nodo pasarela MSEGA. Los mensajes MAP cifrados se descifran en el primer nodo pasarela MSEGA obteniendo un mensaje MAP que comprende el contenido del mensaje MAP original enviado por la petición de protocolo MAP en el quinto nodo de red NEC1. El mensaje MAP obtenido se encamina en el primer dominio hacia la petición de protocolo MAP en el primer nodo de red NEA1 terminando el mensaje MAP.

Por consiguiente un mensaje MAP desde la petición de protocolo MAP en el primer nodo de red NEA1 destinado para la petición de protocolo MAP en el quinto nodo de red NEC1 se encamina en el primer dominio PLMN-A hacia el primer nodo pasarela MSEGA y se cifra obteniendo un mensaje MAP asegurado. El mensaje MAP asegurado obtenido se transmite a través del segundo canal de transmisión asegurado SC_AC1 a la unidad de conversión en el quinto nodo de red NEC1. La unidad de conversión en el quinto nodo de red NEC1 descifra el mensaje MAP asegurado recibido obteniendo un mensaje MAP que comprende el contenido del mensaje MAP original enviado en el primer dominio PLMN-A. El mensaje MAP obtenido se traspasa por la unidad de conversión en el quinto nodo de red NEC1 a la petición de protocolo MAP en el quinto nodo de red NEC1.

El quinto dominio PLMN-D de la red de telecomunicación comprende un séptimo y un octavo nodo de red NED1 y NED2, en cada uno de los cuales se instala una petición de protocolo MAP. El séptimo y el octavo nodo de red NED1 y NED2 están conectados con el primer nodo pasarela MSEGA en el primer dominio PLMN-A a través de un primer y un segundo canal de comunicación no asegurado USC_AD1 y USC_AD2. Para proporcionar un nivel básico de seguridad, el primer nodo pasarela MSEGA realiza un descarte selectivo de mensajes MAP recibidos desde el primer dominio PLMN-A y destinados al quinto dominio PLMN-D y un descarte selectivo de mensajes de la parte de aplicación móvil recibidos desde el quinto dominio PLMN-D y destinados al primer dominio PLMN-A. En una realización ventajosa el descarte selectivo se basa en una dirección en un mensaje MAP o un tipo de un mensaje MAP. El descarte selectivo se puede implementar porque el primer nodo pasarela MSEGA funciona como un cortafuegos hacia el quinto dominio PLMN-D.

El tercer dominio PLMN-E de la red de telecomunicación comprende un noveno nodo de red NEE1 en el cual se instalan una petición de protocolo MAP y una unidad de conversión para el cifrado y descifrado del mensaje MAP y un décimo nodo de red NEE2, en el cual se instala una petición de protocolo MAP. El noveno nodo de red NEE1 está conectado con el primer nodo pasarela MSEGA a través del cuarto canal de comunicación seguro SC_AE, para el cual se proporciona información de seguridad mediante una tercera base de datos de seguridad KACE y se intercambia entre la tercera base de datos de seguridad KACE y la base de datos de seguridad en el primer nodo pasarela MSEGA a través de una tercera conexión de intercambio de información de seguridad IKEC_AE. El décimo nodo de red NEE2 se conecta con el primer nodo pasarela MSEGA en el primer dominio PLMN-A a través del tercer canal de comunicación no asegurado USC_AE. Para proporcionar un nivel básico de seguridad para los mensajes MAP no cifrados intercambiados entre el primer nodo pasarela MSEGA y los nodos de red en el tercer dominio PLMN-E el primer nodo pasarela MSEGA realiza un descarte selectivo de mensajes MAP hacia el tercer dominio PLMN-E. Como se describió para los mensajes MAP hacia el quinto dominio PLMN-D, el descarte selectivo se puede basar en una dirección o un tipo de un mensaje MAP y el descarte selectivo se puede implementar porque el primer nodo pasarela MSEGA funciona como un cortafuegos hacia el tercer dominio PLMN-E.

La Figura 2 representa una arquitectura de un nodo pasarela para convertir un mensaje MAP recibido obteniendo un mensaje MAP asegurado, y para extraer un mensaje MAP no cifrado a partir de un mensaje MAP asegurado. El nodo pasarela comprende una petición de protocolo MAP SMAPPI, la cual está adaptada para procesar mensajes MAP asegurados y no asegurados. La petición de protocolo MAP SMAPPI comprende una máquina de protocolo para generar y responder a los mensajes MAP asegurados y no asegurados. La petición de protocolo MAP SMAPPI comunica con una petición de protocolo TCAP (parte de aplicación de capacidades de transacción) TCAPPI y con una petición de protocolo de usuario MAP MAPUPI intercambiando unidades de datos de servicio adecuadas. La petición de protocolo de usuario MAP MAPUP está conectada con una unidad de operación y mantenimiento OMU que proporciona operación y mantenimiento para el nodo pasarela. La petición de protocolo TCAP TCAPPI se conecta además con una petición de protocolo SCCP (Parte de Control de Conexión de Señalización) SCCPPI. La petición de protocolo SCCP SCCPPI se conecta a otros nodos de red en los cuales se implementan las peticiones de protocolo MAP para comunicar usando mensajes MAP no seguros a través de la interfaz Zf ZFI. Adicionalmente la petición de protocolo SCCP SCCPPI se conecta con otros nodos de red en los cuales se implementan las peticiones del protocolo MAP para comunicar usando mensajes MAP no asegurados a través de una interfaz de red NI.

La petición de protocolo MAP SMAPPI se conecta con una unidad de criptografía CU, que está adaptada para cifrar un mensaje MAP obteniendo un mensaje MAP asegurado. Adicionalmente la unidad de criptografía CU está adaptada para descifrar un mensaje MAP asegurado para obtener el contenido de un mensaje MAP no cifrado respectivo. La unidad de criptografía CU está conectada a una unidad de intercambio de claves KEU para ser dotada con claves para cifrado y claves para descifrado. La unidad de intercambio de claves KEU está conectada con otros nodos de red que realizan una administración de claves de cifrado y descifrado a través de una interfaz Zd ZDI. La unidad de intercambio de claves KEU está conectada con una unidad de gestión de políticas PMU, que coordina la negociación de perfiles de protección y asociaciones de seguridad para canales de comunicación seguros.

La unidad de gestión de políticas PMU está conectada a una base de datos de políticas de seguridad SPD y una base de datos de asociaciones SAD para obtener información necesaria para la negociación de los perfiles de protección. En la base de datos de políticas de seguridad SPD está almacenadas las políticas de seguridad a ser aplicadas para un canal de comunicación seguro. La información en un nivel de seguridad indicado para un dominio particular se puede almacenar en una unidad de información de dominio de seguridad SDIU y proporcionar a la unidad de gestión de políticas PMU en una negociación de una política de seguridad. En una realización preferente

una política de seguridad a ser aplicada hacia un dominio particular de la red de comunicación se puede configurar independientemente de una configuración de una política de seguridad hacia otro dominio. Una política de seguridad puede comprender una indicación de si la seguridad de la capa de aplicaciones MAP va a ser aplicada hacia un dominio, una indicación de si se permite la transmisión no asegurada de los mensajes MAP o una indicación de que no se permite comunicación usando mensajes MAP hacia un dominio particular. Una política de seguridad también puede comprender los mecanismos de seguridad, tales como cifrado o protección de integridad a ser aplicada hacia un dominio particular.

Las políticas potenciales a ser aplicadas hacia un dominio se pueden preconfigurar y almacenar como perfiles de protección potenciales en la base de datos de políticas de seguridad SPD. En la negociación de un perfil de protección a ser aplicado hacia un dominio la unidad de gestión de políticas PMU puede acceder a la base de datos de seguridad SPD para requerir un perfil de protección preconfigurado. Cuando un perfil de protección ha sido negociado por la unidad de gestión de políticas PMU, la información de seguridad a ser usada en una comunicación segura hacia un dominio se intercambia entre la unidad de gestión de políticas PMU y una base de datos de seguridad en ese dominio. La información de seguridad puede comprender una clave cifrada o una descifrada y una indicación para que un algoritmo sea usado en un cifrado o un descifrado. La información de seguridad se agrupa en asociaciones de seguridad y se almacena en la base de datos de asociaciones de seguridad SAD.

Una unidad de administración de base de datos DAU está conectada con la base de datos de políticas de seguridad SPD y la base de datos de asociaciones de seguridad SAD de manera que la base de datos de políticas de seguridad SPD y la base de datos de asociaciones de seguridad SAD se pueden administrar por la unidad de administración de base de datos DAU.

La unidad de administración de base de datos DAU y la unidad de información de dominio de seguridad IKEA se pueden controlar y configurar usando una unidad de interfaz de usuario UI que comprende ventajosamente una interfaz de usuario gráfica o un dispositivo para interpretación de líneas de comando.

La petición de protocolo MAP SMAPPI está conectada con un almacén de repliegue FBS que almacena para un dominio particular una indicación de que es admisible un repliegue a un nivel más bajo de seguridad que el nivel configurado de seguridad para el dominio particular. En una realización preferente de la invención la admisión del repliegue al nivel más bajo de seguridad es configurable para un dominio independientemente de una admisión de un repliegue respectivo a un nivel más bajo de seguridad para otro dominio.

Si un mensaje MAP no cifrado o un mensaje MAP asegurado compatible con un nivel más bajo de seguridad que el nivel preconfigurado de seguridad para el dominio a partir de que el mensaje MAP asegurado fue enviado se recibe en la petición de protocolo MAP SMAPPI, la petición de protocolo MAP SMAPPI puede comprobar el almacén de repliegue FBS si un repliegue a un nivel más bajo de seguridad se permite hacia ese dominio. Si un repliegue a un nivel más bajo de seguridad se permite hacia el dominio, el mensaje MAP se puede procesar de acuerdo con un nivel de seguridad para el cual se permite un repliegue.

La Figura 3 represente una secuencia de pasos de decisión y pasos de procesamiento a ser realizados por un nodo pasarela cuando una petición para un canal de comunicación no asegurado que usa el protocolo MAP se recibe en el nodo pasarela. Los pasos de decisión descritos preferentemente comprenden una consulta a una base de datos de seguridad comprendida en o conectada con el nodo pasarela. Cuando la petición para el inicio del diálogo para el canal de comunicación no asegurado se recibe en el nodo pasarela en un paso de procesamiento de inicio PS0, el nodo pasarela realiza en un primer paso de decisión DS 1 una comprobación, de si se permite una comunicación hacia el dominio desde el cual fue emitida la petición. Si no se permite una comunicación, la petición se descarta y registra por el nodo pasarela en un primer paso de procesamiento PS1.

Si se permite una comunicación hacia el dominio desde el cual fue recibida la petición, el nodo pasarela realiza en un segundo paso de decisión DS2 una comprobación, de si una aplicación de seguridad de la capa de aplicaciones MAP es obligatoria de acuerdo con un nivel preconfigurado de seguridad para una comunicación hacia el dominio que expidió la petición para el inicio de diálogo. Si una aplicación de la seguridad de la capa de aplicaciones MAP no es obligatoria, el inicio del diálogo es aceptado en un segundo paso de procesamiento PS2.

Si una aplicación de la seguridad de la capa de aplicaciones MAP es obligatoria de acuerdo con un nivel preconfigurado de seguridad, el nodo pasarela realiza en un tercer paso de decisión DS3 una comprobación, de si se permite un repliegue a un nivel más bajo de seguridad que el nivel preconfigurado hacia el dominio desde el cual fue recibida la petición. Si se permite un repliegue a un nivel más bajo de seguridad hacia el dominio, el inicio del diálogo es aceptado en un tercer paso de procesamiento PS3.

Si no se permite un repliegue a un nivel más bajo de seguridad, el nodo pasarela realiza en un cuarto paso de decisión DS4 una comprobación, de si un canal de transmisión asegurado es obligatorio para el tipo de mensaje al cual se refiere el inicio del diálogo. Si un canal de transmisión asegurado no es obligatorio para el tipo de mensaje, el inicio de diálogo es aceptado en un cuarto paso de procesamiento PS4.

Si un canal de transmisión asegurado es obligatorio para el tipo de mensaje al cual se refiere el inicio de diálogo, el diálogo se aborta en un quinto paso de procesamiento PS5. La interrupción del diálogo comprende ventajosamente

una salida de la razón para la interrupción del diálogo. La razón para la interrupción ventajosamente especifica que una protección de transporte no es adecuada para el tipo de mensaje.

REIVINDICACIONES

1. La red de telecomunicación con un primer dominio (PLMN-A) que comprende al menos una petición de protocolo de Parte de Aplicación Móvil, MAP, conectada con un modo pasarela (MSEGA) que se adapta para enviar y recibir mensajes MAP y que es conectable a un segundo dominio (PLMN-B, PLMN-C),

caracterizada porque el nodo pasarela (MSEGA) está adaptado para recibir un mensaje MAP desde el primer dominio (PLMN-A), para convertir el mensaje MAP recibido obteniendo un mensaje MAP asegurado, y enviar el mensaje obtenido hacia el segundo dominio (PLMN-B, PLMN-C), el nodo pasarela (MSEGA) que además se adapta para recibir un mensaje MAP asegurado desde el segundo dominio (PLMN-B, PLMN-C), para extraer un mensaje MAP no asegurado a partir del mensaje MAP asegurado recibido y para enviar el mensaje extraído hacia el primer dominio (PLMN-A).

2. La red de telecomunicación de acuerdo con cualquiera de las reivindicaciones precedentes, en la que el nodo pasarela (MSEGA) es conectable con un tercer dominio (PLMN-E) y en el que el nodo pasarela (MSEGA) realiza un descarte selectivo de los mensajes MAP recibidos desde el primer dominio (PLMN-A) y destinados al tercer dominio (PLMN-E) y un descarte selectivo de mensajes MAP recibidos desde el tercer dominio (PLMN-E) y destinados al primer dominio (PLMN-A)

3. La red de telecomunicación de acuerdo con la reivindicación 2, en el que el nodo pasarela (MSEGA) funciona como un cortafuegos hacia el tercer dominio (PLMN-E).

4. La red de telecomunicación de acuerdo con cualquiera de las reivindicaciones precedentes en la que el nodo pasarela (MSEGA) es conectable a diferentes dominios, y los niveles de seguridad son configurables para los diferentes dominios.

5. La red de telecomunicación de acuerdo con la reivindicación 4 en el que para un dominio particular es admisible un repliegue a un nivel más bajo de seguridad que el nivel configurado de seguridad para el dominio particular y en el que la admisión del repliegue al nivel más bajo de seguridad es configurable para un dominio independientemente de una configuración de una admisión de un repliegue respectivo a un nivel más bajo del nivel de seguridad para otro dominio.

6. El nodo pasarela (MSEGA) que comprende una interfaz (NI) con un primer dominio (PLMN-A) de una red de telecomunicación para enviar y recibir mensajes de la Parte de Aplicación Móvil, MAP,

caracterizado porque el nodo pasarela (MSEGA) comprende una interfaz (ZFI) con un segundo dominio (PLMN-B, PLMN-C) de la red de telecomunicación para enviar y recibir mensajes MAP asegurados y porque el nodo pasarela (MSEGA) comprende una unidad de conversión (CU) que se adapta para recibir un mensaje MAP a través del interfaz (NI) con el primer dominio (PLMN-A), para convertir el mensaje MAP recibido obteniendo un mensaje MAP asegurado, y enviar el mensaje obtenido a través de la interfaz hacia el segundo dominio, la unidad de conversión que además está adaptada para recibir un mensaje MAP asegurado a través de la interfaz (ZFI) con el segundo dominio (PLMN-B, PLMN-C), para extraer un mensaje MAP asegurado a partir del mensaje MAP asegurado recibido y para enviar el mensaje extraído a través de la interfaz (NI) hacia el primer dominio (PLMN-A).

7. El nodo pasarela (MSEGA) de acuerdo con la reivindicación 6, que comprende una interfaz con un tercer dominio (PLMN-E) para enviar y recibir mensajes MAP y una unidad de filtrado adaptada para realizar un descarte selectivo de mensajes MAP.

8. El nodo pasarela (MSEGA) de acuerdo con la reivindicación 7, en el que el nodo pasarela (MSEGA) funciona como un cortafuegos hacia el tercer dominio (PLMN-E).

9. El nodo pasarela (MSEGA) de acuerdo con cualquiera de las reivindicaciones 7 a 8, en el que el nodo pasarela (MSEGA) es conectable a diferentes dominios, y el nodo pasarela (MSEGA) comprende una base de datos de seguridad (SDP) para almacenar indicaciones de los niveles de seguridad para los diferentes dominios.

10. El nodo pasarela (MSEGA) de acuerdo con la reivindicación 9, que comprende un almacén de repliegue (FBS) para almacenar para un dominio particular una indicación de que un repliegue a un nivel más bajo de seguridad que el nivel configurado de seguridad para el dominio particular es admisible y en el que la admisión del repliegue al nivel más bajo de seguridad es configurable para un dominio independientemente de una admisión de un repliegue respectivo a un nivel más bajo de seguridad para otro dominio.

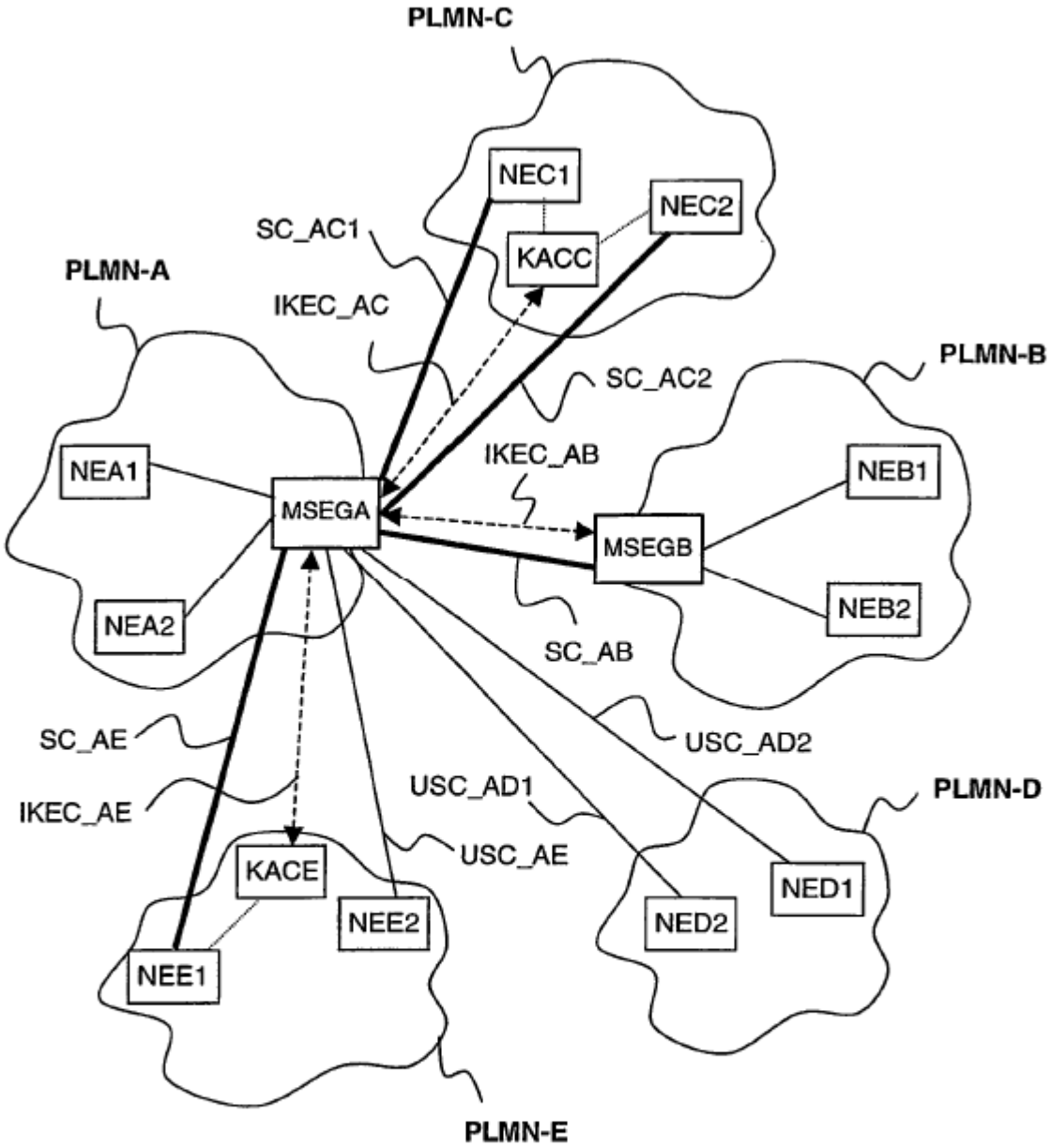
PLMN-C
NEC1
NEC2
KACC
SC_AC1
PLMN-A
IKEC_AC
PLMN-B
SC_AC2
IKEC_AB
NEA1
MSEGA
MSEGB
NEB1
NEB2
NEA2
SC_AB
USC_AD2
SC_AE
IKEC_AE
USC_AD1
PLMN-D
USC_AE
KACE
NEE2
NED1
NED2
NEE1
PLMN-E

Figura 1

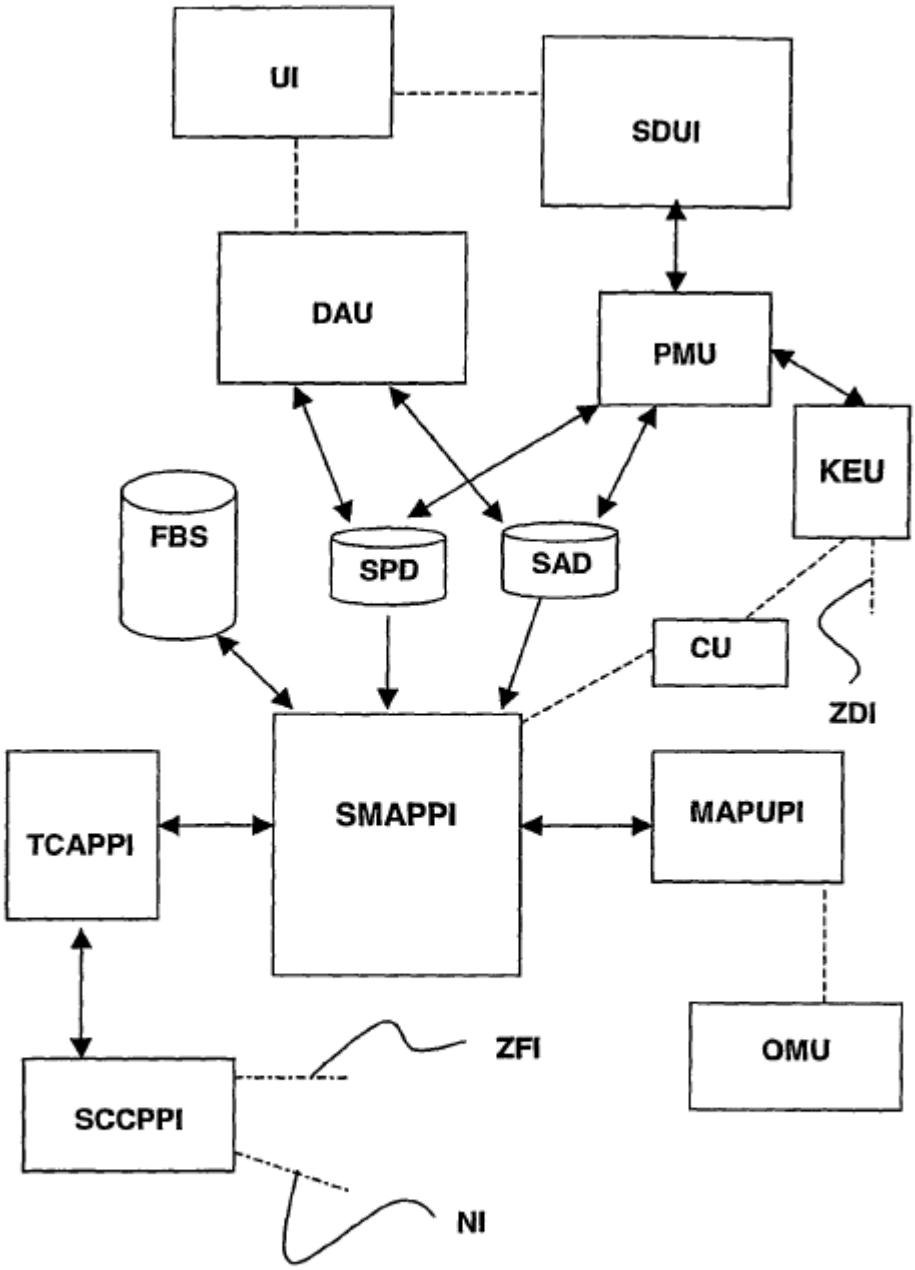
UI
SDUI
DAU
PMU
KEU
FBS
SPD
SAD
CU
ZDI
SMAPPI
TCAPPI
MAPUPI
OMU
ZFI
SCCPPI
NI

Figura 2

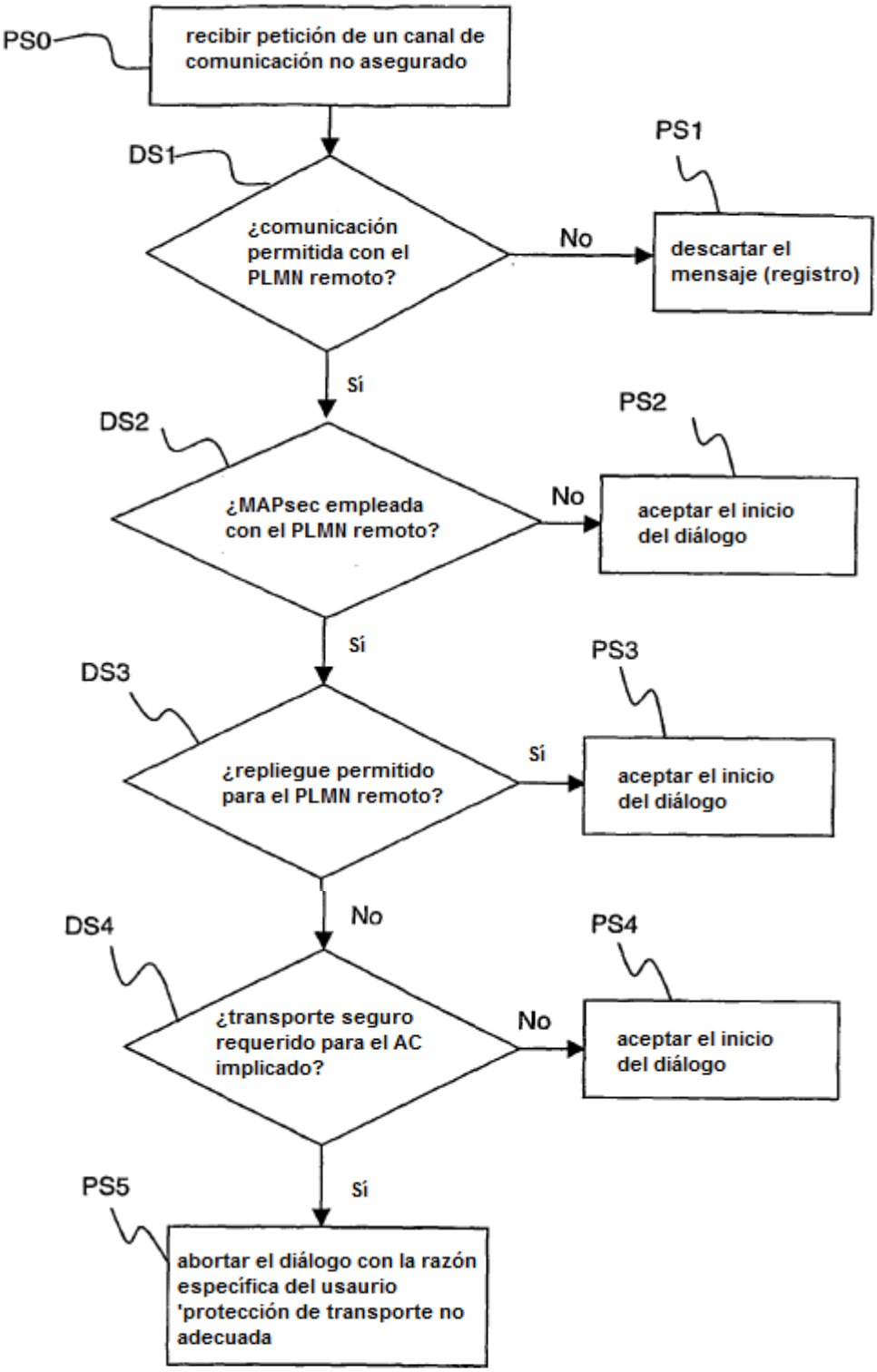
PS0
recibir petición de un canal de comunicación no asegurado
DS1
¿comunicación permitida con el PLMN remoto?
No
PS1
descartar el mensaje (registro)
Sí
DS2
¿MAPsec empleada con el PLMN remoto?
No
PS2
aceptar el inicio del diálogo
Sí
DS3
¿repliegue permitido para el PLMN remoto?
Sí
PS3
aceptar el inicio del diálogo
No
DS4
¿transporte seguro requerido para el AC implicado?
No
PS4
aceptar el inicio del diálogo
Sí
PS5
abortar el diálogo con la razón específica del usaurio 'protección de transporte no adecuada

Figura 3