(19) OFICINA ESPAÑOLA DE PATENTES Y MARCAS

ESPAÑA

(11) Número de publicación: **2 307 108**

(51) Int. Cl.:
H04L 12/28 (2006.01)
H04Q 7/38 (2006.01)

(12) TRADUCCIÓN DE PATENTE EUROPEA T3

(86) Número de solicitud europea: **05101535 .2**
(86) Fecha de presentación : **01.03.2005**
(87) Número de publicación de la solicitud: **1580936**
(87) Fecha de publicación de la solicitud: **28.09.2005**

(54) Título: **Autentificación de abonado.**

(30) Prioridad: **23.03.2004 FI 20045094**

(45) Fecha de publicación de la mención BOPI:
16.11.2008

(45) Fecha de la publicación del folleto de la patente:
16.11.2008

(73) Titular/es: **TeliaSonera Finland Oyj**
Teollisuuskatu 15
00510 Helsinki, FI

(72) Inventor/es: **Vitikka, Ilpo y**
Keisala, Ilkka

(74) Agente: **Carpintero López, Mario**

DESCRIPCIÓN

Autentificación de abonado.

Antecedentes de la invención

1. **Campo de la invención**

La presente invención se refiere a la autentificación de abonados. La invención puede ser ventajosamente utilizada para autentificar a un abonado en un sistema WLAN (Red de área local inalámbrica). No obstante, es importante observar que la presente invención puede ser usada también en otros tipos de sistemas.

2. **Descripción de la técnica anterior**

Se conocen soluciones anteriores en las cuales un abonado es respectivamente autentificado o reautentificado mediante un servidor de autentificación provisto de la información de autentificación necesaria para autentificar a un abonado. Así pues, el servidor de autentificación, utilizando la información de autentificación y un mensaje de autentificación procedente del abonado, puede comprobar si el mensaje de autentificación ha sido transmitido por un autentico abonado. Si es así, la autentificación se ha efectuado correctamente, en caso contrario, la autentificación ha fallado. Si la autentificación se ha efectuado correctamente, se permite que el abonado tenga acceso a los servicios ofrecidos por el sistema de comunicaciones.

Un problema de los procedimientos de autentificación de la técnica anterior, del tipo descrito más arriba, es que los procedimientos de autentificación de la técnica anterior, en ciertas circunstancias, pueden permitir a un abonado el acceso al sistema de comunicaciones, aunque en ese momento el operador considere que ese abonado es un usuario no autorizado del sistema de comunicaciones. Una situación de este tipo puede producirse, por ejemplo, cuando el operador haya cancelado recientemente la cuenta de un abonado, y el abonado esté itinerando (roaming) en otra red. En tal caso la reautentificación del abonado puede efectuarse correctamente y se permite al abonado acceder a la red visitada. También puede darse una situación de este tipo cuando la autentificación se basa en una identidad y contraseña de usuario introducidas por el usuario a través de una interfaz de usuario de una estación de abonado. En este caso puede producirse una situación en la que se utilizan dos diferentes estaciones de abonado para acceder simultáneamente al sistema de comunicaciones usando la misma identidad y contraseña de usuario.

Se conoce anteriormente por el documento WO 2004/002073 A2 una Función de Interfuncionamiento (IWF) para un sistema de comunicaciones. En esta solución una IWF autentifica a un abonado de una WLAN en base a la información de un Vector de Autentificación (AV). Si la IWF tiene el AV cuando el abonado de la WLAN está intentando acceder a la WLAN, la IWF efectúa independientemente la autentificación. En tal situación, la autentificación podría ser correcta y el abonado también podría obtener acceso a la WLAN a través del operador que hubiera cancelado recientemente la cuenta de un abonado. Solo en el caso de que la IWF no tenga el AV cuando el abonado de la WLAN intenta acceder a la WLAN, la IWF solicita el AV a un Centro de Autentificación, en cuyo caso podría detectarse que la cuenta del abonado ha sido cancelada. Esta solución, sin embargo, no basta para impedir que accedan al sistema de comunicaciones abonados que, en opinión del operador, sean usuarios no autorizados del sistema.

Resumen de la invención

Es un objetivo de la presente invención resolver el inconveniente mencionado más arriba y proporcionar una solución que impida acceder a un sistema de comunicaciones a los abonados que, en opinión del operador, sean usuarios no autorizados del sistema. Estos y otros objetivos de la invención se alcanzan mediante el procedimiento de la reivindicación independiente 1, el sistema de comunicaciones de la reivindicación independiente 5, y el servidor de la reivindicación independiente 9.

La presente invención perfecciona las soluciones de autentificación de la técnica anterior mediante la introducción de una comprobación adicional en la autentificación del abonado. Esta comprobación adicional se efectúa recuperando en una base de datos de abonados la información del estado del abonado con respecto a la autentificación. De este modo, ya no basta que el abonado pueda proporcionar al sistema un mensaje correcto de autentificación para obtener acceso al sistema. Además, se efectúa una comprobación de estado para el abonado en cuestión. Esta comprobación de estado proporcionará una información adicional sobre el abonado con la que puede evitarse una situación en la que se proporcione acceso a un abonado, aunque el operador considere en ese momento que ese abonado es un usuario no autorizado.

La ventaja mas significativa alcanzada por la invención es que mejora la capacidad de los operadores para restringir el acceso a la red de abonados no autorizados, ya que el operador puede cambiar la información de estado de estos abonados en la base de datos de abonados para que el acceso sea denegado en función de la autentificación. Otra ventaja significativa de la presente invención es que pueden evitarse las situaciones en las que dos estaciones de abonado estén accediendo simultáneamente al sistema usando en la autentificación la misma identidad y contraseña de usuario.

En las reivindicaciones dependientes 2 a 4, 6 a 8 y 10 se describen las realizaciones preferidas del procedimiento, sistema de comunicaciones y servidor de la invención.

Breve descripción de los dibujos

A continuación se describirá la invención con mayor detalle y a titulo de ejemplo con referencia a los dibujos adjuntos, en los cuales:

La Figura 1 es un diagrama de bloques ilustrando una primera realización preferida de la presente invención.

La Figura 2 es un diagrama de bloques ilustrando una segunda realización preferida de la presente invención.

Descripción de las realizaciones preferidas

La Figura 1 es un diagrama de bloques ilustrando una primera realización preferida de la presente invención. En la Figura 1 se supone, a titulo de ejemplo, que un abonado 1 es un abonado de una WLAN que accede al sistema de comunicaciones por un radioenlace proporcionado por un punto de acceso 2 (una estación base en este ejemplo) y un servidor de acceso 3.

El terminal utilizado por el abonado 1 es supuestamente un cliente EAP SIM (Protocolo Extensible de Autentificación IEEE 802.1x, Módulo de Identidad de Abonado). El terminal incluye pues un SIM que permite al usuario utilizar los servicios de una WLAN y que el coste de los servicios utilizados sean cargados en la factura del teléfono móvil del abonado.

El sistema de la Figura 1 incluye también un servidor 4 que supuestamente es un servidor RADIUS (Servicio de usuario con marcación de autentificación remota). Los servidores RADIUS se utilizan para interconectar entre si las redes WLAN de diferentes operadores. Esta interconexión permite, por ejemplo, ofrecer a los abonados servicios de roaming. El sistema de la Figura 1 incluye adicionalmente un medio de autentificación 5 dispuesto en un servidor de autentificación. Este servidor funciona como un servidor EAP SIM que permite autentificar abonados con clientes EAP SIM. Para efectuar esta autentificación, el medio de autentificación se comunica con un sistema de comunicación móvil, tal como un registro de posición base (HLR) 6 del sistema GSM (Sistema Global de comunicaciones Móviles).

Una base de datos de abonados 7 incluye información sobre los abonados de la WLAN. En el ejemplo de la Figura 1, la base de datos de abonados 7 está conectada al sistema 8 de facturación y atención a los abonados de un operador, el cual es utilizado por el operador para actualizar la información sobre abonados en la base de datos de abonados 7 y el registro de posición base 6, por ejemplo. Cuando se añade al sistema WLAN un nuevo abonado con un cliente EAP SIM, el operador añade la información de abonado sobre este nuevo abonado a la base de datos de abonados 7 y al registro de posición base 6. Si, por el contrario, la cuenta existente de un abonado de la WLAN es cancelada, entonces el operador utiliza el sistema 8 de facturación y atención a los abonados para introducir esta información en la base de datos de abonados 7.

La autentificación del abonado de un cliente EAP SIM se basa en la información de autentificación obtenida del sistema de comunicación móvil. La autentificación EAP SIM ya es conocida y por lo tanto no será explicada con detalle. Dicho brevemente, cuando el abonado 1 ha sido identificado, el medio de autentificación 5 recibe una información de autentificación desde el sistema de comunicación móvil, que en este caso es el sistema GSM. La autentificación se basa en un mecanismo de desafío-respuesta. El cliente EAP SIM recibe un desafío RAND y usa un predeterminado algoritmo para calcular una respuesta SRES, utilizando una clave secreta que es única para el SIM en cuestión. La información de autentificación que incluye tripletas GSM es recibida por el medio de autentificación 5 desde el sistema de comunicación móvil. Esta información de autentificación incluye parejas de RAND y SRES. El RAND es transmitido al abonado 1 que utiliza la clave secreta del SIM para calcular una respuesta con el algoritmo de autentificación. Esta respuesta es devuelta en un mensaje de autentificación al medio de autentificación, que compara la respuesta con el SRES. Si la respuesta coincide con el SRES, entonces la autentificación es correcta. Sin embargo, en la autentificación EAP SIM, se combinan varias tripletas GSM para efectuar una autentificación. La autentificación EAP SIM también mejora la autentificación GSM básica acompañando los desafíos RAND y otros mensajes con un Código de Autentificación de Mensaje para proporcionar una autentificación mutua.

A continuación se explicará la autentificación según la presente invención. Las figuras no muestran todos los mensajes relacionados con la autentificación, sino sólo aquellos mensajes que sean importantes para comprender la presente invención. Para poder autentificar al abonado 1, el medio de autentificación transmite al registro de posición base 6 del sistema GSM una solicitud A de tripletas de autentificación. El registro de posición base responde a esta solicitud transmitiendo B una información de autentificación al medio de autentificación 5. Esta información de autentificación incluye varias tripletas para el abonado 1, lo cual significa que el medio de autentificación puede autentificar varias veces al abonado 1 antes de que tenga que solicitar más tripletas al registro de posición base.

Cuando el abonado 1 en conexión con la autentificación transmite un mensaje de autentificación C a través del radioenlace, este mensaje es recibido por el punto de acceso 2 y enviado por la red al medio de autentificación 5. El término mensaje de autentificación se refiere aquí a un mensaje que incluye la información necesaria que permita autentificar al abonado. En caso de que el abonado haya sido autentificado previamente y el mensaje de autentificación se refiera a una reautentificación, entonces el medio de autentificación puede tener ya la necesaria información de autentificación para el abonado en cuestión, y no se transmiten los mensajes indicados por A y B antes de la recepción del mensaje de autentificación. Una vez recibido el mensaje de autentificación, el medio de autentificación compara el

contenido del mensaje de autentificación C con la información de autentificación del abonado 1 obtenida previamente. Dependiendo de esta comparación, el medio de autentificación 5 informa D al servidor 4 que la autentificación ha sido correcta o que ha fallado.

Si el servidor 4 recibe información indicando una autentificación correcta, entonces el medio de comprobación 9 del servidor transmite un mensaje E a la base de datos de abonados 7 para obtener la información de estado para el abonado en cuestión. El medio de comprobación puede consistir en un circuito, un programa informático, o una combinación de ambos. La información de estado es recibida por el servidor en el mensaje F. La información de estado recibida es utilizada por el servidor 4 para efectuar una comprobación en la cual se determina si la cuenta del usuario ha sido cancelada.

Si el medio de comprobación 9 detecta que la cuenta del usuario ha sido cancelada, entonces el servidor 4 transmite por la red al punto de acceso 2 un mensaje G indicando que la autentificación ha fallado. En caso contrario este mensaje G indica que la autentificación es correcta. Si el punto de acceso 2 recibe un mensaje G indicando que la autentificación ha fallado, entonces el abonado 1 deja de tener acceso a la red.

La presente invención ha sido explicada más arriba con relación a una "autentificación completa", en otras palabras, cuando la información de autentificación es obtenida del sistema de comunicación móvil. Sin embargo, la presente invención también puede ser utilizada ventajosamente para la reautentificación, en la cual un abonado previamente autentificado es autentificado de nuevo. En este caso el medio de autentificación 5 no solicita ni recibe del sistema de comunicación móvil ninguna información de autentificación "actualizada". En su lugar, se utilizan para la reautentificación las tripletas previamente obtenidas que fueron almacenadas en la memoria del medio de autentificación 5. Por lo demás, la reautentificación se efectúa según se explicó más arriba. En este caso la comprobación suplementaria del estado asegura que la información de autentificación "antigua" puede ser utilizada sin ningún riesgo, ya que si se hubieran producido recientemente cambios sobre el abonado (tales como la cancelación de la cuenta), estos cambios pueden ser detectados en la comprobación del estado, que se basa en la información actual del estado.

La Figura 2 es un diagrama de bloques que ilustra una segunda realización preferida de la presente invención. La realización de la Figura 2 es muy similar a la descrita con relación a la Figura 1. Por ello, se describirá a continuación la realización de la Figura 2 explicando principalmente las diferencias con respecto a la realización de la Figura 1.

En la Figura 2, el abonado 1' no es un abonado con cliente EAP SIM, sino que la autentificación del abonado 1' se efectúa en base a una identidad y una contraseña conocida por el usuario del terminal WLAN. La parte de red del sistema es casi idéntica a la explicada con relación a la Figura 1, ya que los mismos elementos de red pueden manejar tanto a los abonados con clientes EAP SIM como a los abonados autentificados con identidad y contraseña de usuario. Sin embargo, en este caso el medio de autentificación 5' está dispuesto en el servidor 4', que así es capaz de autentificar al abonado 1'. El medio de autentificación 5' puede consistir en un circuito, un programa informático, o una combinación de ambos. El registro de posición base y el servidor de autentificación de la Figura 1 no aparecen en la Figura 2 porque no se necesitan para autentificar a un abonado cuya autentificación esté basada en una identidad y contraseña de usuario. El sistema de la Figura 2, sin embargo, también puede incluir ventajosamente el registro de posición base 6 y el servidor de autentificación 5 de la Figura 1 para poder autentificar tanto a los abonados con clientes EAP SIM como a los abonados cuya autentificación esté basada en la identidad y contraseña de usuario.

En la realización de la Figura 2 no es necesario obtener ninguna información de autentificación desde un sistema de comunicación móvil. En su lugar, la información de autentificación, consistente en la identidad y contraseña de usuario de los abonados, puede ser almacenada previamente en el medio de autentificación 5' cuando se abren las cuentas de los abonados en el sistema.

El mensaje de autentificación C' transmitido por el abonado en la Figura 2 incluye pues una contraseña o una identidad de usuario y una contraseña. El medio de autentificación 5' del servidor 4' recibe este mensaje y comprueba si la contraseña del abonado en cuestión es correcta. Si es así, entonces el medio de autentificación 5' indica que la autentificación se ha efectuado correctamente. El medio de comprobación 9' del servidor 4' está dispuesto para solicitar E a la base de datos de abonados 7 la información de estado del abonado en cuestión. La información de estado recibida F es utilizada para comprobar si el abonado autentificado tiene o no acceso al sistema a través de otro mecanismo de autentificación. En caso afirmativo, se dará entonces una situación en la que el mismo abonado que está siendo autentificado tiene ya acceso al sistema con otro terminal. Si se detecta tal situación, entonces se transmite al punto de acceso un mensaje G para indicar que la autentificación ha fallado. En caso contrario este mensaje G es utilizado para indicar al punto de acceso que la autentificación se ha efectuado correctamente. Si la autentificación se ha efectuado correctamente, entonces el servidor 4' transmite un mensaje H a la base de datos de abonados 7 para almacenar en la base de datos de abonados una información indicando que el usuario ha sido autentificado correctamente y dispone de acceso al sistema. Esta información almacenada se recupera en una posible comprobación posterior para indicar que el abonado tiene acceso al sistema a través de otro mecanismo de autentificación. Así puede evitarse que el mismo abonado pueda acceder al sistema con otro terminal.

Cuando el abonado autentificado interrumpe la conexión por alguna razón para dejar de usar los servicios disponibles en la red, entonces el punto de acceso 2 y/o el servidor de acceso 3 lo detectan y transmiten al servidor 4' un mensaje de "cuenta interrumpida", por ejemplo, para indicar que el abonado deja de tener acceso a la red. El servidor 4' envía esta información para interrumpir la cuenta, y además transmite un mensaje a la base de datos de abonados

7 para indicar que el abonado ya no tiene acceso al sistema. Esta información es almacenada en la base de datos de abonados para que sea recuperada como indicación de que el abonado no tiene acceso al sistema a través de otro mecanismo de autentificación la próxima vez que el abonado sea autentificado.

Se ha explicado en la anterior descripción de las realizaciones que en la realización de la Figura 1 la comprobación de estado es utilizada para asegurar que la cuenta del abonado no ha sido cancelada, y en la realización de la Figura 2 para comprobar que el abonado no tiene acceso al sistema con otro mecanismo de autentificación. No obstante, es ventajoso proporcionar el mismo procedimiento de autentificación con ambas comprobaciones. Así pues, se efectúa una comprobación de estado para asegurar que la cuenta del abonado no haya sido cancelada y que el abonado no tenga acceso al sistema a través de otro mecanismo de autentificación. En este caso se transmite un mensaje, indicando que la autentificación ha fallado, si cualquiera o ambas comprobaciones tiene un resultado positivo, o dicho de otro modo, que la cuenta ha sido cancelada o que el abonado tiene acceso a través de otro mecanismo de autentificación.

Debe entenderse que la anterior descripción y las Figuras que la acompañan sólo pretenden ilustrar la presente invención.

REIVINDICACIONES

1. Un procedimiento para autentificar a un abonado de un sistema de comunicación, comprendiendo dicho procedimiento:

recibir (C, C') de un abonado un mensaje de autentificación, y

comprobar la autenticidad del abonado utilizando contenidos de dicho mensaje de autentificación, **caracterizado** por

recuperar (E, F) de una base de datos de abonados la información de estado para dicho abonado, cuando dicha comprobación indique que el abonado ha sido correctamente autentificado,

transmitir (G) un mensaje indicando que la autentificación de dicho abonado ha fallado, si se dan una o más de las siguientes condiciones:

- la autentificación de dicho abonado en base al contenido de dicho mensaje de autentificación ha fallado,
- la información de estado indica que el abonado tiene acceso al sistema a través de otro mecanismo de autentificación, o
- la información de estado indica que la cuenta del abonado ha sido cancelada.

2. El procedimiento de la reivindicación 1, **caracterizado** porque dicho mensaje de autentificación es un mensaje de reautentificación.

3. El procedimiento de la reivindicación 1, **caracterizado** porque dicho sistema de comunicación es un sistema WLAN y dicho procedimiento comprende adicionalmente:

transmitir (A) desde dicho sistema WLAN una solicitud de información de autentificación a un sistema de comunicación móvil,

recibir (B) información de autentificación desde el sistema de comunicación móvil, y

comprobar la autenticidad del abonado utilizando el contenido de dicho mensaje de autentificación y la información de autentificación recibida desde el sistema de comunicación móvil.

4. El procedimiento de una cualquiera de las reivindicaciones 1 a 3, **caracterizado** porque dicho abonado es un cliente EAP SIM.

5. Un sistema de comunicación que comprende:

un punto de acceso (2) que proporciona acceso al sistema para los abonados autentificados,

una base de datos de abonados (7) conteniendo información sobre los abonados del sistema, y

un medio de autentificación (5, 5') para autentificar a un abonado (1, 1') mediante la utilización del contenido de un mensaje de autentificación recibido de dicho abonado (1, 1'), **caracterizado** porque dicho sistema de comunicación comprende adicionalmente:

un medio de comprobación (9, 9') para recuperar de la base de datos de abonados (7) información de estado para dicho abonado (1, 1') cuando el medio de autentificación indique que dicho abonado (1, 1') ha sido correctamente autentificado, para efectuar una comprobación en base a dicha información de estado recuperada, y para transmitir al punto de acceso (2):

- un mensaje indicando que la autentificación de dicho abonado (1, 1') ha fallado, cuando la comprobación indique que el abonado tiene acceso al sistema a través de otro mecanismo de autentificación, y/o que la cuenta del abonado ha sido cancelada, o
- un mensaje indicando que la autentificación de dicho abonado (1, 1') se ha efectuado correctamente, cuando la comprobación indique que el abonado no tiene acceso al sistema a través de otro mecanismo de autentificación, y que la cuenta del abonado no ha sido cancelada.

6. El sistema de comunicación de la reivindicación 5, **caracterizado** porque

dicho punto de acceso (2) es una estación base que proporciona a los abonados autentificados el acceso al sistema de comunicación sobre una interfaz radio,

dicho medio de autentificación (5) está dispuesto para transmitir una solicitud de información de autentificación a un sistema radio celular, para recibir información de autentificación desde un sistema radio celular, y para autentificar a dicho abonado (1) en base al contenido del mensaje de autentificación y a la información de autentificación.

7. El sistema de comunicación de las reivindicaciones 5 ó 6, **caracterizado** porque dicho mensaje de autentificación es un mensaje de reautentificación.

8. El sistema de comunicación de una cualquiera de las reivindicaciones 5 a 7, **caracterizado** porque dicho sistema de comunicación es un sistema WLAN, dicho abonado es un cliente EAP SIM y dicho medio de comprobación (9, 9') está dispuesto en un servidor Radius (4, 4').

9. Un servidor (4, 4') de un sistema de comunicación, respondiendo dicho servidor a un medio de autentificación del sistema de comunicación, **caracterizado** porque dicho servidor comprende un medio de comprobación (9, 9') que, cuando dicho medio de autentificación (5, 5') indica que la autentificación de un abonado (1, 1') ha sido correcta, está dispuesto para recuperar de una base de datos de abonados (7) la información de estado de dicho abonado, para efectuar una comprobación en base a dicha información de estado, y para transmitir:

- un mensaje indicando que la autentificación de dicho abonado (1, 1') ha fallado, cuando la comprobación indique que el abonado tiene acceso al sistema a través de otro mecanismo de autentificación, y/o que la cuenta del abonado ha sido cancelada, o

- un mensaje indicando que la autentificación de dicho abonado (1, 1') se ha efectuado correctamente, cuando la comprobación indique que el abonado no tiene acceso al sistema a través de otro mecanismo de autentificación, y que la cuenta del abonado no ha sido cancelada.

10. El servidor de la reivindicación 9, **caracterizado** porque dicho servidor (4, 4') es un servidor Radius.

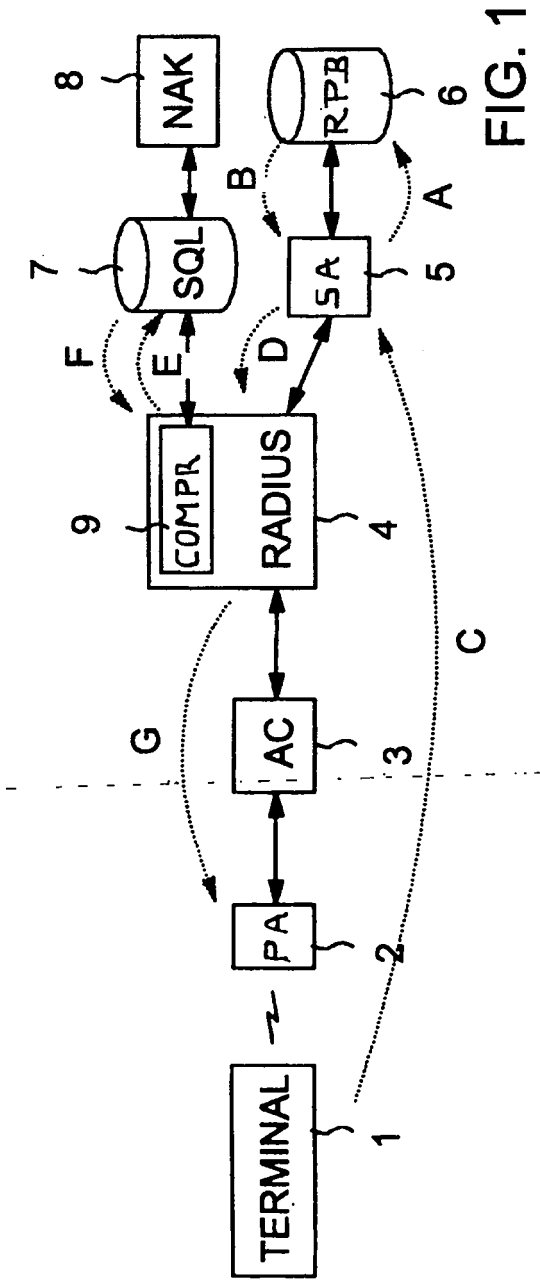
TERMINAL
PA
AC
RADIUS
COMPR
SQL
SA
RPB
NAK
1
2
3
4
5
6
7
8
9
A
B
C
D
E
F
G

FIG. 1

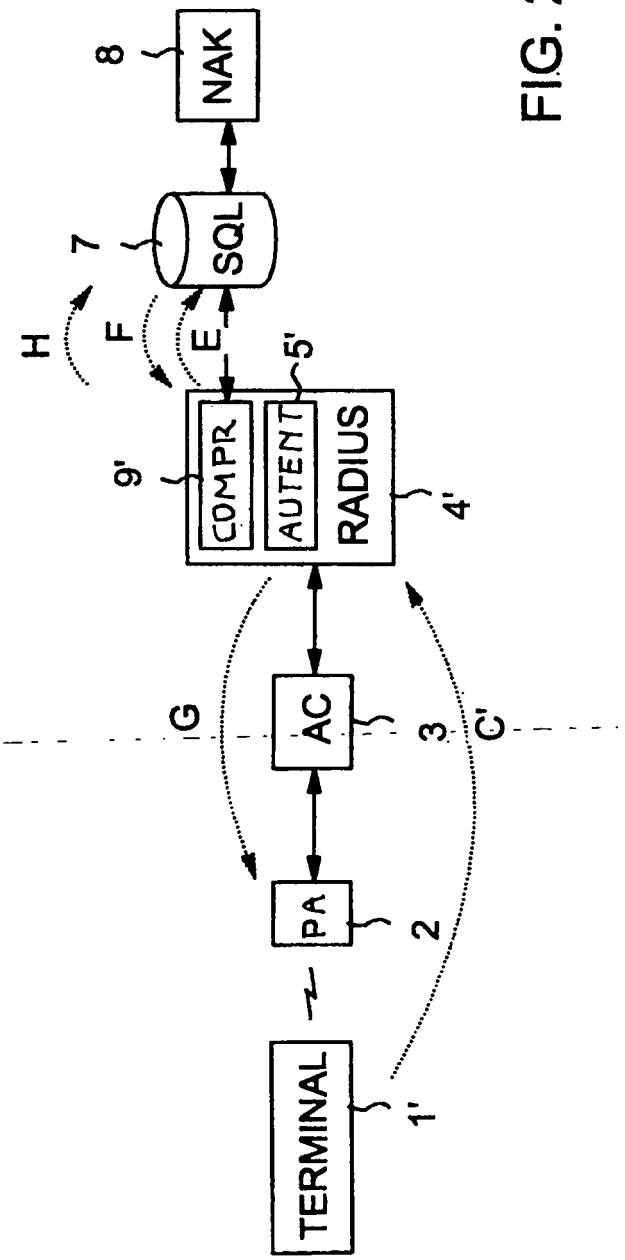
TERMINAL
PA
AC
RADIUS
COMPR
AUTENT
SQL
NAK
1'
2
3
4'
5'
7
8
9'
C'
E
F
G
H

FIG. 2