(19) OFICINA ESPAÑOLA DE PATENTES Y MARCAS

ESPAÑA

(11) Número de publicación: **2 400 527**

(51) Int. CI.:

H04L 29/06 (2006.01)

(12) TRADUCCIÓN DE PATENTE EUROPEA T3

(96) Fecha de presentación y número de la solicitud europea: **30.05.2007 E 07721833 (7)**

(97) Fecha y número de publicación de la concesión europea: **30.01.2013 EP 2044748**

(54) Título: **Procedimiento de autenticación remota de un abonado de red telefónica**

(30) Prioridad:

24.07.2006 CZ 20060478

(45) Fecha de publicación y mención en BOPI de la traducción de la patente:
10.04.2013

(73) Titular/es:

MONET+, A.S. (100.0%)
ZA DVOREM 505
763 14 ZLIN, STIPA, CZ

(72) Inventor/es:

ENDRYS, BRETISLAV

(74) Agente/Representante:

DURÁN MOYA, Carlos

DESCRIPCIÓN

Procedimiento de autenticación remota de un abonado de red telefónica

Sector técnico

La invención se refiere a la autenticación remota de un abonado de red de telefonía móvil que se basa en la utilización de características técnicas de las redes de telefonía móvil y la aplicación de criptografía.

Técnica anterior

La autenticación, es decir, la verificación de la identidad del cliente, se lleva a cabo en las redes telefónicas de diferentes maneras que emplean contraseñas de acceso cifradas u otros medios de identificación. Los procedimientos de verificación de la identidad del abonado disponibles en las redes existentes de operadores móviles se basan en algoritmos criptográficos con resistencia limitada contra el ataque criptográfico de “fuerza bruta”, por tanto son poco fiables. Estos procedimientos se utilizan para la verificación de la identidad de las tarjetas SIM de los teléfonos móviles, por ejemplo. Además, este procedimiento requiere que las claves criptográficas estén en posesión del operador, no pueden ser utilizadas para las necesidades de otras entidades que requieran la verificación de la identidad de la persona que llama.

Otras soluciones disponibles hasta ahora no llevan a cabo la autenticación de la identidad de la persona que llama hasta que se ha establecido la conexión entre la parte que llama y la llamada y utilizan el canal de comunicación establecido para este propósito. Los mismos procedimientos de verificación se basan en el conocimiento de una contraseña secreta, que necesariamente requiere compartir un secreto entre el operador, es decir, la entidad que requiere la autenticación de la identidad, y el abonado. Otro procedimiento de verificación de la identidad del abonado utiliza una contraseña de un solo uso, generada con un método criptográfico que utiliza un equipo técnico adicional en posesión del cliente.

El documento WO 2006/042469, del 27 de abril de 2006 (2006-04-27) describe un procedimiento de autenticación de contraseña dinámica para permitir que un usuario inicie sesión en un sistema de red a través de un ordenador para tener acceso a servicios de aplicaciones. La tecnología propuesta en el documento propone la autenticación de un usuario ya conectado a una red móvil pero que desea tener acceso a servicios de elevada seguridad.

Características de la invención

La solución propuesta permite la autenticación automatizada de la persona que llama, ejecutada transmitiendo los datos específicos de la persona que llama al sistema llamado de información (VIS). Las características claves de la solución incluyen la capacidad de generar datos específicos, tal como un criptograma de autenticación, una contraseña de un solo uso (DTA), etc. en un componente adecuado de un aparato de teléfono, por ejemplo en la tarjeta SIM (Módulo de Identificación del Abonado), y añadir dichos datos a los otros datos que participan en el establecimiento de la conexión requerida. En una ubicación o fase adecuada del proceso de petición de la conexión, es decir, antes del establecimiento de la conexión con el sistema llamado de información (VIS), se lleva a cabo una evaluación automatizada de un criptograma de autenticación que se ha creado como una contraseña de un solo uso (DTA). Esta evaluación se utiliza posteriormente para verificar la identidad de la persona que llama y el resultado es utilizado para el establecimiento lógico de la conexión.

El proceso de autenticación remota de la identidad del abonado de la red de telefonía utiliza el proceso criptográfico. En este procedimiento, tanto el identificador del abonado como un criptograma de identificación, compuestos por los datos especificados generados como una contraseña de un solo uso se transmiten en la red del operador y la clave para generar dichos datos no tiene porque estar en posesión del operador de red. La ventaja del procedimiento descrito es que el aparato de teléfono genera un contraseña de un solo uso que representa un criptograma de identificación, la contraseña de un solo uso se añade a los datos que participan en el establecimiento de la conexión y en una ubicación en la que se procesa la petición de la conexión, la contraseña de un solo uso se evalúa como parte del proceso de la petición de conexión antes del establecimiento de la conexión con el sistema llamado de información, de manera se verifica la identidad del cliente y el resultado de la autenticación se utiliza para decidir si establecer la conexión.

En la solución propuesta, la verificación de la identidad del abonado es forzada por los servicios que se proporcionan a través de los canales de comunicación. Otras ventajas incluyen que la autenticación no tenga que llevarse a cabo a nivel de la aplicación, aumenta el rendimiento de la autenticación, y con los canales de voz, los operadores están exentos de llevar a cabo procedimientos de autenticación verbales.

Modos de realización de la invención

De acuerdo con la invención, la autenticación remota de la identidad del abonado se lleva a cabo utilizando los datos específicos generados como una contraseña de un solo uso (DTA) para las necesidades del sistema llamado de

información (VIS).

El sistema llamado de información (VIS) se puede representar, por ejemplo, mediante un sistema automatizado o mediante un operador que se comunica con el canal de voz que llama.

La identidad del abonado se define en la red del operador mediante el identificador, por ejemplo, mediante el número del abonado móvil (MSISDN), y este valor se transmite normalmente en la red del operador durante el establecimiento de la conexión.

Una contraseña de un solo uso (DTA) se genera criptográficamente desde el identificador (MSISDN) en el módulo SIM (módulo de identificación del abonado). La contraseña de un solo uso (DTA) se transmite durante el establecimiento de la conexión dado que pasa a formar parte del número llamado. Tanto el valor del identificador (MSISDN) y los datos específicos generados como la contraseña de un solo uso (DTA) se transmiten al módulo HSM (Módulo de Seguridad Central) en una ubicación que está equipada con el programa lógico de verificación de la identidad, por ejemplo, una centralita privada del sistema llamado de información (VIS). Este módulo HSM verifica la validez de la contraseña de un solo uso (DTA), que se está transmitiendo, y, de esta manera, la identidad de la persona que llama. Una vez se ha llevado a cabo la verificación de la identidad de la persona que llama (del abonado), se finaliza la conexión con el sistema llamado de información (VIS) conectando el canal de comunicación.

Una vez se ha establecido la conexión, la aplicación llamada, que representa el sistema llamado de información (VIS), no tiene que llevar a cabo ninguna otra autenticación de la persona que llama y puede utilizar el resultado de la autenticación que se llevó a cabo automáticamente durante el establecimiento de la conexión.

La generación de una contraseña de un solo uso (DTA) incluye la imposición de un número de identificación personal (PIN) específico, de manera que se lleva a cabo la autenticación de la tarjeta SIM-abonado.

Es un prerrequisito la utilización de algoritmos criptográficos suficientemente seguros con una longitud de clave correspondiente.

Aplicabilidad industrial

Según la autenticación remota de la identidad de la persona que llama de la invención propuesta, se puede utilizar repetidamente de una manera industrial y se puede utilizar en aplicaciones que requieren autenticación, es decir, la verificación de la identidad del cliente con un mayor grado de seguridad que la seguridad proporcionada por las tecnologías actuales de la red del operador.

REIVINDICACIONES

1. Procedimiento de autenticación remota de la identidad del abonado de la red de telefonía, que utiliza un método criptográfico, durante el que tanto el identificador del abonado como un criptograma de identificación, que comprenden datos específicos generados como una contraseña de un solo uso se transmiten en la red del operador, y la clave para generar dichos datos no tienen que estar en posesión del operador de red, generando una contraseña de un solo uso que representa un criptograma de identificación en el aparato telefónico, caracterizado porque añade esta contraseña de un solo uso al número llamado y, de esta manera, la contraseña de un solo uso pasa a formar parte del número llamado, y en una ubicación en la que se procesa la petición de conexión, se extrae la contraseña de un solo uso a partir del número llamado y se evalúa como una parte del proceso de la petición de conexión previamente al establecimiento de la conexión con el número llamado, de esta manera se verifica la identidad del cliente y el resultado de la autenticación se utiliza para decidir si finalizar el establecimiento de la conexión.