(19) OFICINA ESPAÑOLA DE PATENTES Y MARCAS

ESPAÑA

(11) Número de publicación: **2 403 225**

(51) Int. CI.:

G07C 9/00 (2006.01)
H04L 29/06 (2006.01)
G06F 21/00 (2013.01)

(12) TRADUCCIÓN DE PATENTE EUROPEA T3

(96) Fecha de presentación y número de la solicitud europea: **18.07.2008 E 10187582 (1)**

(97) Fecha y número de publicación de la concesión europea: **16.01.2013 EP 2284802**

(54) Título: **Proceso y esquema para autenticar a un usuario de unas instalaciones, un servicio, una base de datos o una red de datos**

(30) Prioridad:

19.07.2007 DE 102007033812

(45) Fecha de publicación y mención en BOPI de la traducción de la patente:
16.05.2013

(73) Titular/es:

VOICECASH IP GMBH (100.0%)
Claridenstrasse 25
8002 Zürich, CH

(72) Inventor/es:

MUMM, MARC y
KUPPUSWAMY, RAJASEKHARAN

(74) Agente/Representante:

ISERN JARA, Jorge

DESCRIPCIÓN

Proceso y esquema para autenticar a un usuario de unas instalaciones, un servicio, una base de datos o una red de datos

Esta invención se refiere a un proceso y un esquema para autenticar a un usuario de unas instalaciones, un servicio, una base de datos o una red de datos.

En los sistemas convencionales de control de acceso, aplicados a las redes de datos, los medios de identificación o de autenticación, respectivamente, del tipo basado en el conocimiento se están usando para cumplir con los requisitos de seguridad. Particularmente, durante décadas los esquemas de identificación/autenticación basados en contraseña o basados en el PIN se conocen y se usan generalmente. Más específicamente, en aplicaciones sensibles a espías o al fraude, tales como las aplicaciones de banco en casa, las medidas de seguridad adicionales, como la provisión y el uso obligatorio de los códigos de transacción individuales o TAN, respectivamente, se conocen y se usan ampliamente. Incluso tales esquemas complementarios de refuerzo de la seguridad se basan en el conocimiento y presentan, por lo tanto, las desventajas típicas de todos los esquemas basados en el conocimiento, es decir, por un lado los problemas relacionados con la pérdida de la información relevante por parte del usuario autorizado, y por otro lado los riesgos derivados del acceso a dicha información por parte de un usuario no autorizado.

Por lo tanto, en años recientes se han realizado esfuerzos considerables para incluir otros tipos de esquemas de identificación/autenticación en los mecanismos de seguridad de las redes de datos. Particularmente, se han intentado enfoques para adicionar esquemas "basados en la posesión" (tokens) y/o "basados en la persona" (basados en la biometría) a los bien conocidos esquemas basados en el conocimiento, o incluso para sustituir los últimos esquemas con dichos nuevos esquemas. Por ejemplo, en los cajeros automáticos se han propuesto esquemas biométricos de autenticación basados en el reconocimiento de huellas digitales o de retina, respectivamente, para controlar el acceso a las cuentas bancarias. Además, por su parte los bien establecidos medios de control de acceso basados en la huella digital de los ordenadores portátiles y otras computadoras personales se deben mencionar como un tipo de medio para controlar el acceso a las redes de datos.

Más recientemente, las soluciones de autenticación basadas en la voz, como un tipo específico de identificaciones/autenticaciones basadas en la biometría, se han introducido ampliamente por las empresas para complementar sus esquemas internos de control de acceso basados en el conocimiento.

En los servicios y actividades basados en Internet y en los móviles, particularmente en los sitios de mercado de Internet como eBay o los sistemas de transacciones financieras de Internet como PayPal, con la base de usuarios en rápido crecimiento en todo el mundo, el número de ataques fraudulentos aumenta significativamente. La probabilidad de un ataque exitoso en las cuentas de un servicio basado en Internet en todo el mundo con millones de usuarios es mucho mayor que con los ataques de phishing en los bancos locales.

Así, la autenticación basada en la voz también se está discutiendo como un esquema de seguridad para los servicios basados en Internet y en la red de móviles y los sistemas de acceso a datos.

Frente a este tipo de aplicación sofisticada a gran escala, las soluciones biométricas de voz tienen que hacer frente a varios desafíos tecnológicos y tienen que alcanzar un alto nivel de aceptación de los usuarios. Los desafíos específicos están relacionados con el proceso de inscripción, problemas del multi-canal, requisitos de seguridad, demandas de flexibilidad y escalabilidad.

Para el proceso de inscripción, se requiere el ID único de usuario para identificar al usuario. Sin embargo, no existe una forma universal de ID de usuario para identificar a los usuarios de los sistemas biométricos de voz. El formato varía de empresa a empresa. En el mercado de las empresas, el número personal de los empleados se usa frecuentemente para la identificación, mientras que en el mercado de los consumidores el nombre de una persona o cualquier otro sustituto para el nombre (nombre de usuario, dirección de correo electrónico, número del teléfono móvil) se usan o se pueden usar para identificar al usuario, al menos con un cierto grado de fiabilidad.

Actualmente, para esta etapa, se usa el reconocimiento automático del habla (ASR). Sin embargo, básicamente la integración del ASR en una solución de verificación de la voz está limitando su escalabilidad. Las soluciones de ASR no están disponibles en todos los idiomas o presentan varios problemas en una serie de idiomas. Esto significa que: Aunque una solución de verificación de la voz podría, en principio, ofrecerse a los clientes en estos países específicos, la solución como se ofrece actualmente (incluyendo un reconocimiento del habla y una parte de verificación de la voz) no se puede proporcionar a los clientes en estos países debido al componente de ASR faltante o sub-óptimo.

La eliminación del componente de ASR haría al sistema más fácil de usar y más fácil de escalar, pero hasta el

momento no existe ninguna solución para evitar la integración del componente de reconocimiento del habla en un sistema de autenticación basado en un perfil de voz.

Además, la seguridad es un gran problema para los clientes. Hasta el momento, la mayoría de las soluciones de seguridad biométrica de voz dependen exclusivamente de la autenticación de la voz como la única capa de seguridad real además del ID de usuario (comprobados con el reconocimiento de la voz). Sin embargo, esto significa que el umbral de la capa de seguridad de autenticación de la voz tiene que establecerse alto para asegurar un nivel de seguridad resultante alto. Esto puede resultar en limitaciones durante el uso del sistema.

El uso de diferentes tipos de teléfonos (de línea fija (cableado), de línea fija (DECT), teléfono móvil, VoIP) da lugar a problemas en el uso de las soluciones biométricas de voz. Debido a que el ancho de banda de los diferentes canales de telefonía está en el intervalo de 8 kbit/s (VoIP) a 64 kbit/s (RDSI) e incluso mucho más, la calidad de la muestra de voz es diferente. Un usuario inscrito con un teléfono VoIP puede tener problemas para verificar con un teléfono de línea fija cableado, ya que la muestra de voz proporcionada con el teléfono de línea fija se diferencia de la muestra de voz proporcionada durante la inscripción con el teléfono VoIP. Una solución para este problema sería disminuir el umbral que determina la sensibilidad del sistema.

Combinado con los requisitos de seguridad, los problemas del multi-canal pueden dar lugar a un factor de incomodidad en el uso de los productos de autenticación de la voz, relacionado con mayores tasas de falso rechazo (FRR) y problemas durante la inscripción y el uso de la solución.

Como ya se ha mencionado anteriormente, para usar un sistema biométrico de voz cada usuario tiene que registrarse en el sistema, almacenando su impresión de voz en la base de datos. Sólo después de que el usuario se ha inscrito en el sistema él/ella puede usar el sistema. Un problema relacionado con el proceso de inscripción es que la mayoría de los sistemas biométricos de voz tratan de alcanzar un nivel de inscripción de un 100% de los usuarios en el período inicial de la implementación del sistema. Esto resulta en una alta carga en los canales de voz en las primeras semanas/meses después de la instalación. Se necesita un mayor número de canales de voz para manejar el gran número de usuarios a inscribir. Si un sistema sólo se usa con el número de puertos de voz que se necesitan para garantizar un uso diario conveniente después de la fase de inscripción, algunos de los usuarios, que desean inscribirse, pueden no atenderse debido a que los puertos de voz están bloqueados.

La US 2007/061590 A1 describe un proceso para autenticar a un usuario, para controlar su acceso remoto a un servicio, base de datos o red de datos, en donde en una etapa de inscripción se analiza una muestra de voz inicial proporcionada por el usuario para obtener un perfil de voz inicial específico del usuario. En una etapa de verificación posterior, se analiza una muestra de voz actual proporcionada por el usuario para obtener un perfil de voz actual que se compara con el perfil de voz inicial para generar una señal de control de acceso en respuesta al resultado de la etapa de comparación; en donde en la etapa de inscripción, así como en la etapa de verificación, se solicitan al usuario al menos unos elementos de datos de los medios de autenticación adicional como una muestra de voz y lo hablado por el usuario que serán objeto del análisis de su muestra de voz inicial, sin implicar una etapa de reconocimiento del habla.

Este documento, además, describe un esquema para implementar dicho proceso.

Es un objetivo de la invención proporcionar un proceso mejorado y un aparato para controlar el acceso de un usuario a un servicio proporcionado en una red de datos que es, particularmente, relativamente fácil de implementar y usar, así como aceptable con relación a los aspectos de costo.

Este objetivo, con relación a los aspectos del proceso, se resuelve mediante un proceso de acuerdo con la reivindicación 1 y, con relación a los aspectos del dispositivo, se resuelve mediante un esquema de acuerdo con la reivindicación 9. Las modalidades preferidas de la invención son objeto de las reivindicaciones dependientes.

La invención tiene la intención de mejorar un proceso para autenticar a un usuario, para controlar su acceso remoto a un servicio, base de datos o red de datos, en donde, en una etapa de inscripción, se analiza una muestra de voz inicial proporcionada por el usuario para obtener un perfil de voz inicial específico del usuario y, en una etapa de verificación posterior, se analiza una muestra de voz actual proporcionada por el usuario para obtener un perfil de voz actual que se compara con el perfil de voz inicial para generar una señal de control de acceso en respuesta al resultado de la etapa de comparación. La mejora incluye la idea de proporcionar los medios de autenticación adicional especializados en el usuario que se generan en un periodo de pre-inscripción, usándose los medios de autenticación adicional para autenticar al usuario en la etapa de inscripción y/o en una etapa de control de acceso antes e independiente de la etapa de inscripción, en un procedimiento de autenticación provisional o complementario.

Correspondientemente, con relación a los aspectos del aparato, la invención tiene la intención de mejorar un esquema para llevar a cabo este proceso y para este propósito comprende un servidor de autenticación en la medida que el servidor de autenticación comprende los medios de generación de los perfiles de voz, los medios de almacenamiento de los perfiles de voz y los medios de comparación de los perfiles de voz para obtener una primera

salida de autenticación basada en la muestra de voz entrada por el usuario y los medios de procesamiento de los datos de usuario, los medios de almacenamiento de los datos de usuario y los medios de comparación de los datos de usuario para obtener una segunda salida de autenticación a partir de los datos entrados por el usuario y los medios de generación de la señal de control de acceso para generar una señal de control de acceso en respuesta a las salidas de autenticación primera y segunda.

Una diferencia clave con respecto a las soluciones biométricas de voz existentes es que el procedimiento de autenticación del 2.º factor propuesto no se basa en la biometría de la voz como la única capa de seguridad, sino que combina, en una solución de seguridad, una capa de seguridad adicional fuera de banda con la autenticación de la voz.

Esto hace que sea posible aceptar una disminución en el umbral de la parte de verificación de la voz, debido a que la integración de la 2.ª capa de seguridad puede compensar esta disminución en la FAR de la autenticación de la voz e incluso elevar el nivel de seguridad. La información relevante (o los medios de autenticación de hardware) de la 2.ª capa se vincula con un único usuario. Por lo tanto, la misma sólo se puede usar por este usuario específico. En el caso de la pérdida de un componente de hardware (tarjeta de ID), ningún otro usuario puede acceder al sistema, debido a que el nivel de autenticación de la voz-seguridad aún está presente. Se puede otorgar y usar una nueva tarjeta sin ningún problema, ya que la muestra de voz inscrita sigue siendo la misma y sólo tiene que reemplazarse la segunda capa de seguridad. No es necesario repetir la inscripción y el usuario puede usar el sistema inmediatamente después de obtener la nueva tarjeta.

El objetivo final de un sistema biométrico de voz no debe ser un nivel de inscripción del 100%, pero sí un nivel de automatización del 100%. Los usuarios sólo se inscriben en el sistema una vez que tienen la necesidad de un servicio. La inscripción y la obtención de la prestación del servicio se incluirán preferentemente en un único proceso. Esto resulta en una menor carga en los canales de voz debido a que el número de usuarios, que se inscriben en el sistema básicamente al mismo tiempo, se puede reducir considerablemente. La llamada "Inscripción-Bajo-Demanda" resuelve muchos de los problemas existentes: los usuarios no tienen que inscribirse en el sistema dentro de un período de tiempo determinado. El número de puertos no tiene que extenderse solamente para servir el mayor número de usuarios a inscribirse, y los procedimientos de inscripción y de primeros servicios se pueden combinar en un único proceso, aumentando así la aceptación del usuario.

Un esquema para autenticar a un usuario y controlar su acceso remoto a un servicio, base de datos o red de datos comprende:

unos datos de usuario y un terminal de telecomunicaciones que comprende los medios de entrada de datos usando una funcionalidad de DTMF, tal como un teclado o pantalla táctil, y los medios de entrada de voz para introducir una muestra de voz del usuario,

un servidor de autenticación para el procesamiento de los datos y las muestras de voz entrados por el usuario y

una conexión de red al menos temporal del terminal de usuario al servidor de autenticación,

en donde el servidor de autenticación comprende los medios de generación de los perfiles de voz, los medios de almacenamiento de los perfiles de voz y los medios de comparación de los perfiles de voz para obtener una primera salida de autenticación basada en la muestra de voz entrada por el usuario y los medios de procesamiento de los datos de usuario, los medios de almacenamiento de los datos de usuario y los medios de comparación de los datos de usuario para obtener una segunda salida de autenticación a partir de los datos entrados por el usuario y los medios de generación de la señal de control de acceso para generar una señal de control de acceso en respuesta a las salidas de autenticación primera y segunda,

el esquema que comprende además:

los medios de instrucción de la entrada de la muestra de voz para indicarle al usuario que entre un PIN o un código similar o unos elementos de información predeterminados como una muestra de voz mediante los medios de entrada de voz, y

los medios de almacenamiento de muestras de texto para almacenar muestras de texto que están sujetas a la muestra de voz entrada por el usuario, en respuesta a la instrucción obtenida del servidor de autenticación, en donde los medios de almacenamiento de las muestras de texto se conectan a los medios de procesamiento de la voz para habilitar el procesamiento de la muestra de voz del usuario por medio de un análisis de voz independiente del texto, sin una etapa de reconocimiento automático del habla,

en donde, particularmente, los medios de instrucción de la entrada de la muestra de voz se adaptan para emitir las instrucciones al usuario en función de una tarjeta de ID de usuario o una tarjeta de ID específica del sistema que comprende las muestras de texto almacenadas en la memoria de muestras de texto o identificadores únicos de las muestras de texto.

Más específicamente, en dicho esquema el servidor de autenticación comprende:

los medios de procesamiento de la voz para analizar las muestras de voz del usuario para obtener un perfil de voz respectivo específico del usuario,

los medios de almacenamiento de los perfiles de voz para almacenar las muestras de voz del usuario procesadas y el primer medio comparador para comparar un perfil de voz actual evaluado a partir de la muestra de voz actual del usuario con un perfil de voz inicial almacenado en los medios de almacenamiento de los perfiles de voz, y

los medios de generación de la señal de control de acceso que se conectan a una salida del primer medio comparador, para producir una señal de control de acceso en respuesta a la salida del primer medio comparador, en donde

el servidor de autenticación comprende además

los medios de recepción de los datos del usuario para recibir los datos entrados en el terminal de usuario a través de los medios de entrada de datos,

los medios de almacenamiento de los datos para almacenar los datos de referencia correspondientes del usuario, y el segundo medio comparador para comparar los datos del usuario referenciados con los datos actualmente recibidos desde el terminal de usuario, conectándose la salida del segundo medio comparador a una entrada auxiliar de los medios de generación de la señal de control de acceso, para permitir que los medios de generación de la señal de control de acceso produzcan una señal de control de acceso auxiliar en respuesta a una entrada desde el segundo medio comparador.

En otra modalidad, en dicho esquema de acuerdo con la reivindicación 9 ó 10, los medios de instrucción de la entrada de la muestra de voz se adaptan para emitir las instrucciones al usuario en el contexto de un diálogo sistema-usuario través de una red de telecomunicaciones o de datos.

En una modalidad adicional de dicho esquema, se proporcionan los medios de generación de la tarjeta de ID para generar una tarjeta de ID física específica del sistema que comprende un ID específico del sistema o un código similar que se asigna inequívocamente a un conjunto de elementos de información específicos del usuario, incluyendo opcionalmente el conjunto un ID de usuario, y

los medios de almacenamiento de ID para almacenar el ID específico del sistema o un código similar en una asignación inequívoca al conjunto de elementos de información específico del usuario, en donde los medios de almacenamiento de ID actúan como los medios de almacenamiento de los datos de usuario y se conectan a una entrada del segundo medio comparador.

Este último esquema comprende preferentemente los medios de activación de la tarjeta de ID del usuario para activar una tarjeta de ID específica del sistema generada y distribuida previamente en respuesta a la entrada del ID específico del sistema o un código similar a través de un terminal de datos o de telecomunicaciones.

Las ventajas y los aspectos adicionales de la invención resultan de la siguiente descripción de las modalidades preferidas con referencia a las figuras. De estas:

La Fig. 1	muestra una representación esquemática de un primer ejemplo del esquema de acuerdo con la invención como un diagrama de bloques funcional,
Las Figs. 2A y 2B	muestran las dos superficies de una tarjeta de ID de usuario a usarse en una modalidad de la presente invención,
La Fig. 3	muestra un procedimiento de inscripción ilustrativo sobre la base de la tarjeta de ID de usuario de la Fig. 2,
La Fig. 4	muestra un procedimiento de verificación ilustrativo, sobre la base de la tarjeta de ID de usuario de la Fig. 2,
La Fig. 5	muestra un procedimiento de inscripción de acuerdo con una segunda modalidad de la invención, y

Las Figs. 6A y 6B muestran las dos superficies de una tarjeta de ID ilustrativa a usarse en una modalidad adicional de la presente invención.

La Fig. 1 muestra esquemáticamente la estructura de una modalidad del esquema de acuerdo con la invención, con un servidor del sistema 1 (que, ilustrando verbalmente su función principal, se puede referir además como un servidor de autenticación) como un elemento de vínculo entre un teléfono móvil 3 de un usuario y un servidor de gestión de datos 5 de una base de datos 7. El servidor de gestión de datos 5 no se especifica en absoluto más abajo; aquí, generalmente, es sinónimo de cualquier tipo de funcionalidad con la cual el acceso a los datos o servicios gestionados internamente en el sistema se puede activar para el usuario de un teléfono móvil. Con respecto a las conexiones de señales mostradas, la ilustración se basa en la suposición de que el servidor del sistema está en el modo de autenticación.

El servidor del sistema 1 tiene una interfaz de salida de indicaciones al usuario 9, una interfaz de entrada del usuario 11 (que actúa simultáneamente como una interfaz de entrada de la muestra de voz) para la conexión temporal con el teléfono móvil 3 del usuario, y una interfaz de salida de la señal de control 13 para la conexión con el servidor de gestión de datos 5 para la salida de las señales de control al mismo.

De acuerdo con la estructura funcional (mostrada en una forma simplificada en la figura para mayor claridad) del servidor del sistema 1, la interfaz de entrada del usuario 11 se diseña simultáneamente como una bifurcación de la señal de entrada que permite la alimentación de las señales de entrada (por ejemplo, el MSISDN) transmitidas automáticamente por el teléfono móvil 3 hasta las unidades de procesamiento posteriores sobre una primera trayectoria de señal a y la alimentación de las entradas de voz del usuario hasta los componentes posteriores a través de una segunda trayectoria de señal b. En la primera trayectoria de señal a se proporciona una etapa de clasificación de la entrada digital 20 para encaminar los registros generados automáticamente en el teléfono móvil a lo largo de una primera trayectoria de señal parcial a1 hacia una etapa de reconocimiento del número de móvil 15, mientras que los datos introducidos digitalmente por el usuario se encaminan a través de una trayectoria de señal parcial a2 hacia una etapa de procesamiento de los datos del usuario 19 y en paralelo hacia una etapa de conmutación de la entrada del usuario 35.

La unidad de reconocimiento del número de móvil 15 emite una señal de control a una unidad de indicación al usuario 17 en respuesta a la adquisición del número de teléfono del móvil del usuario. Esta unidad 17 realiza toda la indicación al usuario durante los procesos de inscripción o de autenticación ejecutados con el sistema presentado y emite los elementos correspondientes de indicación al usuario a través de la interfaz de salida de indicaciones al usuario 9. El MSISDN adquirido se suministra por la unidad de reconocimiento del número de móvil 15 a una etapa de procesamiento de los datos de usuario 19 que, en total, se diseña para el procesamiento del extremo de entrada de todo tipo de datos de usuario. Allí, los datos se almacenan inicialmente en la memoria intermedia para su posterior procesamiento.

En respuesta a la salida de un indicador de usuario que proporciona una guía a través del procedimiento adicional por parte de la unidad de indicación al usuario 17 (con detalles que se describen posteriormente), el usuario hablará una parte de la muestra de voz. Las muestras de voz se encaminan a través de la trayectoria de señal b hacia una unidad de cálculo del perfil de voz 25, para obtener un perfil de voz actual del usuario.

Un perfil de voz calculado con éxito por la unidad de cálculo del perfil de voz 25 se encamina hacia una unidad de comparación del perfil de voz 27, donde el mismo se somete a una comparación con un perfil de voz del mismo usuario almacenado previamente, que se carga para este propósito fuera de una unidad de almacenamiento del perfil de voz 29. El direccionamiento correspondiente de la unidad de almacenamiento del perfil de voz 29 se asegura a través de la señal de salida de la unidad de reconocimiento del número de móvil 15, que suministra el indicador relevante para la identidad del usuario. Si la conformidad deduce a partir de la comparación de los perfiles de voz en la unidad de comparación 27 a un nivel adecuado de fiabilidad, esta unidad emite una señal de confirmación correspondiente a una primera entrada de una etapa OR 31.

La etapa de procesamiento de los datos del usuario 19 adquiere la información de usuario relevante a partir de un flujo de datos recibidos a través de la interfaz de entrada del usuario 11 y aísla los datos de autenticación relevantes para autenticar el usuario independiente de su perfil de voz. La etapa 19 compara estos datos con los datos de comparación correspondientes almacenados en la unidad de almacenamiento de datos del usuario 33 y puede (además de otras funciones que se han omitido en la funcionalidad simplificada presentada aquí) emitir una señal de confirmación hacia una segunda entrada de la etapa OR 31 como resultado de la comparación.

Otras entradas del usuario encaminadas a través de la bifurcación 20 (por ejemplo, una dirección de acceso requerida de un área de memoria, la designación de un servicio recuperado por el usuario o una cantidad de recarga para una tarjeta de prepago) se pueden encaminar hacia la entrada de una etapa de conmutación de la entrada del usuario 35. La etapa de conmutación de la entrada del usuario 35 se conecta a través de una entrada de control a la salida de la etapa OR 31, que establece la etapa 35 en un estado de conmutación de la entrada del usuario siempre que una señal de confirmación positiva esté presente en al menos una de sus entradas que identifica una

autenticación exitosa del usuario a través de su perfil de voz o a través de otras entradas (es decir, en un procedimiento de autenticación sustituto). En este caso, la entrada del usuario presente en el extremo de entrada se encamina hacia la interfaz de salida de la señal de control 13 y en última instancia conduce a habilitar el acceso a la base de datos 7 a través del servidor de gestión de datos 5 (o a la ejecución de una operación comparable, por ejemplo, la provisión de un servicio requerido o la ejecución de una transacción requerida debido a los datos de transacción almacenados en la base de datos 7).

Al mismo tiempo, una señal de control que indica la conmutación de las entradas del usuario se envía a la unidad de indicación al usuario 17, que emite las salidas correspondientes a la información de confirmación para visualizar/ mostrar datos en el teléfono móvil 3.

Un experto en la materia puede derivar fácilmente detalles de los procesos especiales para los escenarios de aplicaciones específicas a partir de la descripción anterior y por lo tanto será suficiente una explicación de un único ejemplo como se proporciona más abajo. Se deduce además de la siguiente descripción que el cálculo del perfil de voz y el reconocimiento de la voz para el propósito de la autenticación del 2.º factor, mostrada como un procesamiento paralelo en una forma simplificada en la Fig. 1, se pueden combinar condicionalmente de manera que la adquisición de una señal de confirmación para el acceso del usuario a la base de datos se intenta primeramente sobre la base de su perfil de voz y sólo se indica un procedimiento del 2.º factor si este intento de autenticación falla. Naturalmente, en tal modalidad, las combinaciones de señales entre las unidades de procesamiento individuales, la etapa de conmutación de la entrada del usuario y la unidad de indicación al usuario son correspondientemente más complejas y dependientes del tiempo.

A continuación, se describen modalidades ilustrativas de los procedimientos de inscripción y de verificación de acuerdo con la invención, cuyas modalidades incluyen la integración de una capa de seguridad adicional a la capa de seguridad basada en la autenticación de la voz y la eliminación de un reconocimiento automático del habla de la capa de seguridad de autenticación de la voz.

Las Figuras 2A y 2B muestran un ejemplo de una tarjeta de ID de usuario que se adapta al proceso propuesto, en una primera modalidad del mismo y que se puede entender como un medio de autenticación de hardware o "token rudimentario".

Cada usuario de la solución biométrica de voz recibirá una tarjeta de ID física. Él sólo podrá activar la tarjeta con un código PIN, el cual se enviará al usuario en una forma diferente a la tarjeta de ID y que se usa posteriormente para verificar su identidad durante la etapa de inscripción.

Opcionalmente, el usuario puede usar el código PIN recibido para obtener su tarjeta de ID en línea, introduciendo el código PIN en un sitio web específico. Después de introducir algunas credenciales como el código PIN, el usuario puede descargar en su computadora e imprimir la tarjeta de voz virtual en formato pdf o cualquier archivo de datos no modificable.

Como otra opción, el usuario puede usar el código PIN recibido para obtener su tarjeta de ID a través de un teléfono móvil, accediendo a una "página móvil" específica del proveedor del sistema. Después de introducir algunas credenciales como el código PIN, el usuario puede descargar la tarjeta como un bean de Java o cualquier otro archivo que se puede ejecutar en un teléfono móvil. A continuación, una tabla secreta que aparece en la tarjeta en la Fig. 2B se puede ejecutar en el teléfono móvil.

Esta tarjeta de ID incluye un ID de usuario, que está vinculado con una persona y un código de VT, que está vinculado con la empresa de la persona para identificar al usuario. Además de estos dos códigos, la tarjeta de ID de usuario incluye una matriz N x N con números vinculados unívocamente con el propietario de la tarjeta. Estos números o la tabla secreta, respectivamente, se usan como la segunda capa de autenticación. Opcionalmente, los números de la matriz se pueden ocultar con una capa protectora, que se tiene que raspar para usar los números, en este caso estos números serían PIN para un uso único, temporal, que se vuelven inválidos después de usarlos una vez.

Inscripción

1. El usuario llama al sistema para la inscripción. A diferencia del caso de una solución de ASR, donde el usuario tiene que decir su ID de usuario, en el caso de una inscripción basada en una tarjeta de ID de usuario, el usuario tiene que teclear su ID de usuario y su código de VT en la pantalla táctil, usando la funcionalidad de DTMF del teléfono.

Con la eliminación del ASR, se asegura que

a) la solución biométrica de voz permanezca flexible y escalable incluso en los países donde las soluciones de ASR no están disponibles en los idiomas respectivos y

b) se reduzca el factor de incomodidad, que resulta de la potencial falta de reconocimiento del ID de usuario. El usuario tiene que introducir el ID en la pantalla táctil del teléfono o en el teclado de la computadora y se cometen muy pocos errores.

2. El sistema le pide al usuario que introduzca los números específicos de la tabla secreta en la parte posterior de la tarjeta de ID que, opcionalmente, el usuario tiene que raspar antes de poderlos ver. Por ejemplo, en el ejemplo mostrado en la Fig. 2B: Por favor ingrese D2 → El usuario tiene que leer 69, Por favor lea C5 → El usuario tiene que leer 12. En dependencia de la necesidad de seguridad, se usan una o más secuencias de desafío-respuesta.

3. Para garantizar que sólo se inscriban los usuarios reales, se proporciona un PIN al usuario de una manera separada. Este PIN se usa para verificar al usuario durante la inscripción.

4. En una siguiente etapa, el usuario tiene que pronunciar los números entregados por el sistema. Por ejemplo, el sistema podría pedir al usuario que cuente desde cero hasta nueve o le pide al usuario que repita cuatro números en una fila dos veces. Este procedimiento se basa en la autenticación de la voz independiente del texto, ya que el usuario se puede inscribir con otros números diferentes a los usados para la verificación. Por ejemplo, el usuario se inscribe con una cola de dígitos de 1-2-3-4 y verifica con una cola de dígitos de 4-3-2-1.

5. Después de recoger suficientes datos para crear el perfil de voz de la persona que habla, el usuario queda inscrito de manera exitosa en el sistema.

Verificación

1. El usuario llama al sistema para la verificación. El sistema le pide al usuario que introduzca su ID de usuario y el código de VT en una pantalla táctil.

2. El sistema le pide al usuario que introduzca los números específicos de la tabla secreta en la parte posterior de su tarjeta de ID, que opcionalmente, el usuario tiene que raspar antes de poderlos ver. Por ejemplo, en el ejemplo anterior: Por favor ingrese D2 → El usuario tiene que leer 69, Por favor lea C5 → El usuario tiene que leer 12. En dependencia del estándar de seguridad requerido, se usan una o más secuencias de desafío-respuesta.

3. En una siguiente etapa, el usuario tiene que repetir (hablar) los números dados por el sistema. A diferencia del procedimiento de inscripción, se requieren menos datos para verificar al usuario. Por ejemplo, el sistema le pide que repita cuatro números en una fila dos veces. Este procedimiento se basa en la verificación de la voz independiente del texto, ya que el usuario se puede inscribir con otros números diferentes a los usados para la verificación.

No se le informará al usuario sobre el resultado de las únicas etapas de autenticación. Por ejemplo, si la primera autenticación falla, el usuario todavía tiene que pasar por la segunda autenticación y sólo se le informará sobre el resultado después de las dos etapas de autenticación. Esto asegura que los posibles atacantes del sistema sólo obtengan una realimentación limitada sobre el éxito y el fallo de las diferentes capas de autenticación.

Una alternativa a la autenticación del 2.º factor descrita anteriormente basada en un componente de hardware similar a un token es la implementación de un segundo factor basado en secretos compartidos. Al igual que en el escenario explicado anteriormente ya no se necesita el ASR. El proceso de inscripción y de autenticación se basa en la tecnología de DTMF y de verificación de la voz. El siguiente escenario ejemplifica un entorno bancario:

Inscripción

1. El usuario llama al sistema para usar el servicio e inscribirse en el sistema. Para la identificación, el usuario tiene que teclear su número de cuenta bancaria o cualquier otra identificación única del usuario, seguido por el PIN usado o cualquier otra autenticación única del usuario. Estos dos factores se usan para la identificación inicial y la autenticación del usuario.

2. El usuario tiene que hacer una inscripción de voz. En un procedimiento de desafío-respuesta el usuario tiene que responder ciertas preguntas de desafío. Estos desafíos son, por ejemplo, el nombre del usuario o los secretos compartidos. Por ejemplo el usuario tiene que repetir su nombre y decir como un secreto compartido el apellido de soltera de su madre o la fecha/lugar de nacimiento.

3. Después de recoger suficientes datos para crear un modelo de la persona que habla, el usuario queda inscrito de manera exitosa en el sistema.

4. Después de pasar la etapa de inscripción de voz el usuario puede usar inmediatamente el servicio en la misma llamada de servicio. Por ejemplo, el usuario puede cambiar inmediatamente una contraseña o instruir alguna transacción financiera, etc. sin tener que llamar al sistema por segunda vez.

Verificación

1. El usuario llama al sistema para usar el servicio. Para la identificación, el usuario tiene que teclear su número de cuenta bancaria o cualquier otra identificación única del usuario. Como el usuario ya está inscrito en el sistema, ya no se necesita un PIN.

2. En la siguiente etapa, el usuario tiene que hacer una verificación de voz basada en la información proporcionada en la etapa de inscripción (nombre de usuario + secretos compartidos).

3. Después que el usuario se autentica de manera satisfactoria, él/ella puede usar el servicio.

La combinación de biometría de voz con secretos compartidos aumenta el nivel de comodidad y todavía garantiza un cierto nivel de seguridad ya que el usuario tiene que pasar por una etapa de autenticación y tiene que conocer los secretos compartidos. El sistema comprueba de esta manera algo que el usuario es y algo que el usuario conoce.

Un desarrollo adicional de los procedimientos de autenticación del 2.º factor como se explicó anteriormente es una extensión al escenario del secreto compartido. La modalidad explicada anteriormente demanda una autenticación segura del usuario en la fase de inscripción. Si el sistema no puede identificar y autenticar al usuario en la inscripción, un posible intruso podría, en principio, inscribirse en el sistema sin estar autorizado para hacerlo. En el ejemplo, esto se comprobó preguntando el número de cuenta bancaria y el PIN. En otros escenarios, la autenticación segura del usuario basada en una cadena de confianza existente es más difícil. En estos casos, el siguiente escenario, como se ilustra en la Fig. 5, es adecuado, ya que resuelve el problema mencionado en la primera etapa de inscripción de voz mediante la adición de una pre-registro basado en la web.

Inscripción (Parte 1)

1. La autoridad pertinente informa al usuario de la introducción de un sistema de biometría de voz. A diferencia de los esquemas actuales, el usuario no tiene que pasar por todo el procedimiento de inscripción de la autenticación de voz al inicio. El usuario sólo tiene que ejecutar una primera etapa de la registro por web. La inscripción de voz, que se necesita para autenticar al usuario para cualquier transacción futura, se hará más adelante.

2. El usuario tiene que acceder a un sitio web interno, autenticándose con su nombre de usuario existente y el PIN/contraseña o un PIN de registro adicional. Después de la identificación y la autenticación exitosa del usuario, se le pedirá a él/ella que proporcione las respuestas a una lista de preguntas secretas. Estas respuestas se almacenarán en el sistema y se usarán posteriormente para autenticar al usuario para una inscripción de voz y un proceso de cambio de contraseña.

Opción 1: Las respuestas secretas se tienen que teclear.

Opción 2: Las respuestas secretas se tienen que escoger de entre una selección de respuestas ofrecidas al usuario por el sistema (como se ejemplifica en la Fig. 5). No se necesita el ASR para la inscripción de voz; el usuario tiene que teclear el número correcto de la respuesta usando el teclado o la pantalla táctil del teléfono.

3. Después de que el usuario ha proporcionado la información solicitada, se completa la primera etapa de registro. Ahora el usuario puede llamar, por ejemplo, al servicio en cualquier momento que él/ella tenga la necesidad de este y completar el procedimiento de inscripción con las etapas de inscripción de la voz.

Inscripción (Parte 2)

4. Si el usuario tiene la necesidad de una nueva contraseña o desea usar cualquier otro servicio basado en la autenticación de la voz, él/ella llama a un número de teléfono determinado y se identifica con su ID de usuario o con cualquier otra identidad única proporcionada.

5. Basándose en la información proporcionada en la primera etapa del registro se le preguntará al usuario, ya sea que responda (Opción 1) o que teclee (Opción 2) las respuestas a una pregunta de desafío pre-registrada. En la opción 1, las respuestas orales se usan para ejecutar la evaluación del perfil de voz y crear un modelo de voz actual de la persona que habla, mientras que, si la opción 2 es válida, el sistema solicitará al usuario que diga algunas partes de texto predefinidas (números, nombres, etc), como se explicó con más detalle anteriormente en la primera modalidad. En este último caso, el procedimiento se demora un poco más de tiempo y requiere una mayor actividad por parte del usuario de manera que la opción 1 debe, al menos en principio, preferirse desde el punto de vista de la aceptación del usuario.

6. Después de recoger suficientes datos para crear un modelo de la persona que habla, el usuario queda inscrito de manera exitosa en el sistema.

7. Después de la inscripción de voz exitosa, el usuario puede usar inmediatamente el servicio de cambio de contraseña u otro servicio basado en la autenticación de la voz y no tiene que llamar de nuevo, todo se gestiona en una sola llamada.

Siguiendo este diálogo de desafío-respuesta con una combinación de secretos compartidos y la biometría de voz, el sistema garantiza un alto nivel de comodidad y seguridad. Por un lado, se comprueba la exactitud de las respuestas dadas, por otro lado se genera un modelo de voz para que él/ella reutilicen el servicio.

Verificación

1. Para cada acción adicional, el usuario llama al sistema para usar un servicio de voz. Para la identificación, el usuario tiene que teclear su número de cuenta bancaria o cualquier otra identificación única del usuario usando DTMF.

2. En la siguiente etapa, el usuario tiene que hacer una verificación de voz basada en la información proporcionada en las etapas de inscripción (nombre de usuario + secretos compartidos). Como el usuario ya está inscrito en el sistema ya no tiene que elegir entre las diferentes respuestas opcionales en el procedimiento de desafío - respuesta. Él sólo tiene que proporcionar la respuesta correcta a la pregunta formulada por el sistema.

Ahora se explicará una modalidad adicional de la invención, haciendo referencia a las Figuras 6A y 6B donde se ilustra una "tarjeta de voz". Se discutirá el caso de un empleado de una empresa, quien estará autorizado a usar un sistema de autenticación basado en el perfil de voz para tener éxito en el sistema de base de datos de una empresa, incluso después de haber olvidado una contraseña personal. La "tarjeta de voz" se distribuye a todos los empleados usando el sistema de autenticación. El uso de la tarjeta se basa en el principio Bajo Demanda; la tarjeta se tiene que activar antes de que se pueda usar.

En la superficie frontal de la tarjeta (Fig. 6A) existe un número de "tarjeta de voz", vinculado con un usuario específico en la base de datos del sistema antes de que la tarjeta se distribuya entre los usuarios. No existe una pre-vinculación de cualquier tarjeta con cualquier usuario antes de que la misma se envíe al operador del servicio. Las tarjetas se enviarán como tarjetas en blanco. Después de recibir las tarjetas, los ID de usuario existentes (ID numéricos, alfanuméricos, o incluso de múltiples usuarios) se pueden vincular con un cierto número de "tarjeta de voz" en la base de datos.

En la superficie posterior de la "tarjeta de voz" (Fig. 6B) existe una instrucción de cómo el usuario debe usar esta tarjeta para activarla, inscribirse en el sistema y autenticarse a sí mismo si fuera necesario.

Una ventaja importante consiste en que el usuario no tiene que tener en mente su ID de usuario ya que el mismo está vinculado en la base de datos con el número mostrado ("ID específico del sistema") en la tarjeta. Especialmente en empresas donde existen varios ID de usuario se hace difícil para los empleados tener en mente sus ID de usuario. En comparación con las soluciones existentes, existen muchas otras ventajas: en primer lugar, incluso sin acceso a una computadora (que no está disponible en la mayoría de las situaciones en las que un usuario ha olvidado su contraseña) un usuario puede cambiar su contraseña, incluso sin haber registrado su perfil de voz anteriormente. En las soluciones anteriores, un código PIN se envía por correo electrónico al usuario, etapa que es necesaria para la inscripción de voz. Habiendo bloqueado el sistema, el usuario no puede usar el servicio de cambio

de contraseña si él/ella no ha completado la inscripción de voz. El problema que enfrentan muchas soluciones biométricas de voz es que es difícil convencer a un usuario de hacer una inscripción de voz antes de que él/ella necesite realmente el sistema. Esto se puede resolver mediante el procedimiento de inscripción bajo demanda en el cual se basa la "tarjeta de voz".

Además, en el caso de la "tarjeta de voz" no existe una vinculación visible con un usuario y no existen datos específicos del usuario en la tarjeta. Si la tarjeta se pierde o es robada en el camino, un posible usuario fraudulento no puede inscribirse en el sistema ya que la tarjeta sólo se puede activar por el usuario que recibió la tarjeta. La activación se basará en una cadena de confianza existente. Esto significa que la tarjeta sólo se puede activar después de que el usuario ha accedido a un servicio determinado o sistema para el cual se necesitan los datos confidenciales del usuario.

A continuación se describirán unas etapas importantes al usar la "tarjeta de voz".

1. Pre-vinculación de la tarjeta con los datos del usuario

Antes de que la tarjeta se distribuya entre los usuarios, cada tarjeta (es decir, el ID específico del sistema mostrado en la tarjeta de voz) se vinculará con los detalles de los usuarios (por ejemplo, ID de usuario) en la base de datos. Por ejemplo, esto significa que el número de tarjeta 000000000000001 se puede corresponder con el ID de usuario aaa0001. Puede existir también una vinculación con ID de múltiples usuarios. Sin embargo, esta vinculación sólo existirá en la base de datos, no existe una vinculación visible de un cierto número de "tarjeta de voz" con un usuario específico.

2. Activación de la "tarjeta de voz"

Después que la tarjeta se ha entregado a un usuario, él/ella tiene que activarla para asegurarse de que el usuario correcto recibió la tarjeta correcta. Este procedimiento de activación se basa en una cadena de confianza existente. Por ejemplo, después de que el usuario inicie sesión en su computadora se le pedirá a él/ella que active su tarjeta de voz. Por ejemplo, *"Usted ha recibido su tarjeta de voz para realizar cambios de contraseñas automatizados en el futuro basados en la autenticación de la voz". Su número de tarjeta es: 000000000000001. Si esto es correcto, por favor presione."OK" para activar su tarjeta.* "Para este propósito, mediante el sistema de autenticación se proporciona un registro específico del usuario en un esquema, es decir, un esquema que se determina para un usuario específico y accesible sólo por este usuario previamente, sobre la base de los datos que están pre-almacenados en una base de datos del sistema.

Una vez que el usuario ha activado su tarjeta, él/ella puede usar la tarjeta para la inscripción y verificación de cualquier cambio de contraseña u otros servicios. Si la tarjeta se pierde en el camino o un usuario equivocado ha recibido un número equivocado, no se iniciará ni se llevará a cabo la activación y por lo tanto no será posible la inscripción de voz ni el cambio de contraseña para un usuario específico.

3. 1.^{er} uso de tiempo: inscripción de voz

Después de haber activado la "tarjeta de voz", el usuario puede hacer la inscripción de voz y el cambio de contraseña en cualquier momento que él/ella desee. Después de llamar a un número especializado, se le pedirá al usuario que introduzca su número de "tarjeta de voz" mediante DTMF, opcionalmente mediante el reconocimiento de la voz. En la base de datos, el ID específico del sistema se hará corresponder con el ID de usuario. Si el usuario no ha inscrito su voz hasta el momento, se le pedirá a él/ella que realice un procedimiento de desafío/respuesta para la inscripción de voz. En una primera etapa, el usuario tendrá que decir su nombre, respectivamente repetir su nombre un par de veces. Esta etapa sirve como un secreto compartido, ya que el nombre no es visible en ningún lugar de la tarjeta de voz y no es directamente vinculable para los estafadores. Esto significa que existe una autenticación de tres factores una vez que el usuario está inscrito.

Opcionalmente, el número de "tarjeta de voz" (ID específico del sistema) se hará corresponder con el ID de usuario en la base de datos. El ID de usuario o cualquier otra información específica del usuario se solicitará por teléfono y el usuario tendrá que repetirla un par de veces para el uso futuro. Esto significa que existe una autenticación de dos factores una vez que el usuario está inscrito.

Para una inscripción de voz adicional, al usuario se le pedirá que repita una palabra o secuencia de números varias veces hasta que exista un material de voz suficiente para crear un modelo de voz.

Después que se ha almacenado el perfil de voz en el servidor y se ha vinculado al usuario, el usuario puede cambiar inmediatamente una contraseña para un sistema objetivo elegido o puede usar cualquier otro servicio.

4. Uso normal

Para un uso normal, el procedimiento no es diferente a la etapa de inscripción de voz, excepto por el hecho de que las muestras de voz no se tienen que repetir un par de veces para crear una impresión de voz. En primer lugar, el usuario tiene que teclear su número de ID específico del sistema usando DTMF o mediante el reconocimiento de la voz. Como una siguiente etapa, el usuario tiene que, o bien responder a una pregunta de un secreto compartido (por ejemplo, su nombre), o repetir inmediatamente la información solicitada (por ejemplo, el ID de usuario). En las siguientes etapas, el usuario tiene que realizar un procedimiento de desafío/respuesta para verificar su voz. Después de la verificación de voz exitosa, el usuario puede cambiar la contraseña para un sistema objetivo elegido o puede usar cualquier otro servicio.

REIVINDICACIONES

1. Proceso para autenticar a un usuario, para controlar su acceso remoto a un servicio, base de datos o red de datos, en donde, en una etapa de inscripción, se analiza una muestra de voz inicial proporcionada por el usuario mediante los medios de análisis de voz independiente del texto, para obtener un perfil de voz inicial específico del usuario y, en una etapa de verificación posterior, se analiza una muestra de voz actual proporcionada por el usuario mediante los medios de análisis de voz independiente del texto, para obtener un perfil de voz actual que se compara con el perfil de voz inicial para generar una señal de control de acceso en respuesta al resultado de la etapa de comparación,
en donde los medios de autenticación adicional especializados en el usuario se generan en un periodo de pre-inscripción usando una funcionalidad de DTMF, usándose los medios de autenticación adicional para autenticar al usuario en la etapa de inscripción y/o en una etapa de control de acceso antes de, e independiente de la etapa de inscripción, en un procedimiento de autenticación provisional o complementario, en donde en la etapa de inscripción, así como en la etapa de verificación, se solicitan al menos unos elementos de datos de los medios de autenticación adicional como una muestra de voz y lo hablado por el usuario que serán objeto del análisis de su muestra de voz inicial, sin implicar una etapa de reconocimiento del habla.

2. Proceso de acuerdo con la reivindicación 1, en donde los medios de autenticación adicional comprenden un PIN o un código similar y una tarjeta de ID de usuario, en donde la tarjeta de ID de usuario se transmite al usuario a través de una red de datos a petición y en respuesta a una identificación preliminar mediante el PIN o el código.

3. Proceso de acuerdo con la reivindicación 1, en donde los medios de autenticación adicional comprenden un PIN o un código similar y un conjunto de elementos de información específicos del usuario, en donde el conjunto de elementos de información se introduce inicialmente por el usuario en el período de pre-inscripción.

4. Proceso de acuerdo con la reivindicación 1, en donde los medios de autenticación adicional comprenden una tarjeta de ID específica del sistema que visualiza un PIN único específico de sistema o un código similar, en donde el PIN o el código se vincula internamente en el sistema con un usuario específico y con los datos correspondientes de este usuario, incluyendo opcionalmente un ID de usuario y/o un conjunto de elementos de información específico del usuario y enviándose la tarjeta de ID específica del sistema como un tarjeta en blanco y activándose a petición del usuario y en respuesta a una entrada del PIN específico del sistema o el código similar en un terminal de datos o de telecomunicaciones del usuario.

5. Procedimiento de acuerdo con una de las reivindicaciones precedentes, en donde en la etapa de inscripción y/o en una etapa de control de acceso antes de la etapa de inscripción, al usuario se le solicita que ingrese un PIN o un código similar, opcionalmente junto con un elemento de información adicional específico del usuario, hablándolo o por medio de un teclado del terminal de datos o de telecomunicaciones, para identificar y autenticar provisionalmente al usuario para obtener el acceso a la etapa respectiva.

6. Proceso de acuerdo con una de las reivindicaciones precedentes, en donde el período de pre-inscripción y la etapa de inscripción son adyacentes en el tiempo entre sí y, particularmente, los medios de autenticación adicional se generan inmediatamente antes de la etapa de inscripción.

7. Procedimiento de acuerdo con una de las reivindicaciones precedentes, en donde el procedimiento de autenticación complementario se conecta a la etapa de inscripción o la etapa de verificación, respectivamente, de manera que se crea un procedimiento de autenticación combinado con una validez mejorada.

8. Procedimiento de acuerdo con una de las reivindicaciones precedentes, en donde las muestras de voz y datos entrados por el usuario se transmiten a un servidor de autenticación a través de un red de telecomunicaciones, particularmente basada en la telecomunicación móvil o el protocolo VoIP.

9. Esquema para autenticar a un usuario y controlar su acceso remoto a un servicio, base de datos o red de datos, comprendiendo el esquema un terminal de datos y de telecomunicaciones del usuario que comprende los medios de entrada de datos usando una funcionalidad de DTMF, tal como un teclado o pantalla táctil, y los medios de entrada de voz para introducir la muestra de voz del usuario,un servidor de autenticación para el procesamiento de los datos y las muestras de voz entrados por el usuario y
una conexión de red al menos temporal del terminal de usuario al servidor de autenticación,
en donde el servidor de autenticación comprende los medios de generación de los perfiles de voz, los medios de almacenamiento de los perfiles de voz y los medios de comparación de los perfiles de voz para obtener una primera salida de autenticación basada en la muestra de voz entrada por el usuario y los medios de procesamiento de los datos de usuario, los medios de almacenamiento de los datos de usuario y los medios de comparación de los datos de usuario para obtener una segunda salida de autenticación a partir de los datos entrados por el usuario y los medios de generación de la señal de control de acceso para generar una señal de control de acceso en respuesta a las salidas de autenticación primera y segunda,
el esquema que comprende además:

los medios de instrucción de la entrada de la muestra de voz para indicarle al usuario que entre un PIN o un código similar o unos elementos de información predeterminados como una muestra de voz mediante los medios de entrada de voz, y

los medios de almacenamiento de muestras de texto para almacenar muestras de texto que están sujetas a la muestra de voz entrada por el usuario, en respuesta a la instrucción obtenida del servidor de autenticación, en donde los medios de almacenamiento de las muestras de texto se conectan a los medios de procesamiento de la voz para habilitar el procesamiento de la muestra de voz del usuario por medio de un análisis de voz independiente del texto, sin una etapa de reconocimiento automático del habla,

en donde, particularmente, los medios de instrucción de la entrada de la muestra de voz se adaptan para emitir las instrucciones al usuario en función de una tarjeta de ID de usuario o una tarjeta de ID específica del sistema que comprende las muestras de texto almacenadas en la memoria de muestras de texto o identificadores únicos de las muestras de texto.

10. Esquema de acuerdo con la reivindicación 9, en donde el servidor de autenticación comprende
los medios de procesamiento de la voz para analizar las muestras de voz del usuario para obtener un perfil de voz respectivo específico del usuario,
los medios de almacenamiento de los perfiles de voz para almacenar las muestras de voz del usuario procesadas y el primer medio comparador para comparar un perfil de voz actual evaluado a partir de la muestra de voz actual del usuario con un perfil de voz inicial almacenado en los medios de almacenamiento de los perfiles de voz, y
los medios de generación de la señal de control de acceso que se conectan a una salida del primer medio comparador, para producir una señal de control de acceso en respuesta a la salida del primer medio comparador, en donde
el servidor de autenticación comprende además
los medios de recepción de los datos del usuario para recibir los datos entrados en el terminal de usuario a través de los medios de entrada de datos,
los medios de almacenamiento de los datos de usuario para almacenar los datos de referencia correspondientes del usuario, y
el segundo medio comparador para comparar los datos del usuario referenciados con los datos actualmente recibidos desde el terminal de usuario, conectándose la salida del segundo medio comparador a una entrada auxiliar de los medios de generación de la señal de control de acceso para permitir que los medios de generación de la señal de control de acceso produzcan una señal de control de acceso auxiliar en respuesta a una entrada desde el segundo medio comparador.

11. Esquema de acuerdo con la reivindicación 9 ó 10, en donde los medios de instrucción de la entrada de la muestra de voz se adaptan para emitir las instrucciones al usuario en el contexto de un diálogo sistema-usuario través de una red de telecomunicaciones o de datos.

12. Esquema de acuerdo con una de las reivindicaciones 9 a 11, que comprende
los medios de generación de la tarjeta de ID para generar una tarjeta de ID física específica del sistema que comprende un ID específico del sistema o un código similar que se asigna inequívocamente a un conjunto de elementos de información específicos del usuario, incluyendo opcionalmente el conjunto un ID de usuario, y
los medios de almacenamiento de ID para almacenar el ID específico del sistema o un código similar en una asignación inequívoca al conjunto de elementos de información específico del usuario, en donde los medios de almacenamiento de ID actúan como los medios de almacenamiento de los datos de usuario y se conectan a una entrada del segundo medio comparador.

13. Esquema de acuerdo con las reivindicación 12, que corresponde
los medios de activación de la tarjeta de ID del usuario para activar una tarjeta de ID específica del sistema generada y distribuida previamente en respuesta a la entrada del ID específico del sistema o un código similar a través un terminal de datos o de telecomunicaciones.

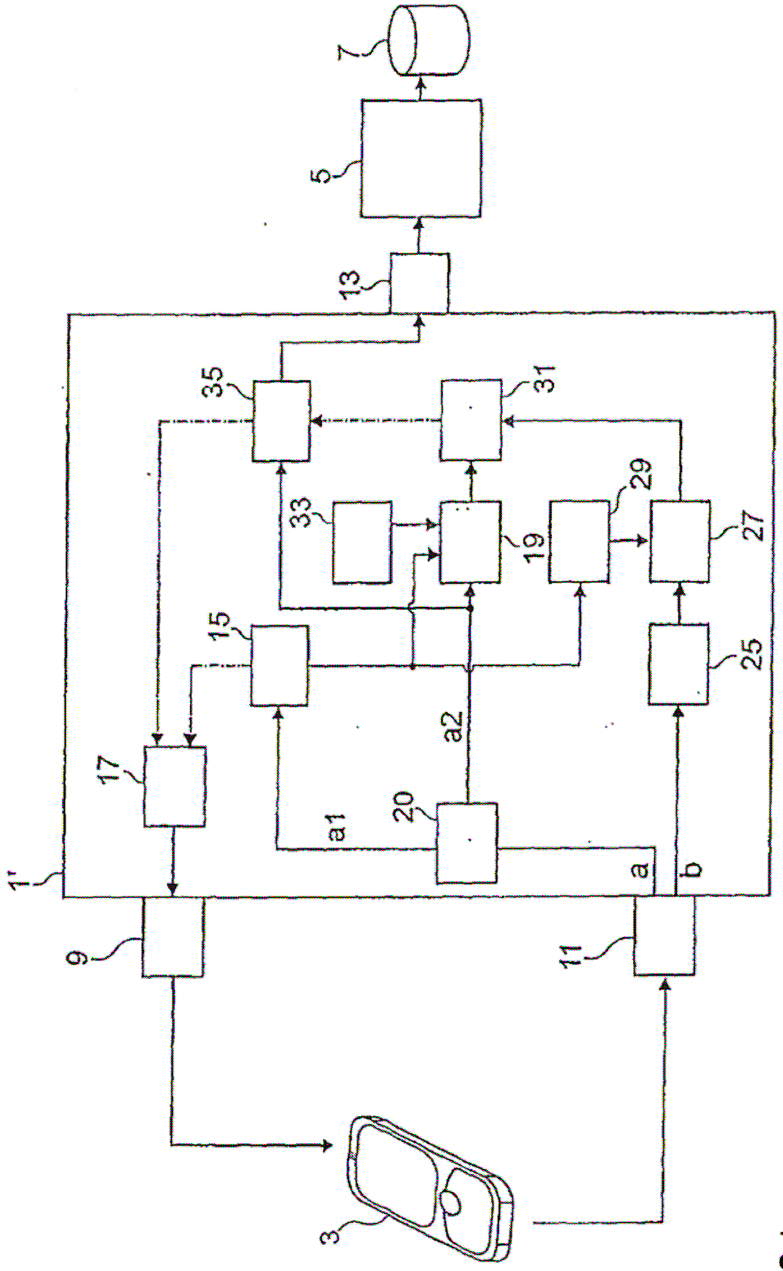


FIG1

FIG 2A

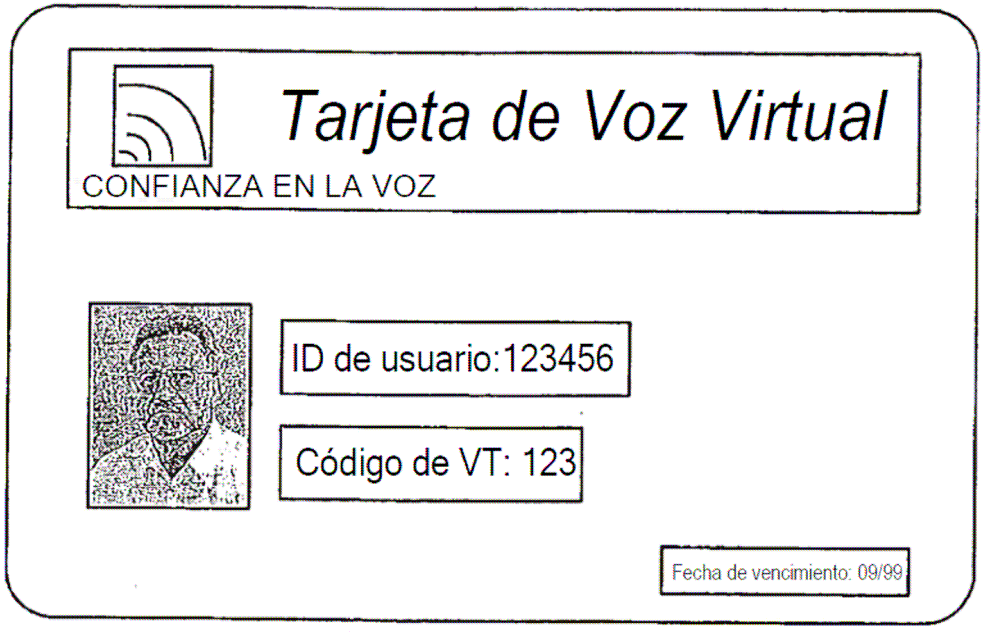
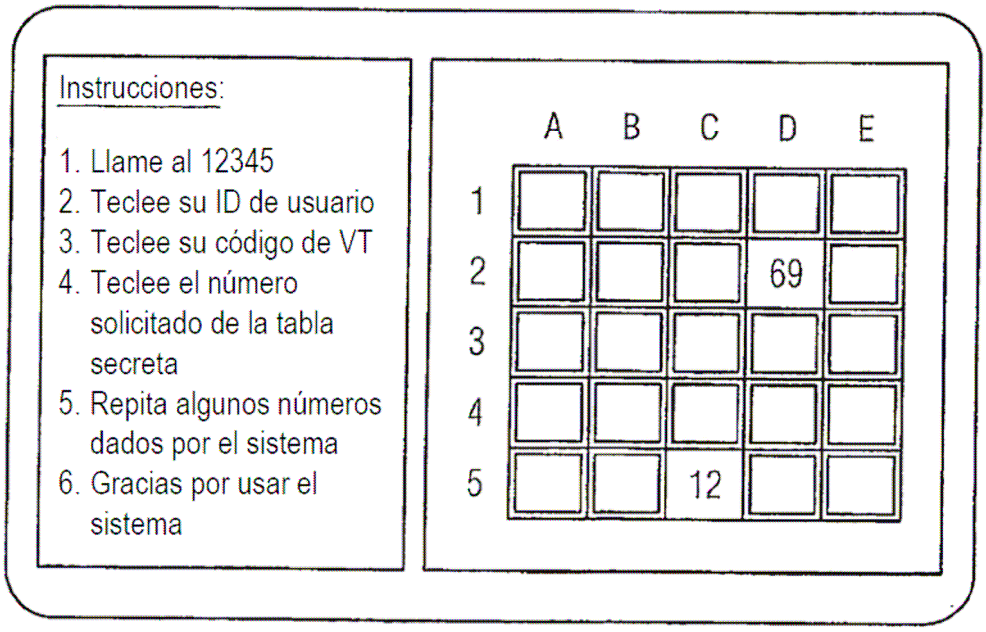

Tarjeta de Voz Virtual
CONFIANZA EN LA VOZ
ID de usuario:123456
Código de VT: 123
Fecha de vencimiento: 09/99

FIG 2B


Instrucciones:
1. Llame al 12345
2. Teclee su ID de usuario
3. Teclee su código de VT
4. Teclee el número solicitado de la tabla secreta
5. Repita algunos números dados por el sistema
6. Gracias por usar el sistema
A B C D E
1
2
3
4
5
69
12

Inscripción

Sistema:	"Bienvenido al servicio de voz virtual para cambio de contraseña. Para comenzar, por favor entre su ID de usuario."
Persona que llama:	"1-2-3-4-5-6-7"
Sistema:	"A continuación, por favor entre su código de VT."
Persona que llama:	"1-2-3"
Sistema:	"A continuación por favor entre los valores de su tabla secreta" A1
Persona que llama:	14
Sistema:	B5
Persona que llama:	56
Sistema:	C4
Persona que llama:	56
Sistema:	D2
Persona que llama:	69
Sistema:	E5
Persona que llama:	45
Sistema:	"Correcto, para inscribirlo al sistema, le preguntaré alguna información que usaré para aprender su voz y crear su impresión única de voz. Entonces cada vez que llame de nuevo podré verificar su identidad usando su voz."
Sistema:	"A continuación, por razones de seguridad por favor entre su PIN"
Persona que llama:	"*-*-*-*"
Sistema:	"A continuación, por favor cuente desde cero hasta nueve así: '0-1-2-3-4-5-6-7-8-9'. Por favor comience a contar ahora."
Persona que llama:	"0-1-2-3-4-5-6-7-8-9"
Sistema:	"La última etapa consiste en que adquiera práctica repitiendo algunos dígitos aleatorios, Ya que así su voz se verificará cuando llame de nuevo. Aquí vamos. Por favor diga éstos cuatro dígitos aleatorios,: cero dos tres cuatro"
Persona que llama:	"0-2-3-4"
Sistema:	Por favor repita "cero dos tres cuatro"
Persona que llama:	"0-2-3-4"
Sistema:	"Correcto, usted se ha inscrito correctamente en el Sistema. ¿Presione cualquier tecla para cambiar su contraseña?"
Persona que llama:	"*"
Sistema:	"Por favor tenga en cuenta, puede demorar hasta 15 minutos antes que pueda iniciar sesión con su nueva contraseña."
Sistema:	"Su nueva contraseña es cookie noventa y uno, se deletrea C-O-O-K-I-E nueve uno. ¿Por favor presione cualquier tecla para escucharlo de nuevo?"
Persona que llama:	"no_entrada"
Sistema:	"Gracias por llamar.¡Adiós!"

FIG 3

Verificación

Sistema:	"Bienvenido al servicio de voz virtual para cambio de contraseña. Para comenzar, por favor entre su ID de usuario."
Persona que llama:	"1-2-3-4-5-6-7"
Sistema:	"A continuación, por favor entre su código de VT."
Persona que llama:	"1-2-3"
Sistema:	"A continuación por favor entre los valores de su tabla secreta" A1
Persona que llama:	14
Sistema:	B5
Persona que llama:	56
Sistema:	C4
Persona que llama:	56
Sistema:	D2
Persona que llama:	69
Sistema:	E5
Persona que llama:	45
Sistema:	"A continuación usted necesitará repetir algunos dígitos aleatorios. Aquí vamos. Por favor diga: nueve seis siete cuatro"
Persona que llama:	"9-6-7-4"
Sistema:	Por favor repita "nueve seis siete cuatro"
Persona que llama:	"9-6-7-4"
Sistema:	"Se ha verificado su identidad. ¿Ahora, presione cualquier tecla para cambiar su contraseña?"
Persona que llama:	"*"
Sistema:	"Por favor tenga en cuenta que puede demorar hasta 15 minutos antes que pueda iniciar sesión con su nueva contraseña."
Sistema:	"Su nueva contraseña es cookie noventa y uno, se deletrea C-O-O-K-I-E nueve uno. ¿Por favor presione cualquier tecla para escucharlo de nuevo?"
Persona que llama:	"No_entrada"
Sistema:	"Gracias por llamar.¡Adiós!"

FIG 4

FIG 5

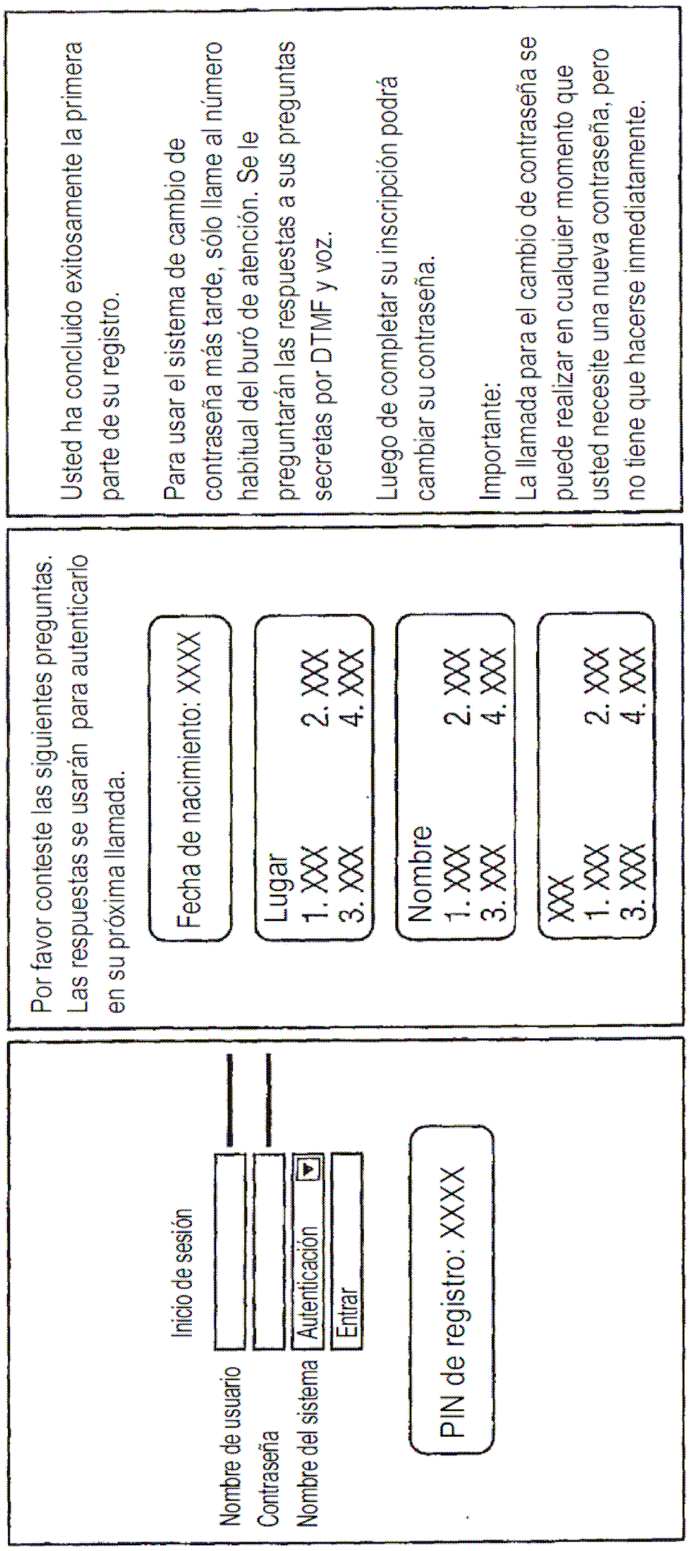

Inicio de sesión
Nombre de usuario
Contraseña
Nombre del sistema
Autenticación
Entrar
PIN de registro: XXXX
Por favor conteste las siguientes preguntas. Las respuestas se usarán para autenticarlo en su próxima llamada.
Fecha de nacimiento: XXXX
Lugar
1. XXX 2. XXX
3. XXX 4. XXX
Nombre
1. XXX 2. XXX
3. XXX 4. XXX
XXX
1. XXX 2. XXX
3. XXX 4. XXX
Usted ha concluido exitosamente la primera parte de su registro.
Para usar el sistema de cambio de contraseña más tarde, sólo llame al número habitual del buró de atención. Se le preguntarán las respuestas a sus preguntas secretas por DTMF y voz.
Luego de completar su inscripción podrá cambiar su contraseña.
Importante:
La llamada para el cambio de contraseña se puede realizar en cualquier momento que usted necesite una nueva contraseña, pero no tiene que hacerse inmediatamente.

FIG 6A

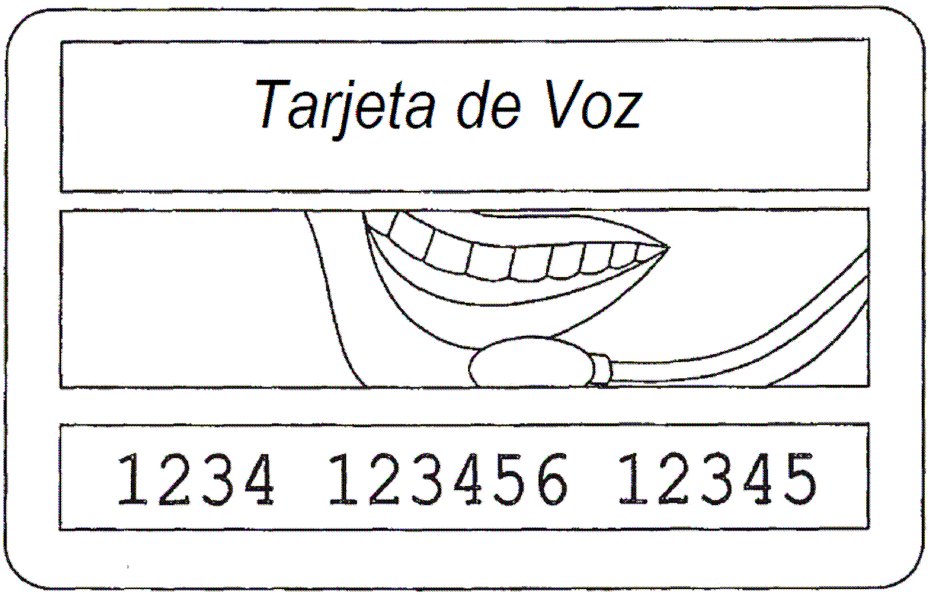
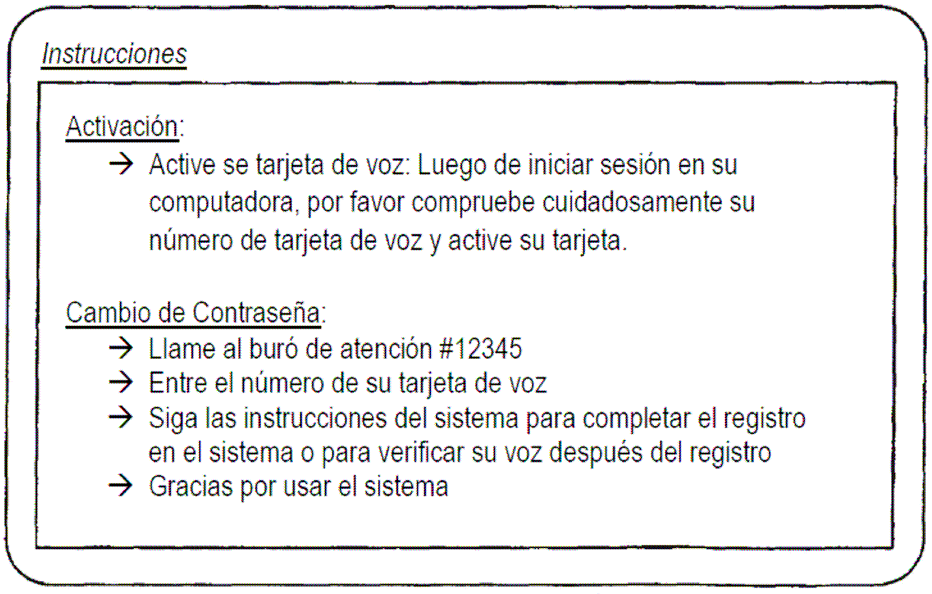

Tarjeta de Voz
1234 123456 12345

FIG 6B


Instrucciones
Activación:
→ Active se tarjeta de voz: Luego de iniciar sesión en su computadora, por favor compruebe cuidadosamente su número de tarjeta de voz y active su tarjeta.
Cambio de Contraseña:
→ Llame al buró de atención #12345
→ Entre el número de su tarjeta de voz
→ Siga las instrucciones del sistema para completar el registro en el sistema o para verificar su voz después del registro
→ Gracias por usar el sistema