(19) OFICINA ESPAÑOLA DE PATENTES Y MARCAS

ESPAÑA

(11) Número de publicación: **2 644 943**

(51) Int. CI.:

H04L 29/06 (2006.01)
G06F 21/33 (2013.01)

(12) TRADUCCIÓN DE PATENTE EUROPEA T3

(96) Fecha de presentación y número de la solicitud europea: **01.10.2008 E 08017269 (5)**

(97) Fecha y número de publicación de la concesión europea: **16.08.2017 EP 2068530**

(54) Título: **Procedimiento y sistema de comunicación para controlar el acceso a contenidos de medios en función de la edad del usuario**

(30) Prioridad:

03.12.2007 DE 102007058351

(45) Fecha de publicación y mención en BOPI de la traducción de la patente:
01.12.2017

(73) Titular/es:

DEUTSCHE TELEKOM AG (100.0%)
FRIEDRICH-EBERT-ALLEE 140
53113 BONN, DE

(72) Inventor/es:

BAUSE, THOMAS;
HESSE, HANS, JOACHIM y
KOMPART, ANDREAS

(74) Agente/Representante:

LEHMANN NOVO, María Isabel

DESCRIPCIÓN

Procedimiento y sistema de comunicación para controlar el acceso a contenidos de medios en función de la edad del usuario

La invención se refiere, en general, a autorizar el acceso a informaciones digitales, que están destinadas sólo a adultos, y en particular a un procedimiento para controlar el acceso a los contenidos de medios en función de la edad de un usuario. Además, la invención se refiere a un sistema de comunicación para controlar el acceso a los contenidos de medios en función de la edad del usuario.

Para garantizar, por ejemplo, que las películas de vídeos ofrecidas en Internet, que sólo están previstas para adultos, el acceso sólo se haga para ese círculo de personas, los usuarios de Internet deberán autentificarse antes de descargar esas películas de video y someterse a una verificación de la edad. Una verificación de la edad adecuada para esto se conoce bajo el nombre de “x-check” de la compañía coolspot AG. Este sistema de verificación de la edad permite el acceso a entretenimiento para adultos también por medio de un radiotransmisor y receptor móvil.

El concepto de “x-check” de la compañía coolspot AG fue valorado positivamente por la Comisión para la Protección Juvenil de los Medios (KJM). Otros conceptos valorados positivamente por la KJM para sistemas o bien módulos individuales para garantizar un grupo cerrado de usuarios, están compilados en un esquema accesible en una dirección de Internet http://web.archive.org/web/20070613084309/www.kjm-online.de/public/kjm/index.php ?show_1=91,85,56>.

Del documento WO 2006/076696 A2 se conoce un sistema y un procedimiento para la verificación de la edad y la identidad de personas y para restringir el acceso a material correspondiente, en el que tiene lugar una autentificación por medio de la configuración de un acceso a Internet, por ejemplo mediante un control cara a cara o mediante una comparación de números. En el caso de la comparación de números el usuario calcula a partir de una información de identificación, la cual identifica inequívocamente al usuario, por medio de una fórmula matemática predeterminada un primer valor numérico. La instancia de verificación determina mediante la misma fórmula matemática de una información de identificación asociada al usuario, cuál se solicita de una base de datos segura accesible, da un segundo valor, compara éste con el primer valor numérico y lleva a cabo por coincidencia una determinación de la edad. Un adulto autentificado con éxito recibe un acceso con completos derechos de acceso. Los menores autentificados pueden utilizar el acceso de los padres, para lo cual los adultos deben crear un perfil de usuario para el usuario menor de edad. Para acceder a un acceso configurado puede estar previsto un método de registro de dos capas, introduciendo inicialmente un ID de acceso con la contraseña correspondiente y después un ID de perfil con la contraseña correspondiente, para posibilitar un uso paralelo de un acceso común por múltiples usuarios de diferentes edades y diferentes perfiles de usuario.

En el documento EP 1804418 A1 se describe un procedimiento y un sistema para la autentificación, en el que un secreto compartido se almacena en un terminal de telecomunicación móvil y un servidor de autentificación y en el que para la autentificación por el terminal de telecomunicación se deposita un secreto compartido, y en el que para una identificación mediante el terminal de telecomunicación móvil, a partir del secreto compartido y de una información adicional, por ejemplo una información temporal, se genera una contraseña dinámica por medio de un algoritmo asociado y se transmite al servidor de autentificación. Allí, se recupera y comprueba la información adicional cifrada a través de la contraseña dinámica por medio de un algoritmo asociado y utilizando el secreto compartido.

La presente invención tiene por objeto proporcionar un procedimiento así como un sistema de comunicación para controlar el acceso a contenidos de medios en función de la edad del usuario, los cuales permitan una mayor seguridad en la verificación de la edad y una identificación inequívoca del usuario.

Una idea central de la presente invención estriba en que se realiza una verificación de la edad con una autentificación inequívoca del usuario para controlar el acceso a un contenido de medios solicitado. La verificación de la edad se realiza en un dispositivo de verificación de la edad y la autentificación del usuario en un servidor Trust-Center (centro de confianza). Para la autentificación y/o autorización del usuario se genera una sola vez, tanto en el servidor como también en el terminal móvil, una contraseña única válida, que se comparan entre sí en el servidor. Las contraseñas únicas se vuelven a calcular en cada autentificación y/o autorización de un usuario. De esta manera, el sistema de comunicación y el procedimiento se pueden asegurar mejor frente a ataques pasivos. Además, los llamados ataques de repetición son imposibles.

El problema técnico mencionado anteriormente se resuelve por un procedimiento conforme a la reivindicación 1. En el caso de los contenidos de medios se trata preferiblemente de páginas web de servidores de Internet, películas de vídeo y similares que sólo pueden desbloquearse para personas con una edad mínima.

Un usuario que quiera solicitar un contenido de medios, introduce un primer identificador de usuario asignado a él en un terminal de comunicación. El primer identificador de usuario se designa a continuación también en el identificador de usuario para un contenido de medio escogido o como identificador de usuario para una página web. El primer identificador de usuario se transmite a un servidor de contenido de medios de un proveedor y a un servidor de un Trust-Center. En un terminal móvil, que está asociado con el usuario solicitante de contenidos de medios, se genera una primera contraseña única válida para el contenido de medios solicitado actualmente. Una segunda contraseña única se genera en el servidor del Trust-Center.

La primera contraseña única se transmite desde el terminal móvil al servidor del Trust-Center. Acto seguido, en el servidor del Trust-Center se lleva a cabo una autentificación y/o autorización del usuario, comparándose la primera y la segunda contraseña únicas.

Además, se lleva a cabo una verificación de la edad del usuario, en la que en respuesta a una segunda identificación correspondiente del usuario, se determina si el usuario que solicita el contenido de los medios tiene la edad mínima predeterminada.

La segunda identificación de usuario se asigna preferiblemente al usuario cuando se conecta al servicio de verificación de edad. En lo que sigue, la segunda identificación de usuario se designará también como el denominado AVS (sistema de verificación de edad). Dependiendo del resultado de la comparación de la autentificación del usuario y del resultado de la determinación de la verificación de la edad, se controla el acceso al contenido de los medios solicitados.

El acceso al contenido de medios solicitado se libera cuando coincide la primera y segunda contraseñas únicas y el usuario tiene la edad mínima preestablecida.

Una ventaja de la autentificación móvil del usuario se ha de ver en que para generar contraseñas únicas no se requiere cobertura de red por la red de telefonía móvil, ya que el cálculo de contraseñas únicas tiene lugar en el propio terminal móvil.

Perfeccionamientos ventajosos son el objeto de las reivindicaciones subordinadas.

Un perfeccionamiento ventajoso prevé que la primera y segunda contraseñas únicas se generen respectivamente bajo la utilización de una contraseña de base secreta compartida. La contraseña de base secreta compartida es conocida tanto por el servidor del Trust-Center como por el terminal móvil.

Debe señalarse en este punto que la contraseña de base secreta compartida está asociada de forma inequívoca al usuario del terminal móvil. Esto significa también, que a cada usuario que participa en el servicio de verificación de la edad y de autentificación, se le asigna una contraseña de base secreta compartida e individual. En la contraseña de base secreta compartida se aplica el mismo algoritmo, para generar la primera y segunda contraseña única. Es concebible que la contraseña de base corresponda a un valor numérico predeterminado, que cambia en cada nueva autentificación del usuario por un valor predeterminado.

Cuando el usuario se registra por primera vez en el servidor de contenido de medios, se introduce así el primer acceso del primer identificador de usuario y también el segundo identificador de usuario. En este caso se transmiten el primer y segundo identificador de usuario al servidor del Trust-Center. Con el fin de poder realizar una autentificación de usuario específica en el servidor del Trust-Center, se almacena el primer y segundo identificador de usuario así como la contraseña de base secreta compartida de al menos un usuario en el servidor o en una base de datos asociada a él, por ejemplo en forma de una tabla de guía.

Si al comparar la primera y segunda contraseña única (autentificación) en el servidor del Trust-Center se determina que ambas contraseñas únicas coinciden, y se determina, además, que el usuario tiene una edad mínima predeterminada (verificación de la edad), el usuario que solicita el contenido de medios en un servidor del Trust-Center se almacena en un grupo de usuarios referido al proveedor. El grupo de usuarios está asociado al proveedor del servidor del contenido de medios. De esta manera, el servidor del Trust-Center puede determinar fácilmente si un usuario que desea acceder a un contenido de medios está incluido en el grupo referido al proveedor. Para ello, se almacena el primer identificador de usuario en el servidor de contenido de medios. Esto garantiza que el usuario en registros siguientes en el servidor de contenido de medios del proveedor, sólo tenga que introducir el primer identificador de usuario.

El procedimiento de la verificación de la edad comprende, además, el paso del acceso a las informaciones del usuario almacenadas en una base de datos, que contienen datos individuales del usuario, especialmente la edad, y el segundo identificador de usuario del al menos un usuario. En la práctica, las informaciones de los usuarios de una pluralidad de usuarios están almacenadas en la base de datos. Los datos de los usuarios individuales se almacenan de forma segura mediante un control cara a cara en la base de datos.

Para asegurarse de que la segunda contraseña única generada por el servidor del Trust-Center pertenece también al usuario que solicita el contenido de medios, bajo la reacción al primer y/o segundo identificador de usuario del usuario se elige la contraseña de base secreta compartida asociada de forma correspondiente y después la segunda contraseña única utilizando la contraseña de base secreta compartida elegida.
Ventajosamente, en el caso del segundo identificador de usuario se trata del número de teléfono del terminal móvil. El terminal móvil es ventajosamente un teléfono móvil.

El terminal de comunicación, al cual se le ha introducido el primer y/o segundo identificador de usuario y ventajosamente está representado el contenido de medios solicitado, es un terminal independiente o el propio terminal móvil.

Para garantizar que el usuario sea el usuario autorizado, se le puede asignar al usuario un PIN de usuario personal. Ese PIN de usuario lo da el usuario cuando inicia sesión en el servicio de verificación de la edad y de autentificación. En consecuencia, este PIN de usuario se denomina a continuación también “AVS via OTP18-PIN” y el servicio se denomina “AVS via OTP18”. AVS representa el sistema de verificación de la edad, mientras que la secuencia de letras OTP representa contraseña única. El número 18 indica la edad mínima a modo de ejemplo. El PIN de usuario puede basarse en un conocimiento (por ejemplo, una contraseña o un PIN), en una propiedad (por ejemplo, una clave o una tarjeta inteligente), en una propiedad (por ejemplo, características biométricas como por ejemplo la voz, la imagen del iris o una huella dactilar) o en una combinación correspondiente. El PIN de usuario se transmite junto con la primera contraseña única del terminal móvil al servidor del Trust-Center. En el servidor del Trust-Center el PIN de usuario se compara con un PIN de usuario, asignado al usuario, almacenado en el servidor.

Mediante el uso de una contraseña única como también de un PIN de usuario asignado al usuario, el servidor del Trust-Center puede asegurar que el usuario que solicita el contenido de medios es realmente el autorizado. El acceso al contenido de medios no se autoriza además tampoco hasta que la verificación de edad muestre que el usuario tiene la edad mínima determinada.

El problema técnico arriba mencionado también se resuelve mediante un sistema de comunicación conforme a la reivindicación 12.

El sistema de comunicación presenta un servidor de un Trust-Center. El servidor del Trust-Center contiene un dispositivo de memoria en el que para al menos un usuario se almacena un primer y un segundo identificador de usuario. Además, el servidor comprende un dispositivo de generación para generar una contraseña única en respuesta al reconocimiento del primer y/o segundo usuario así como de un dispositivo de comparación para comparar una contraseña única generada con una contraseña única recibida por un terminal móvil. Además, el sistema de comunicación comprende al menos un terminal móvil que tiene un segundo dispositivo de generación para generar una contraseña única y un dispositivo de transmisión para transmitir la contraseña única al servidor del Trust-Center. Además, están previstos un servidor de contenidos de medios así como una base de datos, en la que están almacenados datos individuales del usuario, especialmente la edad y el segundo identificador de usuario de al menos un usuario. El sistema de comunicación presenta, además, un dispositivo de determinación, el cual, en respuesta a los datos individuales del usuario almacenados en la base de datos, determina si el usuario que solicita el contenido a los medios tiene una edad mínima determinada. Un dispositivo de control sirve para controlar el acceso a los contenidos de medios facilitados por el servidor de contenido de medios en función del resultado del dispositivo de comparación y del dispositivo de determinación, es decir, dependiendo del resultado de la autentificación y de la verificación de la edad.

Conforme a un perfeccionamiento ventajoso, las bases de datos y el dispositivo de determinación están asociados con el Trust-Center.

Además, el sistema de comunicación comprende ventajosamente un dispositivo de entrada para introducir el primer y/o el segundo identificador de usuario así como un tercer dispositivo de generación para generar una señal de solicitud para solicitar un contenido de medios en el servidor de contenido de medios. El dispositivo de entrada y el dispositivo de generación están asociados al terminal móvil o a un dispositivo de comunicación separado.

La invención se explica con más detalle con ayuda de un ejemplo de realización junto con una única figura.

La figura muestra un sistema de comunicación 10 a modo de ejemplo para la verificación de la edad y la autentificación de una persona utilizando una contraseña única. El sistema de comunicación 10 contiene un servidor 20 que está asociado a un Trust-Center. El servidor 20 presenta un dispositivo de generación 21 para generar una contraseña única. El dispositivo de generación 21 está configurado de tal manera que genera una nueva contraseña única utilizando un algoritmo predeterminado en cada autenticación de un usuario, por ejemplo, a partir de una contraseña base. La contraseña única es una contraseña que se utiliza para la autentificación y/o autorización de un usuario determinado. Una contraseña única de este tipo, sólo es válida para un único proceso de autentificación y no

puede utilizarse una segunda vez. En otras palabras, cualquier autentificación renovada del usuario requiere una nueva contraseña única.

El servidor 20 presenta, además, un dispositivo de comprobación 22 que puede comparar una contraseña única generada por el dispositivo de generación 21 con una contraseña única transmitida desde un terminal de telefonía móvil 40. Al servidor 20 está también asociado un dispositivo de memoria 23, en el que, por ejemplo, se almacenan todas las informaciones de usuario de todos los usuarios, que se reúnen formando un grupo de usuarios de un proveedor A. Naturalmente pueden almacenarse también grupos de usuarios de otros proveedores en el dispositivo de memoria 23. En el dispositivo de memoria 23 del servidor 20 están almacenados para cada usuario, por ejemplo, un identificador de usuario AVS, una contraseña de base secreta compartida, un PIN-AVS así como un identificador de usuario para la página web o las páginas web del servidor de contenido de medios 60 a la que un usuario correspondiente quiere acceder.

Al proveedor A está asociado en el presente ejemplo un servidor de contenidos de medios 60. De acuerdo con ello, los usuarios 1 hasta los usuarios n, almacenados en el dispositivo de memoria 23, son aquellos usuarios que se han registrado con éxito en el proveedor A y que quieren acceder por primera vez a contenidos de medios o ya han accedido a contenidos de medios que están almacenados en un dispositivo de memoria 63 del servidor de contenido de medios 60. El control y la supervisión del servidor 20 los asume un dispositivo de control 24. El dispositivo de control 24, el dispositivo de comprobación 22, el dispositivo de generación 21 y el dispositivo de memoria 23 pueden estar conectados todos entre sí para permitir una comunicación directa.

El terminal móvil 40, que es preferentemente un teléfono móvil, presenta, al igual que el servidor 20, un dispositivo de generación 41 para generar una contraseña única. El dispositivo de generación 41 utiliza el mismo algoritmo para la generación de una contraseña única que el dispositivo de generación 21 del servidor 20. Debe observarse en este punto, que el teléfono móvil 40 está asociado al usuario 1, cuyos datos están almacenados en la memoria 23. Además, el teléfono móvil 40 comprende una memoria 42 en la que está almacenada la contraseña secreta compartida que está asociada también al usuario 1 en la memoria 23. De manera usual, el teléfono móvil 40 dispone de una tarjeta SIM, en la que está almacenado un software de aplicación para apoyar el servicio de autentificación y verificación de la edad, en lo que sigue también denominada aplicación OTP (One-Time-Passwort). El usuario 1 puede llamar a la aplicación OTP al teléfono móvil 40 para controlar la iniciación del proceso de autentificación.

El servidor 20 puede estar unido con una base de datos AVS 30, que está dispuesta dentro o fuera del Trust-Center. La base de datos AVS 30 forma la base para una verificación de la edad por ejemplo del usuario 1, como se explicará con más detalle a continuación. La base de datos AVS está representada por una zona de memoria 31, en la que se almacenan informaciones del usuario tales como, por ejemplo, el identificador del usuario AVS del usuario 1, su nombre así como el dato de edad. En la práctica, en la zona de memoria 31 de la base de datos AVS 30 están contenidos los datos relevantes del usuario de aquellos usuarios 1 hasta m que participan en el servicio de autentificación y verificación de edad. Las informaciones del usuario se almacenan tras un control cara a cara del usuario respectivo en la base de datos 30. En la base de datos AVS 30 está dispuesto, además, un dispositivo de verificación de edad 32. Alternativamente, en el caso del dispositivo de verificación de edad 32 puede tratarse de un dispositivo separado localmente de la base de datos.

Como muestra la Figura, en el presente ejemplo al usuario 1 del teléfono móvil 40 está asociado un ordenador personal 50. El usuario 1 puede acceder por medio del ordenador personal 50, por ejemplo a través de una conexión a Internet, al menos a una página web almacenada en la memoria 63 del servidor de contenidos de medios 60. Para habilitar el acceso, la página web solicitada se transmite desde el servidor de contenidos de medios 60, por ejemplo a través de una conexión de Internet establecida, al ordenador personal 50 y se muestra allí. Al ordenador personal 50 está asociado un dispositivo de entrada 51, a través del cual el usuario 1, como se explica a continuación aún con más detalle, puede introducir un identificador de usuario para la página web y/o su identificador de usuario AVS. Con los símbolos de referencia 52 y 53 se indican los correspondientes campos de entrada.

En este punto cabe destacar, que el usuario 1 puede utilizar en una forma de realización alternativa, el teléfono móvil 40 en lugar del ordenador personal 50 para acceder al servidor de contenido de medios 60 cuando está configurado de manera correspondiente. En este caso, se construye por ejemplo una conexión a Internet entre el teléfono móvil 40 y el servidor de contenido de medios 60.

Además, cabe señalar que la base de datos AVS, el dispositivo de verificación de edad 32 y el servidor 20 pueden estar dispuestos dentro del Trust-Center o en lugares diferentes.

Los datos transmitidos desde el teléfono móvil 40 al servidor 20 del Trust-Center se transmiten preferiblemente a través de Internet. Para ello, el teléfono móvil 40 envía en primer lugar los datos a transmitir a través de una red de telefonía móvil a una estación base próxima, la cual transmite entonces los datos a través de Internet al servidor 20 junto con un controlador de comunicación móvil. De manera similar se pueden intercambiar datos de la base de datos AVS 30 y del dispositivo para la verificación de edad 32 con el servidor 20 a través de una conexión a Internet.

De forma ventajosa, el ordenador personal 50, el servidor de contenido de medios 60, el servidor 20 del Trust-Center, el teléfono de radio móvil, la base de datos AVS 30 y/o el dispositivo para la verificación de edad 32 pueden intercambiar entre sí datos con la participación de Internet.

Seguidamente se explica con más detalle el modo de funcionamiento del sistema de comunicación 10 ilustrado.

Se supone que el usuario 1 desea descargar una página web desde el servidor de contenido de medios 60 en su ordenador personal. Para ello, se debe realizar una verificación de edad y autentificación para el usuario 1.

Para poder realizar una verificación de la edad, al principio se realiza una comprobación de mayoría de edad y de existencia del usuario 1, por ejemplo, a través de un contacto personal (control cara a cara) en la operación de vencimiento del contrato del teléfono móvil (post-pago). Preferentemente, el usuario 1 debe identificarse de forma inequívoca presentando su documento nacional de identidad. Si el usuario 1 además se registra en el servicio de verificación de edad, entonces asigna un identificador de usuario AVS. El identificador de usuario AVS del usuario 1 está conectado ventajosamente con una cuenta prepago o post-pago, que se realiza en un Payment-Service-Provider (proveedor de servicios de pago). De esta manera, se pueden descontar los contenidos con coste de las páginas web solicitadas. Un sistema de pago de este tipo no se muestra en la Figura. Tras el control con éxito cara a cara, se almacenan datos del usuario en la zona de almacenamiento 31 de la base de datos 30, el identificador de usuario AVS y datos que demuestran que el usuario 1 existe y, por ejemplo, tiene por lo menos 18 años. De forma similar, la información de otros usuarios m se almacenan en la base de datos AVS.

Como ya se ha mencionado arriba, los datos necesarios para el uso de los servicios de autentificación son preferentemente la contraseña de base secreta compartida, el PIN AVS y el identificador AVS del usuario en cuestión almacenados en el servidor 20 del Trust-Center.

Antes de que el usuario 1 del teléfono móvil 40 pueda solicitar y descargar páginas web en función de la edad del servidor de contenido de medios 60 a través de su ordenador personal 50, tiene que registrarse una única vez en el proveedor A del servidor de contenido de medios 60. Para ello, en primer lugar se crea una conexión de comunicación del ordenador personal 50 al servidor de contenido de medios 60. El servidor de contenido de medios 60 transmite entonces un formulario de registro correspondiente al ordenador personal 50. El registro del usuario 1 se produce introduciendo en el dispositivo de entrada 51 del ordenador personal 50 un nuevo identificador de usuario para al menos una página web deseada o para el servidor de contenido de medios 60 en el campo de entrada 52, así como introduciendo su identificador de usuario AVS en el campo de entrada 53. El identificador de usuario AVS se le comunicó al usuario 1, por ejemplo en el registro del servicio de verificación de edad. De forma alternativa, el usuario 1 puede haberse asignado a sí mismo este identificador de usuario AVS. Cabe destacar en este punto que el usuario 1 puede asignarse un identificador de usuario propio para cada página web limitada en edad del servidor de contenido de medios 60. Alternativamente, también es concebible que el usuario 1 asigne un identificador de usuario único para el servidor de contenido de medios 60, de manera que pueda acceder no sólo a una determinada página web limitada en edad, sino a todas aquellas páginas web almacenadas en el servidor de contenido de medios 60. El identificador de usuario para la página web y el identificador de usuario AVS del usuario 1 se transmiten ahora desde el ordenador personal 50 directamente al servidor 20 del Trust-Center. Alternativamente, se puede transmitir el identificador de usuario para la página web 52 y/o el identificador de usuario AVS 53 del ordenador personal 50 al servidor de contenido de medios 60, y entonces ser reenviado al servidor 20. Además, el servidor de contenido de medios 60 puede transmitir una señal de petición al servidor 20 y eventualmente a la base de datos AVS 30. Debe señalarse en este punto, que el servidor de contenido de medios 60 puede reenviar a la base de datos AVS 30 el identificador de usuario AVS del usuario 1 recibido del ordenador personal 50. El identificador de usuario asociado al usuario 1 para la página web se almacena al principio temporalmente en el servidor de contenido de medios 60.

Tan pronto como el usuario haya llamado a la aplicación OTP en su teléfono móvil 40, se le pedirá que active su dispositivo de generación de contraseña única 41 e introduzca su PIN AVS. El dispositivo de generación 41 lee entonces de la memoria 42 la contraseña de base secreta compartida. Utilizando un algoritmo predeterminado, el dispositivo de generación 41 genera una contraseña única. La contraseña única generada por el dispositivo de generación 41 es transmitida junto con el PIN AVS introducido preferiblemente del teléfono móvil 40 al servidor 20.

Con el fin de generar en el servidor 20 asimismo una contraseña única, el dispositivo de control 24 puede procurar, en respuesta a la señal solicitada procedente del servidor de contenido de medios 60 y en respuesta al identificador de usuario AVS asociado al usuario 1 y/o del identificador del usuario de la página web, que la contraseña de base secreta compartida del dispositivo de generación 21 sea suministrada al usuario 1. El dispositivo de generación 21 genera entonces utilizando la contraseña de base secreta compartida asimismo una contraseña única para el usuario 1. En el servidor 20 tiene ahora lugar una autentificación del usuario 1, al comparar la contraseña única generada por el dispositivo de generación 21 con la contraseña única recibida del teléfono móvil 40. Adicionalmente, en el dispositivo de comprobación 22, el PIN AVS recibido del teléfono móvil 40 se puede comparar con el PIN AVS asociado al usuario 1 en la memoria 23. En el presente ejemplo se supone que tanto las dos contraseñas únicas

como también el PIN AVS almacenado en la memoria 23 coincidan con el PIN AVS recibido del teléfono móvil 40. De este modo se detecta la autenticidad del usuario 1.

El dispositivo de verificación de edad 32 comprueba, en respuesta al identificador de usuario AVS del usuario 1 recibido del servidor de contenido de medios 60 o del servidor 20, si el usuario 1 tiene la edad mínima predeterminada. En respuesta al identificador de usuario AVS, el dispositivo de verificación de edad 32 lee los datos de edad asociados al usuario 1 de la zona de memoria 31 y comprueba su contenido. En el presente ejemplo, el dispositivo de verificación de edad 32 determina que el usuario 1 es mayor de edad y, por tanto, puede acceder a las páginas web solicitadas del servidor de contenido de medios 60.
Conforme a una forma de realización preferida, el dispositivo de verificación de edad 32 informa al dispositivo de control 23 del servidor 20 que el usuario 1 es mayor de edad. El dispositivo de control 24 informa, por consiguiente, al servidor de contenido de medios 60 que el usuario 1 ha sido autentificado y que tiene más de 18 años. El registro del usuario 1 en el servidor de contenido de medios 60 se completa cuando los datos del usuario 1 - estos pueden ser el identificador de usuario AVS, la contraseña de base secreta compartida, el PIN AVS y el identificador de usuario para la página web solicitada – son asociados al grupo de usuarios del proveedor A y son almacenados correspondientemente en el dispositivo de memoria 23. Además, el identificador de usuario asociado al usuario 1 para la página web solicitada se almacena en una memoria 61 del servidor de contenido de medios 60 y se desbloquea el acceso a la página web dependiente de la edad almacenada en el servidor de contenido de medios 60 para el usuario 1. A continuación, el servidor de contenido de medios 60 puede transmitir la página web almacenada en la memoria 63 al ordenador personal 50 y/o al teléfono móvil. El usuario 1 puede darse de baja del grupo de usuarios para el proveedor A cuando encarga la cancelación de sus datos, por ejemplo, su identificador de usuario, en la memoria 23 del servidor 20 y en la base de datos AVS 30.

Si el usuario 1 desea en un momento posterior acceder de nuevo a la página web almacenada en el servidor de contenido de medios 60, sólo tiene que introducir su identificador de usuario para la página web solicitada en el campo de entrada 52 del ordenador personal 50 y activar la aplicación OTP 43 en su teléfono móvil 40. La aplicación OTP solicita de nuevo al usuario 1 activar el dispositivo de generación 41, y eventualmente introducir su PIN AVS. Utilizando la contraseña de base secreta compartida almacenada en la memoria 42, el dispositivo de generación 41 genera una nueva contraseña única que se transmite junto al PIN AVS al servidor 20. El identificador de usuario introducido en el ordenador personal 50 para la página web solicitada es transmitido al servidor de contenido de medios 60. Un dispositivo de comparación 62 comprueba si el usuario 1 ya se había registrado en el servidor de contenido de medios 60. Si es así, el identificador de usuario para la página web se reenvía al servidor 20. Si no es así, el servidor de contenido de medios 60 espera también aún un identificador de usuario AVS que indique que un nuevo cliente desea registrarse. Sin embargo, en el presente ejemplo, el identificador de usuario asociado al usuario 1 para la página web solicitada se reenvía al servidor 20. El servidor 20, es decir, el dispositivo de control 24, puede leer del dispositivo de memoria 23, según una ejecución ventajosa, en respuesta al identificador de usuario recibido, el identificador AVS asociado al usuario 1, y transmitirlo a la base de datos AVS 30 a través de una conexión de comunicación. Además, el dispositivo de control 24 provoca al dispositivo de generación 21 que éste genere una nueva contraseña única utilizando la contraseña secreta compartida del usuario 1 almacenada en la memoria 23. El dispositivo de comprobación 22 comprueba entonces de nuevo la contraseña única generada por el dispositivo de generación 21 y la contraseña única recibida del teléfono móvil así como el PIN AVS para el usuario 1 almacenado en la memoria 23 con el PIN AVS recibido del teléfono móvil 40. Además, el dispositivo de verificación de edad 32, en respuesta al identificador de usuario AVS recibido por el servidor 20, comprueba los datos de edad asociados al usuario 1. Se supone que tanto la verificación de la edad como la autentificación han confirmado la autorización para que el usuario 1 acceda a la página web ofrecida por el servidor de contenido de medios 60. A continuación de ello, el dispositivo de control 24 transmite un mensaje correspondiente al servidor de contenido de medios 60 que permite el acceso del ordenador personal 50 a las páginas web almacenadas en la memoria 63 y transmite la página web solicitada al ordenador personal 50.

Naturalmente, el acceso al servidor de contenido de medios 60 no se autoriza cuando la autentificación del usuario 1 en el servidor 20 y/o la verificación de la edad en el dispositivo de verificación de edad 32 no han dado un resultado positivo.

A continuación se explica a modo de ejemplo cómo puede registrarse el usuario 1 en el servicio de autentificación y verificación de edad. Se entiende que el usuario 1 quiere firmar un contrato temporal en un proveedor de telefonía móvil. Para ello primero solicita un acceso al móvil. Adicionalmente se registra el usuario 1 en el servicio de autentificación y verificación de edad “AVS via OTP18” mediante la indicación de su PIN AVS personal y su identificador de usuario AVS personal. Como ya se ha dicho, estos datos del usuario 1, que van a servir para el servicio de autentificación y verificación de edad, se almacenan en la base de datos AVS 30 junto con el identificador de usuario AVS que, por ejemplo, puede ser el número de móvil del teléfono móvil 40.

Alternativamente, los clientes existentes, es decir, los clientes que ya tienen un contrato temporal en un proveedor de telefonía móvil y han sido sometidos a un control cara a cara, se registran en el servicio de autentificación y verificación de edad con un WEB-Front-End. El vínculo con los clientes existentes, por ejemplo el usuario 1, tiene

lugar en este caso a través de un número de teléfono móvil. Para asegurarse de que el titular del contrato puede registrarse en el servicio de autentificación y verificación de edad, debe indicar el código PUK2 asignado por el operador de telefonía móvil, que luego es verificado por el operador de telefonía móvil. Si el operador de telefonía móvil determina que el usuario 1 es mayor de edad y que el teléfono móvil tiene una tarjeta SIM adecuada, la aplicación OTP se carga automáticamente por el proveedor de telefonía móvil en la tarjeta SIM. La transferencia de la aplicación OTP tiene lugar mediante una comunicación por radio según la tecnología Over-the-Air. Sin embargo, para ello el teléfono móvil 40 tiene que estar registrado en una red de telefonía móvil.

REIVINDICACIONES

1. Procedimiento para controlar el acceso a contenidos de medios en función de la edad de un usuario, con los siguientes pasos:

a) introducir un primer identificador de usuario del usuario en un terminal de comunicación (40, 50) de un usuario que solicita un contenido de medios;

b) transmitir el primer identificador de usuario a un servidor de contenido de medios (60) de un proveedor y un servidor (20) de un Trust-Center;

c) generar una primera contraseña única válida en un terminal móvil (40) para el contenido de medios actualmente solicitado, la cual está asociada al usuario que solicita el contenido de medios;

d) generar una segunda contraseña única en el servidor (20) del Trust-Center en respuesta al primer y/o segundo identificador de usuario del usuario;

e) transmitir la primera contraseña única del terminal móvil (40) al servidor (20) del Trust-Center;

f) comparar la primera y la segunda contraseña única en el servidor (20) del Trust- Center;

g) determinar, en respuesta al segundo identificador de usuario asociado al usuario, si el usuario que solicita el contenido de medios tiene una edad mínima determinada a través de un dispositivo de determinación (32); y

h) controlar el acceso al contenido de medios solicitado en función de los resultados de los pasos f) y g) mediante un dispositivo de control (24).

2. Procedimiento según la reivindicación 1, caracterizado por que la primera y segunda contraseña única se genera en cada caso utilizando una contraseña de base secreta compartida.

3. Procedimiento según una de las reivindicaciones precedentes, caracterizado por que en el caso de la primera entrada del primer identificador de usuario, paso a) contiene el paso de la introducción del segundo identificador y paso b) contiene el paso de la transmisión del segundo identificador al servidor (20) del Trust-Center y por que el primer identificador de usuario se almacena en el servidor de contenido de medios (60).

4. Procedimiento según la reivindicación 3, caracterizado por que el usuario que solicita el contenido de medios se almacena en el servidor (20) del Trust-Center en un grupo de usuarios de un proveedor relacionado, cuando en el paso f) se determina que coinciden la primera y la segunda contraseña única y cuando en el paso g) se comprueba que el usuario tiene una edad mínima determinada.

5. Procedimiento según una de las reivindicaciones precedentes, caracterizado por que el paso g) comprende los siguientes pasos:

acceder a la información de usuario almacenada en una base de datos (30), la cual contiene datos individuales del usuario, especialmente la edad, y el segundo identificador de usuario del al menos un usuario.

6. Procedimiento según una de las reivindicaciones precedentes, caracterizado por que en el servidor (20) del Trust-Center se almacenan el primer y segundo identificador de usuario así como una contraseña de base compartida del al menos un usuario.

7. Procedimiento según la reivindicación 6, caracterizado por que el paso d) comprende los siguientes pasos:
seleccionar en respuesta al primer y/o segundo identificador de usuario la contraseña de base secreta compartida asociada a este usuario y generar la segunda contraseña única elegida utilizando la contraseña de base secreta compartida.

8. Procedimiento según una de las reivindicaciones precedentes, caracterizado por que el segundo identificador de usuario es el número de teléfono del terminal móvil (40).

9. Procedimiento según una de las reivindicaciones precedentes, caracterizado por que el terminal de comunicación es un terminal móvil (40) o un terminal separado (50).

10. Procedimiento según una de las reivindicaciones precedentes, caracterizado por que se libera el acceso al contenido de medios solicitado cuando coinciden la primera y la segunda contraseña única y el usuario tiene la edad mínima determinada.

11. Procedimiento según una de las reivindicaciones anteriores, caracterizado por que en el servidor (20) del Trust-Center se almacena un PIN de usuario asociado al usuario, en el paso e) la primera contraseña única y un PIN de

usuario se transmiten del terminal móvil (40) al servidor (20) del Trust-Center y por que en el paso f) el PIN de usuario recibido por el terminal móvil (40) se compara con el PIN de usuario almacenado para el usuario.

12. Sistema de comunicación (10) para controlar el acceso a contenidos de medios en función de la edad de un usuario con

- un servidor (20) de un Trust-Center que presenta las siguientes características:

un dispositivo de memoria (23) en el que están almacenados un primer y un segundo identificador de usuario para al menos un usuario,

un primer dispositivo de generación (21) para generar una contraseña única en respuesta al primer y/o segundo identificador de usuario y un dispositivo de comparación (22) para comparar una contraseña única generada con una contraseña única recibida por un terminal móvil (40);

- al menos un terminal móvil (40) que comprende un segundo dispositivo de generación (41) para generar una contraseña única y un dispositivo de transmisión para transmitir la contraseña única al servidor (20) del Trust-Center;

- al menos un servidor de contenido de medios (60);

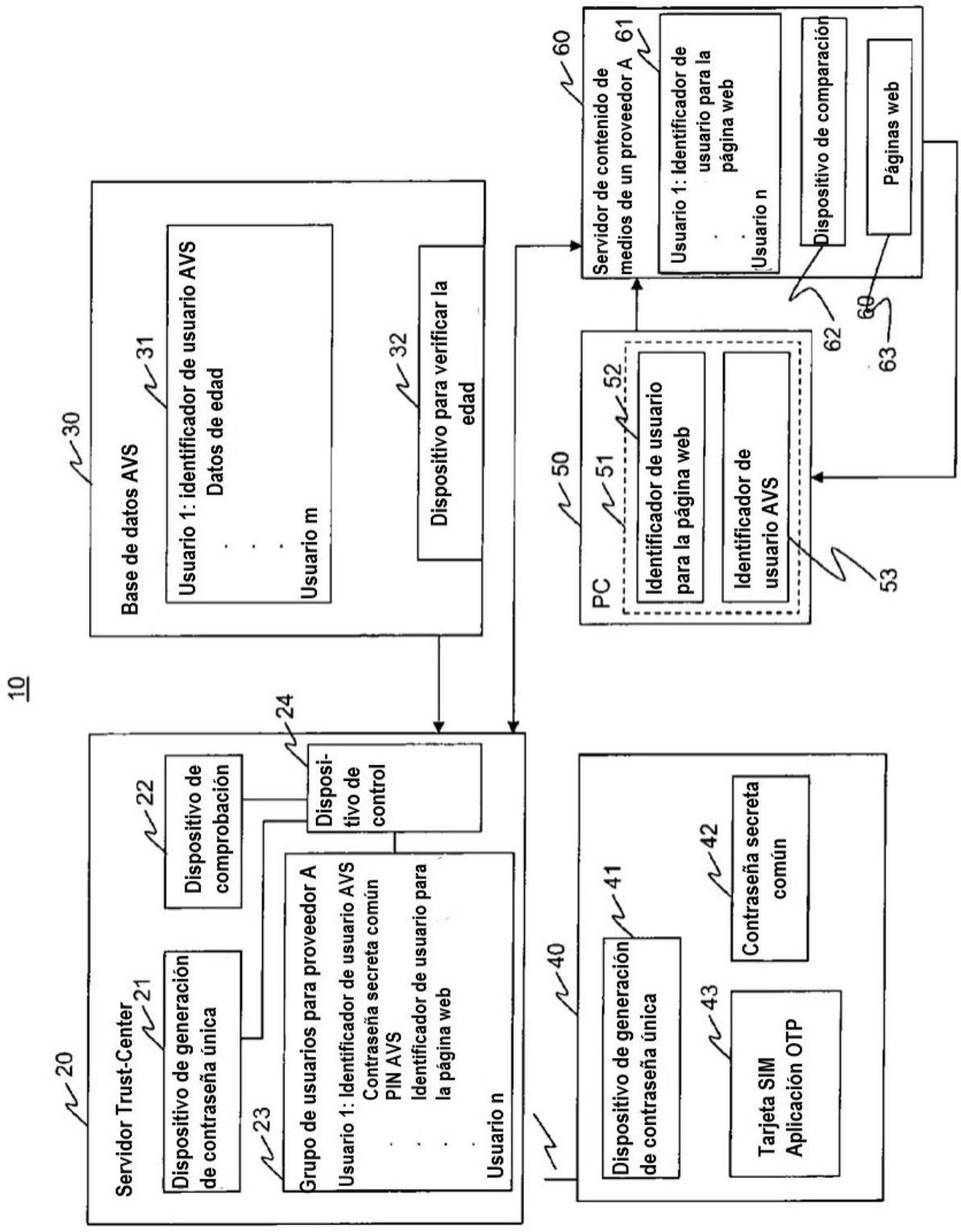
- una base de datos (30) en la que están almacenados datos individuales del usuario, especialmente la edad, y el segundo identificador de usuario del al menos un usuario;

- un dispositivo de determinación (32) para determinar, en respuesta a datos específicos del usuario almacenados en la base de datos (30), si el usuario que solicita un contenido de medios tiene una edad mínima predeterminada; y

- un dispositivo de control (24) para controlar el acceso al contenido de medios proporcionado en el servidor de contenido de medios (60) en función del resultado del dispositivo de comparación (22) y del dispositivo de determinación (32).

13. Sistema de comunicación según la reivindicación 12, caracterizado por que la base de datos (30) y el dispositivo de determinación (32) están asociados al Trust-Center.

14. Sistema de comunicación según la reivindicación 12 o 13, caracterizado por un dispositivo de entrada (51) para introducir el primer y/o segundo identificador de usuario así como un tercer dispositivo de generación para generar una señal de solicitud para solicitar el contenido de medios en el servidor de contenido de medios (60), en donde el dispositivo de entrada (51) y el dispositivo de generación están asociados al terminal móvil (40) o a un dispositivo de comunicación (50) separado.


10
20
Servidor Trust-Center
21
Dispositivo de generación de contraseña única
22
Dispositivo de comprobación
23
Grupo de usuarios para proveedor A
Usuario 1: Identificador de usuario AVS
Contraseña secreta común
PIN AVS
Identificador de usuario para la página web
Usuario n
24
Dispositivo de control
30
Base de datos AVS
31
Usuario 1: identificador de usuario AVS
Datos de edad
Usuario m
32
Dispositivo para verificar la edad
40
41
Dispositivo de generación de contraseña única
42
Contraseña secreta común
43
Tarjeta SIM
Aplicación OTP
50
PC
51
52
Identificador de usuario para la página web
Identificador de usuario AVS
53
60
Servidor de contenido de medios de un proveedor A
61
Usuario 1: Identificador de usuario para la página web
Usuario n
62
Dispositivo de comparación
63
Páginas web