(19) OFICINA ESPAÑOLA DE PATENTES Y MARCAS

ESPAÑA

(11) Número de publicación: **2 607 218**

(51) Int. CI.:

H04L 29/06 (2006.01)
G06F 21/32 (2013.01)

(12) TRADUCCIÓN DE PATENTE EUROPEA T3

(86) Fecha de presentación y número de la solicitud internacional: **17.06.2009 PCT/IB2009/052579**

(87) Fecha y número de publicación internacional: **23.12.2009 WO09153742**

(96) Fecha de presentación y número de la solicitud europea: **17.06.2009 E 09766279 (5)**

(97) Fecha y número de publicación de la concesión europea: **05.10.2016 EP 2291978**

(54) Título: **Mejora de la identificación y autentificación biométricas**

(30) Prioridad:

20.06.2008 EP 08158651

(45) Fecha de publicación y mención en BOPI de la traducción de la patente:
29.03.2017

(73) Titular/es:

KONINKLIJKE PHILIPS N.V. (100.0%)
High Tech Campus 5
5656 AE Eindhoven, NL

(72) Inventor/es:

KOSTER, ROBERT, P.;
AKKERMANS, ANTONIUS, H., M. y
VAN RIJNSOEVER, BARTHOLOMEUS, J.

(74) Agente/Representante:

ISERN JARA, Jorge

DESCRIPCIÓN

Mejora de la identificación y autentificación biométricas

CAMPO TÉCNICO

La presente invención se refiere a un procedimiento para mejorar la identificación y autentificación biométricas de los usuarios de los dispositivos electrónicos de consumo conectados a la red.

ANTECEDENTES

Con respecto a los dispositivos de electrónica de consumo (CE), hay una tendencia de que estos estén cada vez más y más habilitados para servicios en línea en red. Por ejemplo, las consolas de videojuegos actuales son compatibles con los servicios en línea (por ejemplo, Xbox Live). Además, los televisores estarán pronto equipados con funcionalidades tales como la funcionalidad de navegación por internet para acceder a los servicios. Normalmente, los dispositivos de CE habilitados para servicios se complementan con un portal de red que proporciona acceso a los servicios reales (como por ejemplo, la arquitectura presentada en Open IPTV Forum, Arquitectura Funcional - V 1.1 15 de enero de 2008).

Normalmente, los dispositivos de CE tienen medios de interacción con el usuario limitados, y los usuarios esperan que los dispositivos sean prácticos y fáciles de usar, requiriendo pocas operaciones para lograr un resultado. Por ejemplo, los usuarios suelen ser reacios a utilizar procedimientos de inicio de sesión repetitivos complejos usando nombre de usuario / contraseñas.

Con respecto a la identidad digital, los dispositivos de CE adoptan un enfoque limitado, por ejemplo para cumplir con el argumento de que sean prácticos, como se explicó anteriormente. Por ejemplo, la consola de videojuegos Nintendo Wii es compatible con múltiples caracteres ("Mii's"), pero estos no se utilizan para las transacciones o servicios con el acceso. Para las transacciones, el propietario del dispositivo puede vincular solo una cuenta por consola que será utilizada para realizar transacciones en línea, tales como la compra de juegos descargables. El uso de esta cuenta puede protegerse usando, por ejemplo, un PIN.

No hace falta decir que los dispositivos de CE, tales como consolas de videojuegos, son muy a menudo usados por varias personas, es decir, no solo el propietario de una consola de videojuegos utiliza la consola. Sin embargo, hasta ahora los servicios en línea son están personalizados, o como máximo, están asociados con un único usuario fijo (por ejemplo, para las transacciones).

El uso de características biométricas, biometría, proporciona una forma muy práctica para la sustitución de nombres de usuario, contraseñas y códigos pin en situaciones donde se necesita autentificación e identificación. La biometría es única para cada ser humano y no puede olvidarse, robarse ni perderse. Como tal, es un buen candidato para ser utilizado en el control de acceso y sistemas de transacciones electrónicas. En muchos de estos sistemas, se utiliza la biometría para realizar autentificación de uno a uno práctica y segura. Sin embargo, a pesar de la enorme mejora que ha tenido lugar durante la última década, las prestaciones de reconocimiento de casi todas las modalidades biométricas todavía no es suficiente para hacer que la biometría sea una herramienta fiable para fines de identificación de uno a muchos a gran escala, y se espera que esto siga así durante muchos años más.

Las prestaciones del estado de la técnica en términos de sistemas biométricos en la actualidad está en el orden del 1 % de tasa de error igual (EER). La EER se define como el punto de funcionamiento de los sistemas biométricos a una tasa de falsa aceptación (FAR) que es igual a la tasa de falso rechazo (FRR). En general, el TCE es una medida de prestaciones útil, y cuanto menor sea el valor, mejor es el sistema. Ajustando ligeramente un sistema de este tipo a un FFR algo mayor que 1 %, una FAR mínima de un 0,1 % parece posible. En consecuencia, si la FAR para un sistema de reconocimiento dado es de 0,1 %, esto significa que un impostor tiene un 0,1 % de probabilidad de que sus datos biométricos "parezcan" los de una persona genuina. Se puede demostrar que si se tiene que realizar la identificación, es decir, una comparación de uno a muchos, la probabilidad de que una persona se reconozca mal pasa a ser $FAR_{tot} = 1- (1-FAR)^{n.}$

Por ejemplo, si la FAR de un sistema de reconocimiento biométrico es de 0,1 %, y una persona se debe identificar de entre una base de datos de 30 personas, la probabilidad FAR_{tot} de encontrar a la persona equivocada es de $1-0,999^{30} = 0,03$, lo cual podría ser aceptable. Sin embargo, si se tiene que buscar en una base de datos de 300, la FAR_{tot} se convierte en el 26 %, lo cual hace que este sistema de identificación sea esencialmente inútil.

Además, dado que la biometría proporciona la información personal acerca de un ser humano, por lo general hay un problema de privacidad en relación con el almacenamiento y el uso de los datos biométricos. Con el fin de resolver este problema, los datos biométricos nunca deben almacenarse sin cifrar en una base de datos, sino más bien en una forma cifrada para garantizar la privacidad y evitar ataques maliciosos de determinación de compatibilidad cruzada de base de datos. Resolviendo este problema se incrementará el nivel de aceptación de la biometría. Tales

técnicas de preservación de la privacidad, a menudo denominadas sistemas de protección de plantilla, se han descrito en la técnica anterior, por ejemplo en WO2005/122467.

US2005/180618, el 18 de agosto de 2005 (2005-08-18), divulga un procedimiento para la autentificación de la identificación de una persona utilizando medios biométricos, y más particularmente, para su uso en terminales de punto de venta, para acceder a una red de ordenadores, para aplicaciones que implican ordenadores basados en el lápiz y bolígrafos inteligentes, y para el comercio electrónico.

SUMARIO

Con el fin de mejorar la técnica anterior, se proporciona, según un primer aspecto, un procedimiento de autentificación de un usuario en un dispositivo electrónico en una red de comunicación. El procedimiento comprende la obtención de una característica biométrica del usuario, la transmisión, a un servicio de red social, de la información que especifica al menos un usuario principal del dispositivo, recibiendo, desde el servicio de red social, la información que especifica un grupo de personas que tienen una relación social con al menos un usuario principal, obteniendo información que especifica un resultado de una operación de comparación biométrica con la característica biométrica de las características de los usuarios y biométricas de las personas en el grupo de personas especificado, con el resultado que indica si el usuario está autentificado en el dispositivo electrónico o no.

En otras palabras, mediante la reducción del tamaño del espacio de búsqueda necesario durante una operación de comparación mediante la utilización de información con respecto a un grupo de personas en una red social, la tasa de falsa aceptación se reduce y con ello se facilita la autentificación biométrica de un usuario en un dispositivo electrónico, por ejemplo, para acceder a la funcionalidad deseada del dispositivo o acceder a un servicio deseado.

Es decir, con respecto a los dispositivos electrónicos tales como dispositivos CE, por lo general solo una cierta parte de la población total es probable que sea relevante, a diferencia de las situaciones que implican, por ejemplo, servicios en línea, sistemas de seguridad de los aeropuertos, etc. Los invitados y nuevos usuarios de un dispositivo electrónico pueden autentificarse de forma práctica utilizando su identidad y perfil biométrico, sin necesidad de introducir información como su identificador y sin la necesidad de inscribir sus datos biométricos en el dispositivo.

Los modos de realización incluyen aquellos en los que la transmisión de información que especifica al menos un usuario principal del dispositivo comprende la transmisión de al menos un parámetro de limitación para limitar el número de personas en el grupo de personas especificado.

La transmisión de al menos un parámetro de limitación puede comprender la transmisión de un número que especifica el número máximo de personas en el grupo de personas especificado.

Los modos de realización incluyen aquellos en los que la transmisión de al menos un parámetro de limitación comprende la transmisión de información que especifica tipos de relaciones entre al menos un usuario principal y personas en una red social del usuario.

Los modos de realización incluyen aquellos en los que la transmisión de al menos un parámetro de limitación comprende la transmisión de información que especifica al menos un parámetro característico relacionado con las prestaciones del dispositivo en la obtención de la característica biométrica del usuario.

La transmisión de información que especifica al menos un parámetro característico relacionado con las prestaciones del dispositivo en la obtención de la característica biométrica del usuario puede comprender la transmisión de información relacionada con una tasa de falsa aceptación o una tasa de falso rechazo.

Los modos de realización incluyen aquellos que también comprenden la transmisión, a un proveedor de identidad, de información del grupo especificado de personas, recepción, del proveedor de identidad, de características biométricas de las personas en el grupo de personas especificado, y en los que la obtención de información que especifica un resultado de una operación de comparación biométrica comprende realizar la operación de comparación.

La recepción, del proveedor de identidad, de características biométricas de personas en la red social puede comprender la recepción de plantillas biométricas seguras y datos auxiliares asociados a las plantillas biométricas seguras, y en la que la operación de comparación puede comprender la utilización de las plantillas biométricas seguras y datos auxiliares.

Los modos de realización incluyen aquellos que también comprenden la transmisión, a un proveedor de identidad, de información del grupo especificado de personas, y en el que la obtención de información que especifica un resultado de una operación de comparación biométrica comprende la recepción de información, del proveedor de identidad, que especifica un resultado de una operación de comparación biométrica con la característica biométrica del usuario y las características biométricas de las personas en el grupo de personas especificado.

Tales modos de realización pueden comprender también la recepción, del proveedor de identidad, de datos auxiliares relacionados con plantillas biométricas que se asocian con las personas en el grupo de personas especificado, la generación de plantillas biométricas que utilizan los datos auxiliares y la característica biométrica del usuario, y la transmisión de las plantillas biométricas generadas al proveedor de identidad.

Los modos de realización incluyen aquellos que comprenden la determinación, en función de la información obtenida del resultado de la comparación biométrica, de si el usuario está autentificado para acceder a un servicio deseado por el usuario. Es decir, la autentificación del usuario para usar un servicio puede realizarse como consecuencia de que el usuario haya sido autentificado en el dispositivo.

En tales modos de realización, la transmisión de al menos un parámetro de limitación puede comprender la transmisión de al menos un parámetro de limitación que se obtiene de un proveedor del servicio deseado.

Según un segundo aspecto, se dispone de un dispositivo electrónico que comprende medios de entrada biométricos, circuitería de procesamiento y comunicaciones que están configurados para la autentificación de un usuario en el dispositivo electrónico en una red de comunicación. La circuitería de control está configurada para obtener una característica biométrica del usuario, transmitir, a un servicio de red social, la información que especifica al menos un usuario principal del dispositivo, recibir, desde el servicio de redes sociales, la información que especifica un grupo de personas que tienen una relación social con al menos un usuario principal, obtener información que especifica un resultado de una operación de comparación biométrica con la característica biométrica del usuario y las características biométricas de las personas en el grupo de personas especificado, con el resultado que indica si el usuario está autentificado en el dispositivo electrónico.

Según un tercer aspecto, se dispone de un producto de programa de ordenador que comprende instrucciones de software que, cuando se ejecutan en una unidad de procesamiento, llevan a cabo el procedimiento resumido anteriormente.

Según un cuarto aspecto, se dispone de un procedimiento para habilitar la autentificación de un usuario en una red de comunicación. Tal procedimiento comprende la recepción de información que especifica al menos un usuario principal, la recepción de una característica biométrica del usuario, la obtención de información que especifica un grupo de personas que tienen una relación social con al menos un usuario principal, la realización de una operación de comparación biométrica con la característica biométrica del usuario y las características biométricas de personas en el grupo de personas especificado, con el resultado que indica si el usuario está autentificado o no.

En consecuencia, los aspectos quinto y sexto proporcionan un aparato y un producto de programa de ordenador que realizan un procedimiento de este tipo.

BREVE DESCRIPCIÓN DE LOS DIBUJOS

Los modos de realización se describirán ahora con referencia a los dibujos adjuntos, donde:

la figura 1 ilustra esquemáticamente un diagrama de bloques de entidades que interactúan conectadas a una red de comunicación,

la figura 2 ilustra esquemáticamente un dispositivo electrónico,

la figura 3 es un diagrama de flujo de un procedimiento de autentificación, y

la figura 4 ilustra las redes sociales.

Descripción detallada de los modos de realización

Una red social especifica las relaciones sociales entre los usuarios. De esta manera, una red social de un usuario puede especificar su familia, amigos, colegas, amigos con quien hablar, etc. Desde un punto de vista tecnológico, las redes sociales son la representación de las relaciones sociales reales en algún tipo de estructura de datos o formato de datos. Los servicios de redes sociales ayudan a los usuarios a gestionar su(s) red(es) social(es) y utilizarlas, divulgarlas y compartirlas para una serie de propósitos. Este último puede ser el caso de la red en total, partes de la misma, o solo aspectos específicos como ciertos tipos de relaciones, un subconjunto de usuarios, etc.

Las redes sociales se han convertido en un concepto cada vez más popular con un número de diferentes instancias. Bien conocidos son los sitios de redes sociales como MySpace, Orkut, LinkedIn y Facebook. Estos servicios permiten a los usuarios publicar parte de su identidad personal en línea, incluyendo la relación con otros usuarios que, por lo general, también tienen una cuenta.

La red social de un usuario también se puede utilizar fuera del ámbito de un único servicio. Por ejemplo, Open-Social

Alliance permite esto en cierta medida. Define un conjunto de interfaces de programación de aplicaciones (API) que permiten a los desarrolladores acceder a las siguientes funciones básicas y la información en las redes sociales participativas: información de perfil (datos de usuario), información de amigos (gráfico social) y actividades (cosas que suceden, información tipo noticias). Las actividades de especificaciones y API de redes sociales participativas relacionadas son FaceBook API y OpenSocialWeb. Open-SocialWeb define las soluciones de interoperabilidad de redes social, por ejemplo, a través de formatos micro.

La información sobre redes sociales puede especificarse usando la especificación FOAF (amigo de un amigo). Las entradas FOAF se pueden utilizar en múltiples contextos, incluyendo los metadatos incorporados de las páginas web. De esta manera, la información puede estar disponible para, por ejemplo, aplicaciones y motores de búsqueda. Google Social Graph API es una aplicación experimental que hace uso de ello junto con otras fuentes para determinar y visualizar las relaciones sociales entre las personas.

A continuación seguirá ejemplos de cómo puede utilizarse este tipo de servicios de redes sociales en conexión con la autentificación biométrica.

La figura 1 ilustra esquemáticamente un sistema en el que se puede realizar un procedimiento como se ha resumido anteriormente. La figura 1 representa un sistema distribuido que comprende un dispositivo electrónico 102, por ejemplo un dispositivo electrónico de consumo, un dispositivo CE, tal como una consola de videojuegos o un televisor, que es capaz de interactuar con un usuario 101.

El dispositivo 102 puede tener diferentes tipos de usuarios. Uno o más usuarios principales asociados al dispositivo 102 suelen utilizar el dispositivo de forma más o menos regular. Con este fin, el dispositivo puede contener alguna información acerca de estos usuarios principales, por ejemplo, un identificador y características biométricas, que se pueden haber aprendido, por ejemplo, como parte de algún registro, inscripción o paso de autentificación anterior. Ejemplos de usuarios principales son el (los) propietario(s) del dispositivo, así como otros usuarios regulares, por ejemplo, miembros de la familia en la misma casa. En contraste con un usuario principal, un invitado es de otro tipo de usuarios que pueden hacer un uso menos habitual o esporádico del dispositivo 102. Normalmente, el dispositivo no tiene información sobre un usuario invitado que no ha encontrado antes.

La información se distribuye en varias partes: un proveedor de servicios 104, un servicio de redes sociales 106 y un proveedor de identidad 108, todos ellos realizados en la forma de uno o más servidores informáticos conectados con y configurados para comunicarse entre sí a través de una red de comunicación 110. Aunque la figura 1 ilustra un sistema distribuido, en una forma más básica, el proveedor de servicios 104 puede mantener la identidad y los datos de las redes sociales él mismo, lo cual comprende por lo tanto el servicio de red social 106 y el proveedor de identidad 108.

El proveedor de servicios 104 es la parte que proporciona uno o más servicios a los usuarios, por ejemplo, un sitio web de videos generados por los usuarios o un sitio para compartir fotos. El proveedor de servicios 104 mantiene una cuenta por usuario del servicio, con el perfil asociado en el que normalmente se almacenan aspectos específicos del usuario del servicio, por ejemplo, el contenido publicado. Esta cuenta está vinculada a la cuenta en el proveedor de identidad 108, que también es responsable de la autentificación del usuario.

El servicio de red social 106 mantiene, por usuario, la relación con otros usuarios. Opcionalmente, también se mantiene el tipo de relación en el servicio de red social 106, tal como las relaciones familiares "hermano", "hermana", "padre", "madre", etc, u otras relaciones tales como "colega", "compañero de trabajo ", "conocido", "amigo", etc. En base a esta información, el servicio de redes sociales 106 puede determinar un grupo de personas comprendidas en la red social de un usuario. El número de personas que puede determinarse es efectivo hasta un tamaño arbitrario, por ejemplo, el amigo de un amigo de un amigo hasta un cierto grado, etc., También es capaz de determinar si dos usuarios tienen una relación a través de relaciones mutuas o no, etc. .

Entre los ejemplos de servicios de redes sociales existentes, se incluyen "MySpace", "Facebook" y "LinkedIn". Sin embargo, también son posibles otras opciones. Por ejemplo, un servicio especializado que determina las relaciones de otras fuentes de información, como la información que se ha publicado en la web. Otro ejemplo puede ser que un portal de dispositivo construya su propia red social como cosa, por ejemplo, teniendo en cuenta los dispositivos específicos, por ejemplo, consolas de videojuegos, que son utilizados por múltiples usuarios, obteniendo esa información, y suponiendo una relación social basada en una relación de dispositivo compartido. Otro ejemplo está formado por los servicios de comunicaciones de mensajería instantánea que mantienen un contacto o una lista de "amigos" para los usuarios.

El proveedor de identidad 108 es la parte en el sistema 100 que mantiene la información de identidad de los usuarios, que puede incluir las credenciales de inicio de sesión y perfil biométrico. El proveedor de identidad 108 es responsable de autentificar a un usuario de tal modo que un proveedor de servicios, tal como el proveedor de servicios 104, puede ofrecer sus servicios en base a esa autentificación. El proveedor de identidad 108 puede ser un proveedor de identidad como se conoce en el campo de la gestión de identidades, por ejemplo, la arquitectura de

Liberty Alliance, OpenID, etc. Por supuesto, estos están en tal caso ampliados con la funcionalidad para soportar el procedimiento como se ha resumido anteriormente.

El dispositivo electrónico 102, por ejemplo un dispositivo de CE en la forma de una consola de videojuegos o televisor, está configurado de tal manera que es capaz de ocuparse de la autentificación biométrica de los usuarios. Para este fin, está equipado con sensores biométricos y lógica para interpretar y combinar mediciones biométricas. El dispositivo electrónico 102 puede mantener a nivel local, por ejemplo por medio de una memoria caché, la información sobre los usuarios, por ejemplo, los usuarios principales asociados u otros usuarios conocidos por el dispositivo. En esta memoria caché se puede almacenar información sobre el usuario que utiliza el dispositivo, una referencia a la identidad de los usuarios en el proveedor de identidad, y una copia del perfil biométrico del usuario.

La figura 2 ilustra esquemáticamente un dispositivo electrónico 202, tal como el dispositivo 102 en la figura 1. El dispositivo 202 puede ser un dispositivo CE, incluyendo dispositivos tales como una consola de videojuegos y un televisor. Una unidad de procesamiento 204 está conectada a una unidad de memoria 206 que ilustra el almacenamiento de datos, así como instrucciones de software que implementa el procedimiento resumido anteriormente. Los datos que se almacenan en la memoria 206 pueden incluir datos, por ejemplo en forma de uno o más perfiles biométricos de uno o más usuarios principales asociados con el dispositivo 102. La unidad de procesamiento 204 está conectada, a través de una unidad de interfaz de entrada / salida 208, a una pantalla 210, teclas de entrada de usuario 212, una unidad de salida de audio 214 y una unidad de detección biométrica 216. La información sobre cómo estas unidades funcionan y se comunican entre sí, incluyendo la unidad de detección biométrica 216, es conocida en la técnica y por lo tanto no se explica en detalle.

Volviendo ahora a la figura 3, se describirá un procedimiento de autentificación de un usuario que utilice un dispositivo electrónico en una red de comunicación para acceder a un servicio deseado por el usuario a un proveedor de servicios por medio de un diagrama de flujo. Se harán referencias a un dispositivo electrónico, un proveedor de servicios, un servicio de red social y un proveedor de identidad que corresponden a las entidades respectivas 102, 104, 106 y 108 descritos anteriormente en relación con las figuras 1 y 2.

En un paso de medición biométrica 301, el dispositivo electrónico 102 toma una medición biométrica del usuario. Esta medición puede ser cualquier característica biométrica conocida en la técnica, incluyendo la forma de la cara, la huella digital, el iris, la voz, etc.

En un paso de comprobación 303, el dispositivo 102 intenta comparar la medición biométrica con cualquier perfil biométrico almacenado en su memoria caché local, por ejemplo, perfiles de los usuarios principales asociados con el dispositivo 102. Si esto tiene éxito, entonces el usuario es autentificado y el procedimiento continúa con el paso de inicio de sesión 315.

Si en el paso de comprobación 303, se averigua que la medición biométrica no se corresponde con un perfil ya presente localmente en el dispositivo 102, el dispositivo envía una consulta al servicio de red social 106 para un grupo de personas en la red social de los usuarios principales asociados con el dispositivo 102. Un parámetro de la consulta es información que especifica los usuarios principales. La consulta también puede incluir uno o más parámetros de seguridad que pueden indicar un tamaño máximo deseado del grupo de personas, es decir, el número de usuarios para volver al dispositivo electrónico 102.

Los parámetros de seguridad pueden basarse en las políticas de seguridad definidas por el proveedor de servicios 104, en las características del dispositivo 102, y en la información que define una estrategia de inclusión. El proveedor de servicios 104 puede requerir un cierto nivel de seguridad, por ejemplo, un nivel que corresponde a la probabilidad de que se permita que un impostor tenga éxito en 1 de cada 100 intentos. El dispositivo 102 puede estar equipado con un sensor y un algoritmo biométrico, es decir, código de software ejecutado en una unidad de procesamiento, tal como la unidad de procesamiento 204 en la figura 2, que tiene una tasa de falsos negativos de 0,01 %. Esto implica que el dispositivo 102 por sus características puede realizar una comparación con una población de 100 usuarios y cumplir 104 requisitos del proveedor de servicios.

La estrategia de inclusión define qué usuarios incluir en esta población limitada. La figura 4 representa dicho proceso e ilustra una estrategia de inclusión que, por ejemplo, da preferencia a la familia distante respecto a los amigos de los compañeros de trabajo de un usuario. Es decir, en la figura 4 un usuario 401 se sitúa en el centro de subconjuntos de poblaciones de personas, ilustrados con los límites 420, 421, 422 y 423. El límite exterior 423 encierra una población completa de personas, por ejemplo, la población total del mundo, incluyendo a personas de ejemplo 406 y 407, y el límite intermedio 422 define la red social completa del usuario 401. El límite más interior 420 encierra un grupo de personas que están asociadas con el usuario 401 según una primera relación de grado. Por ejemplo, el grupo de personas dentro del límite más interior 420 comprende un padre 402 y un compañero de trabajo 403 del usuario 401. El límite de trazos 421 encierra una red social limitada del usuario 401, estando la limitación definida por uno o más parámetros de seguridad como el número máximo de personas y/o las relaciones con el usuario 401. Por ejemplo, un tío 404 puede incluirse en la red social limitada definida por el límite 421.

Continuando ahora con el diagrama de flujo de la figura 3, se consulta el servicio de red social, en un paso de consulta 305, para determinar una red social combinada basada en los uno o más usuarios principales y parámetros de seguridad.

La determinación de la red social para un único usuario principal sigue el contorno de los límites de la red social explicados anteriormente en relación con la figura 4. En caso de que el dispositivo 102 tenga múltiples usuarios principales, estos usuarios pueden considerarse en conjunto, se determinan sus límites de grados primero y superior combinados, y a continuación se aplica una estrategia de inclusión para limitar el número de personas a incluir en el grupo de personas de la red social.

A continuación, en un paso de recepción 307, el servicio de red social 106 proporciona el resultado de la determinación del grupo de personas de la red social limitada al dispositivo 102. Efectivamente, se proporciona una lista de identificadores de usuario y es recibida en el paso de recepción 307 por el dispositivo 102.

A continuación, el dispositivo 102 envía, en un paso de solicitud 309, una solicitud al proveedor de identidad 108 para proporcionar una lista de perfiles biométricos para el grupo de personas de la red social limitada identificada y proporcionada al dispositivo en el paso 307. La lista es recibida por el dispositivo 102 en un paso de recepción 311.

En un paso de comparación 313, el dispositivo 102 tiene tanto la medición biométrica que obtuvo en el paso 301, como la lista de identificadores de usuario obtenidos en el paso de recepción 307 y la lista de perfiles biométricos correspondientes a estas personas obtenidos en el paso de recepción 311. Se realiza una comparación de la medición biométrica obtenida en el paso 301 con los perfiles biométricos recibidos. En caso de fallo, la identificación biométrica falló y puede ofrecer al usuario una forma menos práctica para autentificar, por ejemplo, la entrada manual de un nombre de usuario / contraseña. En caso de una coincidencia, el dispositivo 102 selecciona el identificador de usuario apropiado y continúa con un paso de inicio de sesión del servicio 315.

En el paso de inicio de sesión de servicio 315, el dispositivo 102 se conecta al servicio del proveedor de servicios 104 para el usuario identificado. ¿Cómo funciona esto precisamente con la autentificación fuera del alcance de esta descripción?

El procedimiento descrito anteriormente autentifica a un usuario en un dispositivo electrónico. Aquí se aplica la autorización para permitir al usuario tener acceso a un servicio a un proveedor de servicios. Para este propósito, se obtienen perfiles biométricos y se mantienen en la memoria en el propio dispositivo (paso cf. 311), que en algunas situaciones y entornos pueden considerarse inseguras y un riesgo para la privacidad. Esto puede abordarse de dos maneras como se describe a continuación.

En lugar de realizarse en el propio dispositivo 102, la verificación biométrica, es decir, la comparación, puede llevarse a cabo en el proveedor de identidad 108. Esto obvia la necesidad de que el dispositivo electrónico 102 trate los perfiles biométricos reales, lo cual ofrece una mejor privacidad. Esta alternativa cambiaría el procedimiento que se lleva a cabo en los pasos 309-313 antes descritos por pasos que implicarían la transmisión de la medición biométrica del usuario al proveedor de identidad 108 junto con la información que especifica el grupo de personas de la red social limitada del usuario principal. A continuación, el proveedor de identidad 108 realiza la comparación de la medición biométrica con los perfiles biométricos de las personas en la red social limitada, y proporciona el resultado de la comparación, por ejemplo, en forma de un identificador de usuario, al dispositivo electrónico 102. Una variación adicional de esta alternativa sería que el proveedor de identidad 108 obtenga, por ejemplo, mediante la utilización de un servicio de redes sociales, la información que especifique el grupo de personas de la red social limitada, en base a la información recibida que especifica el usuario principal.

Además, el paso de devolver del identificador de usuario del proveedor de identidad una coincidencia puede mejorarse también devolviendo, al dispositivo electrónico, una aserción de autentificación (por ejemplo, por medio de Security Assertion Markup Language, SAML) que indica que el usuario se autentificó con éxito mediante biometría. A continuación, el dispositivo electrónico 102 puede utilizar esta afirmación y presentarla al servicio en el paso de inicio de sesión 315.

La protección de la plantilla es otra manera de obviar la necesidad de que el dispositivo electrónico 102 almacene perfiles biométricos, lo cual ofrece una mejor privacidad. En cambio, el dispositivo electrónico 102 puede almacenar los datos auxiliares biométricos y proteger las plantillas biométricas. Esto es ventajoso, ya que a partir de los datos auxiliares y las plantillas biométricas seguras no es posible reconstruir el perfil biométrico original. Esta alternativa sería cambiar el procedimiento que se lleva a cabo en los pasos 309-313 antes descritos por pasos que involucrarían, después de haber proporcionado la información que especifica el grupo de personas de la red social limitada del usuario, recibir del proveedor de identidad 108 datos auxiliares y proteger las plantillas biométricas correspondientes a las personas en la red social limitada. A continuación, el dispositivo electrónico 102 utilizaría esta información junto con la medición biométrica obtenida del usuario en un procedimiento de protección de la plantilla mediante el uso de todos los datos auxiliares disponibles y verificaría si el resultado coincide con la plantilla

biométrica segura correspondiente. En caso de éxito, se selecciona el identificador de usuario correspondiente y el proceso continúa en el paso de inicio de sesión 315.

Es de notar que el paso de aplicación del procedimiento de protección de plantilla tiene una complejidad de N, donde N representa el número de personas en la red social combinada limitada. Dado que el procedimiento de protección plantilla es relativamente ligero, se considera que es factible para pequeñas cantidades de N, por ejemplo, del orden de 100. El cálculo de las características de la medición biométrica del usuario es el paso que requiere más procesamiento y solo tiene que hacerse una vez.

Una forma alternativa de utilizar el procedimiento de protección de plantilla es tener el proveedor de identidad 108 para realizar la verificación. Esta alternativa cambiaría el procedimiento que se lleva a cabo en los pasos 309-313 antes descritos por pasos que involucrarían, después de haber proporcionado la información que especifica la red social limitada del usuario, la recepción de los datos auxiliares del proveedor de identidad 108. A continuación, los datos auxiliares se procesarían junto con la medición biométrica del usuario en un procedimiento de protección de plantilla que produce una plantilla respectiva para todas las personas en la red social limitada, que se proporcionan a continuación al proveedor de identidad 108. A continuación, estas plantillas se revisan para ver si coinciden o no con la plantilla biométrica segura correspondiente y, en caso de coincidencia, se selecciona el identificador de usuario apropiado y se proporciona al dispositivo electrónico 102. También en esta forma alternativa de utilización de plantillas, el proveedor de identidad 108 puede devolver una afirmación de autentificación (usando SAML) para su uso posterior.

Por lo tanto, para resumir brevemente, la autentificación de un usuario en un dispositivo electrónico en una red de comunicación se describe en el presente documento. El procedimiento comprende la obtención de una característica biométrica del usuario, la transmisión, a un servicio de red social, de la información que especifica al menos un usuario principal del dispositivo, recibiendo, desde el servicio de red social, la información que especifica un grupo de personas que tienen una relación social con al menos un usuario principal, obteniendo información que especifica un resultado de una operación de comparación biométrica con la característica biométrica de las características de los usuarios y biométricas de las personas en el grupo de personas especificado, con el resultado que indica si el usuario está autentificado en el dispositivo electrónico o no. Reduciendo el tamaño del espacio de búsqueda necesario durante una operación de comparación mediante la utilización de información referente a un grupo de personas en una red social, la tasa de falsa aceptación se reduce y con ello se facilita la autentificación biométrica de un usuario en un dispositivo electrónico, por ejemplo, para el acceso a la funcionalidad deseada del dispositivo o el acceso a un servicio deseado.

REIVINDICACIONES

1. Un procedimiento para autentificar a un usuario (101) en un dispositivo electrónico (102, 202) en una red de comunicación (110, 218), que comprende:

- la obtención de una característica biométrica del usuario,

- la transmisión, a un servicio de red social (106), de la información que especifica al menos un usuario principal del dispositivo,

- la recepción, desde el servicio de redes sociales, de información que especifica un grupo de personas (420, 421, 422) que tienen una relación social con al menos un usuario principal,

- la obtención de información que especifica un resultado de una operación de comparación biométrica con la característica biométrica del usuario y las características biométricas de personas en el grupo de personas especificado, con el resultado que indica si el usuario está autentificado en el dispositivo electrónico o no.

2. El procedimiento de la reivindicación 1, en el que

- la transmisión de información que especifica al menos un usuario principal del dispositivo comprende la transmisión de al menos un parámetro de limitación para limitar el número de personas en el grupo de personas especificado.

3. El procedimiento de la reivindicación 2, en el que la transmisión de al menos un parámetro de limitación comprende la transmisión de un número que especifica el número máximo de personas en el grupo de personas especificado.

4. El procedimiento de la reivindicación 2 o 3, en el que la transmisión de al menos un parámetro de limitación comprende la transmisión de información que especifica los tipos de relaciones entre al menos un usuario principal y personas en una red social del usuario.

5. El procedimiento de cualquiera de las reivindicaciones 2 a 4, en el que la transmisión de al menos un parámetro de limitación comprende la transmisión de información que especifica al menos un parámetro característico relacionado con las prestaciones del dispositivo en la obtención de la característica biométrica del usuario.

6. El procedimiento de la reivindicación 5, en el que la transmisión de información que especifica al menos un parámetro característico relacionado con las prestaciones del dispositivo en la obtención de la característica biométrica del usuario comprende la transmisión de información relacionada con una tasa de falsa aceptación o una tasa de falso rechazo.

7. El procedimiento de cualquiera de las reivindicaciones 1 a 6, que comprende;

- transmitir, a un proveedor de identidad (108), información del grupo especificado de personas,

- recibir, del proveedor de identidad, características biométricas de las personas en el grupo especificado de personas, y

- en el que la obtención de información que especifica un resultado de una operación de comparación biométrica comprende realizar la operación de comparación.

8. El procedimiento de la reivindicación 7, en el que

- la recepción, del proveedor de identidad, de características biométricas de personas en la red social comprende la recepción de plantillas biométricas seguras y datos auxiliares asociados con las plantillas biométricas seguras, y en el que

- la operación de comparación comprende utilizar las plantillas biométricas seguras y los datos auxiliares.

9. El procedimiento de cualquiera de las reivindicaciones 1 a 7, que comprende;

- transmitir, a un proveedor de identidad, la característica biométrica del usuario e información del grupo especificado de personas, y en el que la obtención de información que especifica un resultado de una operación de comparación biométrica comprende:

- recibir información, del proveedor de identidad, que especifica un resultado de una operación de comparación biométrica con la característica biométrica del usuario y las características biométricas de las personas en el grupo de personas especificado.

10. El procedimiento de la reivindicación 9, que comprende:

- recibir, del proveedor de identidad, los datos auxiliares relacionados con plantillas biométricas que están asociados con las personas en el grupo de personas especificado,

- generar plantillas biométricas utilizando los datos auxiliares y la característica biométrica del usuario, y

- transmitir las plantillas biométricas generadas al proveedor de identidad.

11. El procedimiento de cualquiera de las reivindicaciones 1 a 10, que comprende;

- determinar, en función de la información obtenida del resultado de la comparación biométrica, si el usuario está autentificado para acceder a un servicio deseado por el usuario (104).

12. Dispositivo electrónico (102, 202) que comprende medios de entrada biométricos (216), circuitería de procesamiento y comunicaciones (204, 206, 208) que están configurados para la autentificación de un usuario (101) en el dispositivo electrónico en una red de comunicación (110, 218), estando la circuitería configurada para:

- obtener una característica biométrica del usuario,

- transmitir, a un servicio de red social (106), información que especifique al menos un usuario principal del dispositivo,

- recibir, desde el servicio de redes sociales, información que especifique un grupo de personas (420, 421, 422) que tengan una relación social con al menos un usuario principal,

- obtener información que especifica un resultado de una operación de comparación biométrica con la característica biométrica del usuario y las características biométricas de personas en el grupo de personas especificado, con el resultado que indica si el usuario está autentificado en el dispositivo electrónico o no.

13. Un procedimiento para habilitar la autentificación de un usuario (101) en una red de comunicación (110, 218), que comprende:

- recibir información que especifique al menos un usuario principal,

- recibir una característica biométrica del usuario,

- obtener información que especifique un grupo de personas (420, 421, 422) que tengan una relación social con al menos un usuario principal,

- realizar una operación de comparación biométrica con la característica biométrica del usuario y las características biométricas de personas en el grupo de personas especificado, con el resultado que indica si el usuario está autentificado o no.

14. Aparato (104, 106, 108) que comprende circuitería de procesamiento y comunicaciones que está configurado para habilitar la autentificación de un usuario (101) en una red de comunicación (110, 218), estando el circuito configurado para:

- recibir información que especifique al menos un usuario principal,

- recibir una característica biométrica del usuario,

- obtener información que especifique un grupo de personas (420, 421, 422) que tengan una relación social con al menos un usuario principal,

- realizar una operación de comparación biométrica con la característica biométrica del usuario y las características biométricas de las personas en el grupo de personas especificado, con el resultado que indica si el usuario está autentificado.

15. Un producto de programa informático que comprende instrucciones de software que, cuando se ejecuta en una unidad de procesamiento, realiza el procedimiento de una cualquiera de las reivindicaciones 1 a -13.

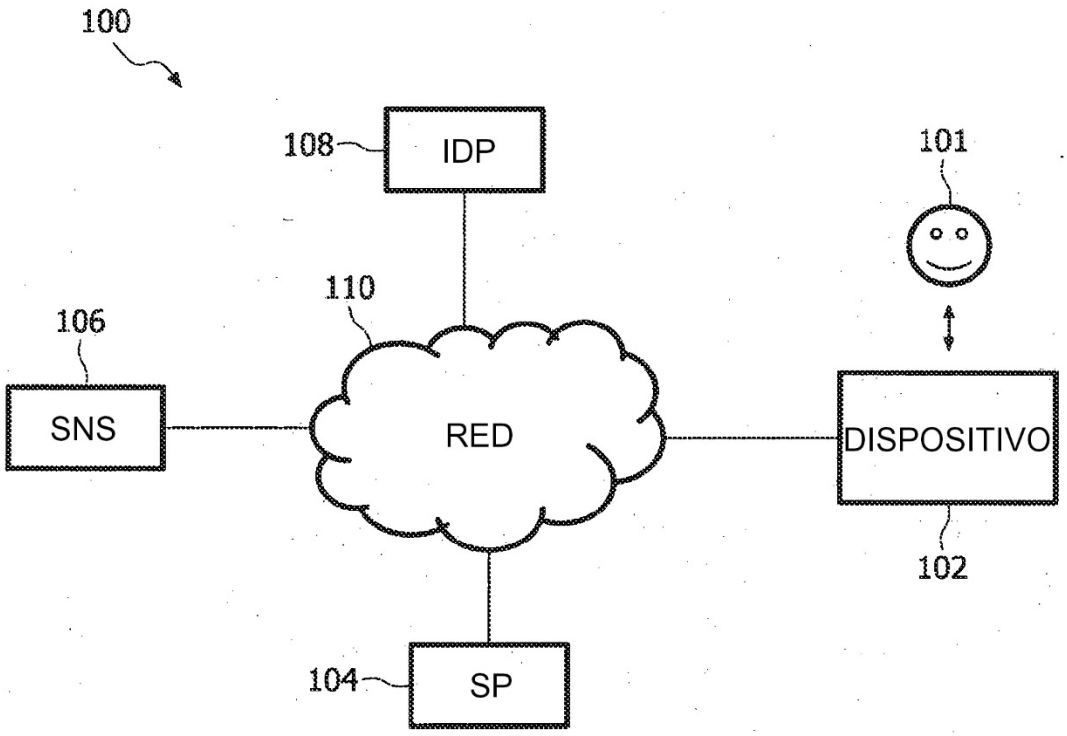
100
108
IDP
101
110
106
SNS
RED
DISPOSITIVO
102
104
SP

FIG. 1

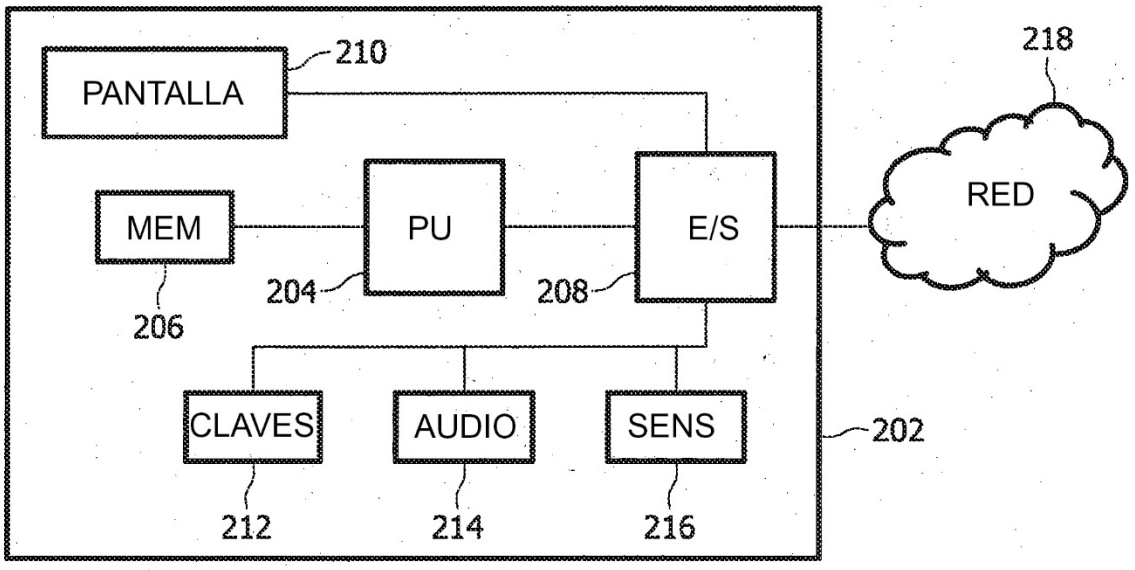
PANTALLA
210
218
MEM
PU
E/S
RED
204
208
206
CLAVES
AUDIO
SENS
202
212
214
216

FIG. 2

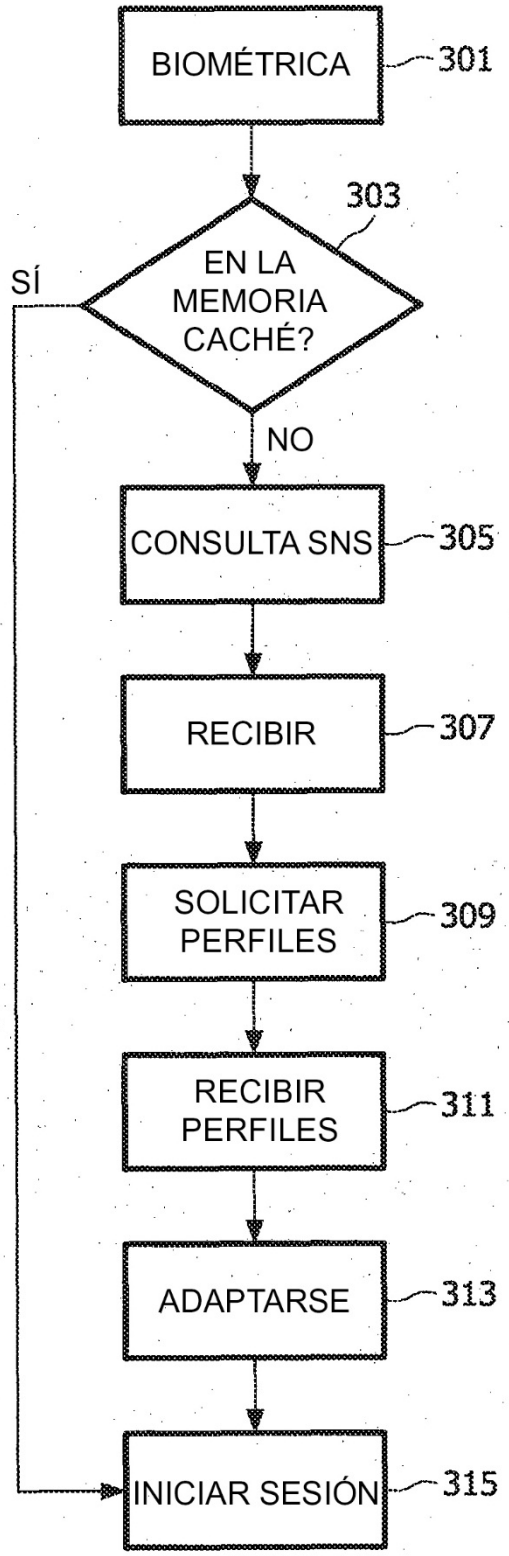
BIOMÉTRICA
301
303
EN LA MEMORIA CACHÉ?
SÍ
NO
CONSULTA SNS
305
RECIBIR
307
SOLICITAR PERFILES
309
RECIBIR PERFILES
311
ADAPTARSE
313
INICIAR SESIÓN
315

FIG. 3

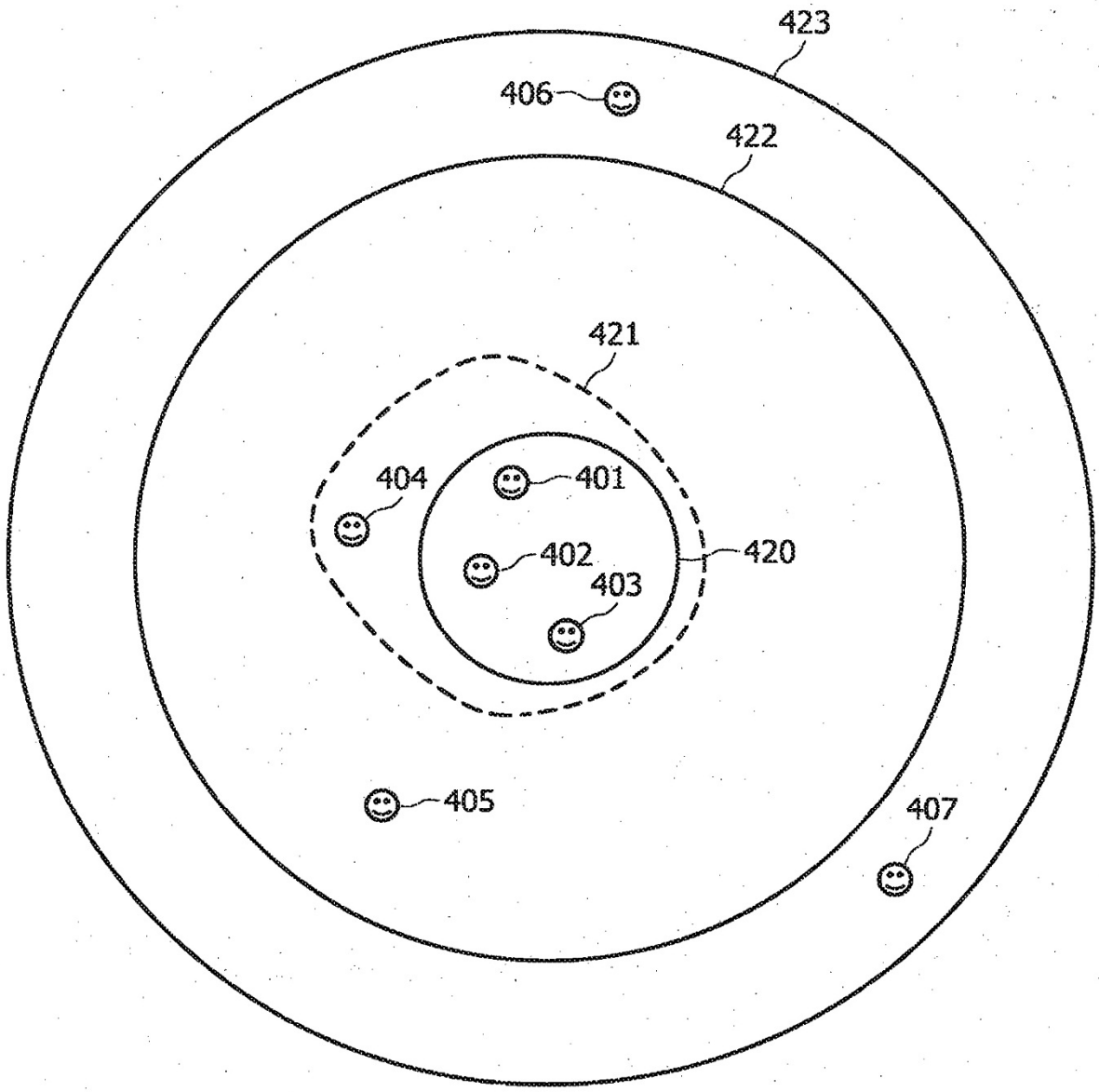

FIG. 4