

SISTEMA DE CONTACTO SEGURO PARA TELÉFONOS MÓVILES (SMCS)

PRIORIDAD

[0001] La presente solicitud reivindica prioridad de la nueva solicitud no provisional de EE.UU. No. 14/816,755, presentada el 3 de agosto de 2015, la cual reivindica el beneficio de la solicitud provisional de EE.UU. con No. de serie 62/033,052, presentada el 4 de agosto de 2014 y la solicitud provisional con No. de serie 62/157,516, presentada el 6 de mayo de 2015, cuyas descripciones se incorporan al presente documento para referencia.

ANTECEDENTES DE LA INVENCION

[0002] Las personas se preocupan cada vez más por su seguridad y su privacidad al utilizar redes digitales. La principal preocupación de los consumidores es el robo de identidad y transacciones fraudulentas relacionadas. En segundo lugar se encuentra la privacidad de datos personales. Las personas desean asegurarse de que su información personal esté segura. Ellos desean tener control sobre cómo se utilizan los datos personales y a quién se da a conocer. Dos de los tipos de información que la mayoría de personas desean proteger son sus números de teléfono móvil y de Seguridad Social.

[0003] No existe un sistema centralizado para hacer frente a estas necesidades y satisfacer el nivel elevado de seguridad que los consumidores, los reguladores y las empresas requieren. Tal como se ilustra en esta solicitud, la demanda de un sistema ubicuo para la verificación de identidad, la autenticación de transacciones, la protección de personas contra el robo de identidad y el mejoramiento de la privacidad del teléfono móvil, es un fenómeno generalizado. Los consumidores, los reguladores y las empresas se verán beneficiados de un servicio que cubra estas necesidades, tal como la presente invención.

RESUMEN DE LA INVENCION

[0004] En un aspecto de la invención, se describe un sistema para la autenticación de una identidad de un usuario. El sistema comprende un procesador y un medio de

almacenamiento no volátil que comprende instrucciones ejecutables por ordenador para instruir al procesador a: a) recibir un archivo de imagen relacionado con el usuario, desde un dispositivo de usuario de propiedad del usuario; b) determinar si el archivo de imagen coincide con la información de imagen almacenada en una base de datos, en donde la información de imagen almacenada no es un archivo de imagen y contiene información de identificación sobre la imagen; y c) si el archivo de imagen coincide con la información de imagen almacenada, permitirle al usuario i) solicitar el envío de un mensaje de autenticación al dispositivo de usuario, o ii) solicitar el envío de un mensaje a un tercero cuyo mensaje que abarca información es desconocido al usuario.

[0005] En un aspecto de la invención, el sistema comprende además la etapa de d) enviar el mensaje a un tercero desde el usuario autenticado. En un aspecto de la invención, el mensaje incluye un archivo de audio. En un aspecto de la invención, el archivo de audio es un mensaje grabado creado por el usuario. En un aspecto de la invención, el mensaje puede enviarse al tercero solo si existen datos relacionados con el tercero en la base de datos. En un aspecto de la invención, el mensaje incluye información de identificación para el usuario y en donde la información de identificación se añade al mensaje sin intervención del usuario en la creación del mensaje.

[0006] En un aspecto de la invención, el sistema de la reivindicación 2, que comprende además la etapa de enviar un mensaje Opt-in al tercero si el tercero no es un usuario registrado del sistema, antes de entregar el mensaje al tercero. En un aspecto de la invención, el tercero puede responder al mensaje sin revelar su información de contacto y en donde el tercero puede bloquear al usuario para que no pueda enviar mensajes futuros al tercero. En un aspecto de la invención, se almacena en una base de datos una preferencia del tercero en relación con la posibilidad de bloquear al usuario u otros usuarios para que no puedan enviar mensajes.

[0007] En un aspecto de la invención, si el archivo de imagen coincide con la información de imagen almacenada, se le permite al usuario enviar un mensaje a otro usuario a través de un alias. En un aspecto de la invención, el procesador determina si el archivo de imagen coincide con la información de imagen almacenada utilizando un algoritmo de coincidencia no minucioso. En un aspecto de la invención, el procesador puede determinar si el archivo de imagen coincide con la información de imagen

almacenada a pesar de que el archivo de imagen y la información de imagen almacenada fueron creados con factores ambientales diferentes.

[0008] Un aspecto de la invención comprende además instrucciones ejecutables por ordenador para instruir al procesador para obtener información relativa a una ubicación del dispositivo de usuario y las instrucciones ejecutables por ordenador para instruir al procesador para registrar un tiempo en el que se realiza una petición para autenticación. Un aspecto de la invención comprende además instrucciones ejecutables por ordenador para instruir al procesador para recibir información de destino para la entrega del mensaje de autenticación.

[0009] En un aspecto de la invención, se identifica una forma de ponerse en contacto con el tercero utilizando datos de más de una base de datos controlada por más de una entidad. Un aspecto de la invención comprende además instrucciones ejecutables por ordenador para instruir al procesador para recibir una petición de un tercero para autenticar al usuario e instruir al procesador para enviar una solicitud del archivo de imagen al usuario. En un aspecto de la invención, el sistema está en funcionamiento sin tener en cuenta el fabricante del dispositivo de usuario o el sistema operativo que se ejecuta en el dispositivo de usuario.

[0010] En un aspecto de la invención, se describe un método para el registro de un usuario para un sistema para la autenticación de la identidad del usuario. El método que comprende las etapas de: a) recibir, de parte de un dispositivo de usuario, información de identificación de sujeto relacionada con el usuario e información de identificación de dispositivo relacionada con el dispositivo de usuario; b) utilizar la información de identificación de sujeto para consultar información adicional relacionada con el usuario en una base de datos; c) crear una pregunta relacionada con la información adicional; d) transmitir la pregunta al dispositivo de usuario; e) recibir una respuesta del dispositivo de usuario; f) si la respuesta es correcta, solicitar una imagen de identificación del dispositivo de usuario; g) recibir la imagen de identificación, convertir la imagen de identificación a un formato de información de imagen almacenada en donde el formato de información de imagen almacenada no es un archivo de imagen y contiene información de identificación acerca de la imagen y almacenar datos correspondientes a la imagen de identificación en el formato de información de imagen almacenada; y h) almacenar la información de

identificación de sujeto y la información de identificación de dispositivo en asociación con los datos correspondientes a la imagen de identificación.

[0011] En un aspecto de la invención, la imagen de identificación es una imagen de seguridad biométrica. Un aspecto de la invención comprende además la etapa de i) solicitar información adicional a ser almacenada en la base de datos, en donde dicha información adicional solo puede liberarse después de que se transmita con éxito un mensaje de autenticación. En un aspecto de la invención, la información adicional se extrae de más de una base de datos controlada por más de una entidad.

[0012] En un aspecto de la invención, se describe un sistema para la autenticación de una identidad de un documento o asunto. El sistema comprende un procesador y un medio de almacenamiento no volátil que comprende instrucciones ejecutables por ordenador para instruir al procesador a: a) recibir un archivo de imagen del documento o asunto desde un dispositivo; b) determinar si el archivo de imagen coincide con la información de imagen almacenada en una base de datos, en donde la información de imagen almacenada no es un archivo de imagen; y c) si el archivo de imagen coincide con la información de imagen almacenada, enviar un mensaje de autenticación al dispositivo o al tercero.

BREVE DESCRIPCIÓN DE LOS DIBUJOS

[0013] La FIG. 1 es una vista de todo el sistema que incorpora la herramienta de red, así como los servicios de mensajería segura y de autenticación.

[0014] La FIG. 2 es una vista de un diagrama de flujo que explica el proceso de registro dentro de la herramienta de red.

[0015] La FIG. 3 es una vista de un diagrama de flujo que explica el proceso para el envío de un mensaje de confirmación de autenticación a la herramienta de red.

[0016] La FIG. 4 es una vista de un diagrama de flujo que explica el proceso para generar una solicitud de autenticación del usuario de la herramienta de red.

[0017] La FIG. 5 es una vista de un diagrama de flujo que explica el proceso para generar una solicitud de autenticación de un tercero.

[0018] La FIG. 6 es una vista de un diagrama de flujo que explica el proceso para enviar un mensaje seguro.

[0019] La FIG. 7 es una vista de un diagrama de flujo que explica el proceso Opt-In(optar por hacer parte)/Opt-Out(optar por no hacer parte).

[0020] La FIG. 8 es una vista de un diagrama de flujo que explica el proceso para responder al mensaje seguro.

DESCRIPCIÓN DETALLADA DE LOS DIBUJOS

[0021] La presente invención define un sistema y un método para la incorporación, la adición y la administración de grandes volúmenes de datos e imágenes de múltiples fuentes a través de una plataforma segura, centralizada y basada en la nube para el suministro de servicios de comunicación seguros, protegidos por privacidad y autenticados (el “Sistema de Contacto Seguro para Teléfonos Móviles” o “SMCS”).

[0022] Tal como fue diseñado, la presente invención permitirá: a) la verificación y el registro de la identidad del teléfono móvil del usuario; b) cinco factores de autenticación (dispositivo móvil, persona, tiempo, ubicación y objeto, por ejemplo, documento, tarjeta de crédito, pasaporte, permiso de conducir, moneda, etc.); c) mensajería segura entre un usuario de teléfono móvil registrado y cualquier otro usuario de teléfono móvil de una manera protegida por privacidad cuando la información de contacto no está disponible.

[0023] El SMCS será accesible para todos los usuarios de telefonía móvil en los Estados Unidos e internacionalmente. Su tecnología centralizada es respaldada mediante registros traslapados del perfil de usuario e incluye la autenticación basada en conocimiento (“KBA”) contemporánea, así como las capacidades de reconocimiento agnóstico de imagen.

[0024] El SMCS permite dos nuevos servicios para abordar la seguridad y privacidad de las personas, lo que les permite autenticarse para transacciones financieras, minoristas, gubernamentales, de salud y otras transacciones personales importantes. Este servicio también le permite a las personas autorizar y controlar expresamente el uso de su información de identificación personal (“PII”), incluyendo sus números de Seguridad Social, sobre una base de transacción por transacción.

[0025] El segundo servicio le permite a un individuo ser contactado a través de su teléfono móvil de una manera protegida y controlada por privacidad, por personas que no

conocen el número de teléfono móvil de la persona. El servicio protege la privacidad de los individuos que son contactados a través de una variedad de medios y no da a conocer su número de teléfono móvil a los terceros que les están contactando. Por otra parte, el servicio requiere que la parte que se pone en contacto revele su nombre y número de teléfono móvil al individuo que recibe el contacto.

[0026] Ambos servicios anteponen los intereses de privacidad y seguridad. Las personas pueden reafirmar el control sobre la divulgación y el uso de su información personal. Las personas conocen la identidad de cualquier persona que intenta ponerse en contacto con ellos.

[0027] En un aspecto, los servicios se proporcionan a través de un centro de intercambio de información con el apoyo de proveedores de servicios inalámbricos para facilitar servicios de comunicación autenticados y protegidos por privacidad.

[0028] La plataforma SMCS incorpora autenticación basada en conocimiento contemporánea, tecnología de reconocimiento agnóstico de imagen, datos de referencia de registros traslapados del perfil de usuario y mensajería protegida por privacidad.

[0029] Se puede acceder a la plataforma SMCS y a los servicios a través de una herramienta de red (tal como mensajería o correo de voz) que puede estar pre-instalada en los teléfonos o que puede descargarse. Ambos servicios pueden ser utilizados por cualquier persona con un dispositivo inalámbrico que tenga funcionalidad de cámara y acceso a datos (por ejemplo, Internet). La invención, en un aspecto, trabaja sin tener en cuenta la identidad del fabricante del equipo del usuario, del desarrollador del sistema operativo o del proveedor de servicios inalámbricos.

Autenticación

[0030] El estándar para la autenticación en los EE.UU. implica dos factores: un factor físico (por ejemplo, tarjeta de crédito) y un factor de conocimiento (por ejemplo, PIN). El SMCS expande el estándar a 5 factores: 1) reconocimiento biométrico de la persona; 2) identificación del teléfono o dispositivo inalámbrico mediante número de serie; 3) autenticación de un documento (si es parte de una transacción); 4) confirmación sistémica

de la hora a la que se hace una solicitud de autenticación; y 5) cálculo sistémico de la ubicación del solicitante a través de GPS.

[0031] La plataforma SMCS realiza autenticación en tres niveles. El primer nivel es pasivo. El sistema captura automáticamente el nombre y la identificación del dispositivo del usuario, ya que registra la hora y el lugar de la solicitud.

[0032] El segundo nivel es activo y requiere que se verifique la identidad del usuario a través de autenticación basada en conocimiento. El sistema genera una serie de preguntas (por ejemplo, 3-5 preguntas) que se relacionan específicamente con el historial personal del usuario o transacciones financieras pasadas, por ejemplo, “¿Alguna vez ha poseído uno de los carros que figuran en la lista anterior?” O “¿Alguna vez ha vivido en una de las direcciones anteriores?” O “¿En qué año fue emitido su número de Seguridad Social?”

[0033] El tercer nivel de autenticación utiliza tecnología de reconocimiento agnóstico de imagen. “Agnóstico de imagen” se refiere a la eficacia de igualdad de la tecnología con imágenes biométricas o no biométricas. Después de completar con éxito el proceso de autenticación basada en conocimiento, un usuario puede registrar una imagen de seguridad biométrica de su elección, combinando una imagen física única con un factor de conocimiento (solo el registrante tiene conocimiento de la imagen seleccionada).

[0034] La tecnología de reconocimiento permite que una imagen contemporánea de la imagen de seguridad se tome en condiciones de iluminación muy variables, por ejemplo, en un cuarto oscuro o bajo un sol radiante. Sólo una imagen contemporánea de la imagen biométrica real otorgará acceso al SMCS y permitirá autenticación. Tal como fue diseñado, el sistema no va a autenticar una imagen de una imagen.

[0035] En un aspecto, la tecnología de reconocimiento puede emplear algoritmos de coincidencia no minuciosos, basados en reconocimiento de patrones. Estos algoritmos utilizan una gran parte de la imagen como un todo para la verificación de usuario - es decir, mucha más información que cuando se trabaja con puntos individuales (minucioso) - lo que los hace muy precisos. Esto significa que sus tasas de error (especialmente la tasa de aceptación falsa, que es por mucho la más importante de las dos) son mucho menores que en otros sistemas.

[0036] La nueva tecnología de concordancia es inherentemente inmune a diversas distorsiones de imagen e imperfecciones. Este hecho hace posible el uso de sensores menos

costosos sin degradar el rendimiento. La tecnología permite incluso “coincidencia cruzada”, es decir, el emparejamiento de un patrón ingresado a través de un modelo de escáner frente a una base de datos que fue producida utilizando otro modelo.

[0037] Otra ventaja de la tecnología de reconocimiento agnóstico de imagen es su facilidad de uso. En contraste con algunos otros productos biométricos, en los que el procedimiento de inscripción de nuevos usuarios es muy tedioso, la tecnología de concordancia de la presente descripción, en un aspecto, no requiere nada de parte del usuario, más que presentar el patrón del usuario en una única instancia al procedimiento de inscripción. El sistema en sí toma la imagen y todo lo demás se realiza automáticamente. Todo el proceso toma, en comparación con protección por contraseña, menos de un segundo.

Mensajería protegida por privacidad

[0038] Para habilitar la mensajería segura y protegida por privacidad, la herramienta de red proporciona un sistema de respuesta interactiva para obtener criterios de consulta por parte del usuario y recurre a bases de datos referenciales de terceros centralizadas que contienen registros traslapados del perfil de usuario, además de datos de identificación del suscriptor de proveedores de telefonía móvil, para encontrar la persona que se busca. El uso de estas múltiples fuentes aumenta exponencialmente el porcentaje de coincidencias. Además, el sistema está diseñado para aprender de cada transacción, mejorando de esta manera su información subyacente para permitir con el tiempo mejores tasas de coincidencia. El recurso colectivo, junto con datos de operadores, permitirá la identificación adecuada de la gran mayoría de los usuarios móviles dentro de una región geográfica.

[0039] Una vez que un usuario ha sido autenticado y el individuo con el que busca ponerse en contacto ha sido encontrado por el sistema, puede enviarse un mensaje seguro y protegido por privacidad. El sistema interactivo automatizado del SMCS solicita al usuario que proporcione una breve descripción del mensaje que se enviará. El usuario tiene la opción de grabar un mensaje de voz (por ejemplo, un archivo .wav) que puede adjuntarse al mensaje generado por la plataforma SMCS que se envía.

[0040] El SMCS ofrece al usuario la oportunidad de revisar el mensaje e informa al usuario de cualquier tarifa que pueda llegar a cobrarse, antes de que el mensaje sea enviado. De aplicar, el usuario autorizará la transmisión del mensaje.

[0041] Si el destinatario no ha optado previamente por hacer parte del SMCS, lo que implica el consentimiento del destinatario para recibir mensajes seguros, el sistema le informa al destinatario con un mensaje Opt-In de notificación que una persona identificada específica está tratando de ponerse en contacto con él/ella por una razón genérica (por ejemplo, médica, personal, de negocios o de otro tipo). El destinatario podrá ver el nombre del remitente y una razón genérica para el contacto, pero no el mensaje completo. El destinatario también está provisto de todas las revelaciones e instrucciones necesarias sobre cómo optar por hacer parte del SMCS. El destinatario solo tendrá que optar por hacer parte del sistema una vez, siempre y cuando no haya optado por no hacer parte del sistema entre transacciones. Un consumidor puede optar por no hacer parte del sistema en cualquier momento.

[0042] Una vez que el destinatario ha optado por hacer parte del SMCS, el destinatario recibirá el mensaje con los detalles adicionales del usuario (es decir, nombre, número de teléfono móvil y mensaje). El destinatario tendrá la opción de volver a llamar o enviar un mensaje de respuesta al usuario con el número del destinatario bloqueado u oculto para proteger la privacidad de la información de contacto del destinatario. El SMCS también le proporciona al destinatario la posibilidad de bloquear todos los mensajes seguros futuros del usuario de contacto.

Desempeño del sistema

[0043] La plataforma SMCS está diseñada para fiabilidad, capacidad de respuesta, seguridad y escalabilidad. El centro de intercambio de información es tanto con base en la nube como con base a servidor para proporcionar redundancia. El tiempo de respuesta del reconocimiento de imagen es de 4 segundos o menor. El sistema se escalará a cualquier tipo de transacción simultánea que se requiera.

Arquitectura del sistema

[0044] Tal como se contempla, el sistema integra cuatro tecnologías (herramienta de red, recuperación de identificación básica, bases de datos referenciales externas y reconocimiento agnóstico de imagen) para llevar a cabo la autenticación de usuario (personas e instituciones) en tiempo real y la funcionalidad de mensajes seguros y protegidos por privacidad. La comunicación con el sistema puede hacerse a través de conexiones de internet, pero para mejorar la seguridad, puede utilizarse una red privada y segura.

[0045] La herramienta de red funciona como una aplicación móvil que el cliente habrá instalado en, o descargado en, su dispositivo inalámbrico. La herramienta de red es la interfaz entre el cliente y los otros componentes y servicios soportados del sistema.

[0046] El componente de recuperación de identificación básico proporciona capacidades de búsqueda utilizando nombre/apellido, dirección y otros datos estipulados. Estos elementos básicos se utilizan para buscar e identificar a un individuo y localizar el proveedor del número del teléfono móvil del individuo con el fin de enviar un mensaje seguro y protegido por privacidad.

[0047] La administración del componente de recuperación de identificación básico del sistema necesitará, como mínimo:

- El mantenimiento de una interfaz SMS entre el sistema y los proveedores de telefonía móvil, ya que los proveedores de telefonía móvil enviarán el texto real y protegido por privacidad a su cliente;
- El mantenimiento de la base de datos de preferencias del subscriptor, la cual realiza un seguimiento de personas/números móviles que optan por no tomar parte del servicio o que bloquean a otras personas para que no les puedan contactar;
- El mantenimiento de una API (interfaz de programación de aplicación) para la herramienta de red;
- El mantenimiento de una API para cada una de las bases de datos referenciales externas, así como los proveedores de telefonía móvil;
- El hosting del servidor/middleware que proporciona grabación de voz para mensajes de texto; y,

- El hosting del servidor/middleware que permite a un destinatario de texto recibir y responder mensajes de forma anónima.

[0048] Se puede acceder a la base de datos referencial externa mediante el sistema para proporcionar la autenticación necesaria y asegurar la funcionalidad de mensajería. La primera base de datos/bases de datos soporta el servicio de autenticación basada en conocimiento, el cual se utiliza durante el proceso de registro. El proveedor(es) de tal servicio mantendrá la API para la herramienta de red. La otra base de datos/bases de datos se utilizan para la función de búsqueda básica, antes mencionada, que se utiliza para identificar individuos y habilitar el servicio de mensajería segura contemplado.

[0049] Finalmente, el sistema también proporciona el reconocimiento agnóstico de imagen para facilitar la autenticación de usuario. La imagen designada (por ejemplo, la palma de la mano) se utiliza para el registro y el posterior acceso autenticado a la herramienta de red, descrita anteriormente. El proveedor de la tecnología de reconocimiento mantendrá una API para la herramienta de red.

[0050] Mediante el uso de API seguras, que están codificadas y encriptadas, los componentes del SMCS están vinculados entre sí a través de conexiones directas y privadas, mejorando de este modo la transmisión segura de datos.

Uso - Autenticación y verificación de identidad

[0051] Como se ha indicado, durante el proceso de registro del SMCS, un usuario de telefonía móvil se identifica definitivamente mediante el uso de los dos primeros niveles de autenticación. Se le solicita a la persona entonces que registre una “imagen de seguridad” biométrica con el fin de acceder al sistema en el futuro, que gestione preferencias de cuenta, que verifique identidad, que autentique transacciones, que envíe mensajes seguros, etc. La herramienta de red le permite al usuario emplear la cámara del dispositivo inalámbrico para grabar una serie de, por ejemplo, imágenes de la palma de cualquiera mano, que luego se convierte en la imagen de seguridad del usuario.

[0052] La próxima vez que el usuario desee acceder a los servicios del SMCS, todo lo que necesita es abrir la herramienta de red y, mediante el uso del dispositivo inalámbrico, tomar una imagen contemporánea de su palma para la verificación por parte del centro de

intercambio de información. El proceso es simple y, lo más importante, prácticamente instantáneo.

[0053] A partir de esto, un usuario puede autenticarse al teléfono o a un tercero, como una institución financiera o un comerciante. En la mayoría de los casos, el tercero establecerá un “puntero” (una palabra eufemística/combinación de números para sustituir un número de teléfono móvil). Por ejemplo, un comerciante puede instruir a un comprador de una compra grande a autenticarse a sí mismo mediante el envío de un mensaje a través del centro de intercambio de información del SMCS al “Comerciante 100”. El comprador pulsa el icono de autenticación en la herramienta SMCS y dice: “Enviar al comerciante 100”. "La transacción debería tener aproximadamente 4 segundos.

[0054] En otra iteración, el usuario puede optar por registrarse en el SMCS mediante la grabación de impresiones de voz como una herramienta de registro de copia de seguridad. La tecnología de reconocimiento de voz estará incorporada en la herramienta. Una vez registrado, el usuario puede tener acceso al sistema mediante comandos de voz que correspondan con las impresiones de voz pregrabadas almacenadas en el SMCS. El análisis empleado para el reconocimiento de voz dentro del SMCS es prácticamente idéntico al análisis hecho con la tecnología de reconocimiento agnóstico de imagen.

[0055] Se pueden verificar, registrar y proteger los números de Seguridad Social y otras PII a través de la plataforma del SMCS. Durante el proceso de registro, los individuos ingresarán sus datos personales (nombre y apellido, dirección, código postal y los últimos 4 dígitos de su número de Seguridad Social) en la herramienta en el dispositivo inalámbrico. Los individuos podrán solicitarle a las organizaciones que soliciten permiso para utilizar los números de Seguridad Social de los individuos u otras PII sobre una base de transacción por transacción a través del SMCS. Del mismo modo, las organizaciones podrán solicitarle a las personas que verifiquen sus números de Seguridad Social u otras PII sobre una base de transacción por transacción a través del SMCS para protegerse contra individuos que intentan cometer fraude usando números de Seguridad Social u otras PII robados. Por ejemplo, en lugar de solicitar un número de Seguridad Social u otra PII, el tercero puede simplemente solicitar al usuario que haga que el sistema de autenticación envíe un mensaje al tercero. Debido a que, en un aspecto de la invención, el mensaje por sí solo no contiene información de identificación sino simplemente el resultado de que el usuario ha

sido autenticado, no hay oportunidad para que un posible ladrón de identidad intercepte la información.

[0056] Además, los individuos podrán solicitar que las instituciones con las que desean tratar sean autenticadas. A través del SMCS, las instituciones y sus empleados o agentes pueden autenticarse sobre una base de transacción por transacción. Con el fin de autenticarse, se le solicitará a la institución que proporcione una información institucional de identificación única, tal como credenciales gubernamentales o un código de barras de matriz, durante el proceso de registro en el SMCS. La institución también puede optar por registrar algunos de sus empleados o agentes para que esos individuos sean autenticados por estar vinculados con la institución (por ejemplo, un técnico, un repartidor, etc.).

[0057] Una vez registrada una institución en la plataforma SMCS, un individuo puede solicitar a la institución que se autentifique antes de proceder con una transacción. Si se requiere autenticación institucional, la institución iniciará el proceso de autenticación de forma directa con el SMCS o por medio de la herramienta en el teléfono inteligente de un empleado. Una vez realizada la solicitud de autenticación, el SMCS buscará en su base de datos para determinar si la institución, y/o su empleado o agente en particular, está registrada en el SMCS y, de ser así, el SMCS enviará al individuo solicitante un mensaje de autenticación para confirmar la identidad de la institución específica y/o de su empleado o agente en particular. Cabe señalar que antes de que se realice la solicitud de autenticación, la institución y el individuo pueden ponerse de acuerdo sobre un puntero específico para el teléfono inteligente del individuo para el resultado de autenticación que se enviará.

[0058] Si la institución, y/o su empleado o agente en particular, no está registrada en el SMCS, el SMCS no puede verificar la identidad de la institución, y/o su empleado o agente en particular, y se lo hará saber al individuo solicitante. El individuo decidirá, entonces, si debe proceder con la transacción.

[0059] Por ejemplo, una institución puede enviar un empleado (por ejemplo, un técnico o un repartidor) a la casa de alguien. Antes de que el propietario de la casa permita que un empleado ingrese a la misma, el propietario puede solicitarle al empleado que se autentifique a sí mismo como un empleado actual de la institución con la que el propietario solicitó la visita. En ese momento, el empleado puede interactuar con el SMCS a través de la herramienta en su teléfono inteligente. Al igual que cualquier persona que se autentifica a

sí misma, el empleado puede tomar una foto de su imagen de seguridad (por ejemplo, la palma de cualquier mano), ingresar en el teléfono inteligente un código institucional específico (o escanear un código de barras institucional contenido en, por ejemplo, su ID de empleado (la herramienta tiene la capacidad tecnológica incorporada de escanear y leer el código de barras que se presenta)) y enviar la solicitud al SMCS. El SMCS realizará una búsqueda para verificar a ese empleado en particular y, mediante la utilización del código institucional específico, verificará que ese empleado se encuentre registrado como empleado actual de la institución. Una vez verificado, el SMCS enviará un texto de autenticación al propietario de la casa verificando que el empleado se encuentra vinculado con la institución específica, con la que el propietario se ha comprometido.

[0060] En un aspecto, la presente invención puede utilizarse como un servicio para verificar identidad y autenticar documentos o transacciones. Cada año miles de millones de transacciones requieren de identificación, por ejemplo, viajes de avión de pasajeros en los EE.UU. (que se aproximan a los mil millones por año), bancarias, acceso a edificios, compra de alcohol, programas federales de asistencia social, compra de armas de fuego, accidentes o violaciones de tráfico, votación, uso de servicios por suscripción, tales como Netflix desde una ubicación o dispositivo diferente, etc. Los usuarios finales pueden solicitarle a terceros la verificación de identidad mediante la solicitud de un texto a través de la Plataforma SMCS. Esto proporciona una nueva y significativa protección contra el fraude y el abuso y mayor seguridad durante llamadas de servicio al hogar o tranquilidad en situaciones de citas en línea.

[0061] La tecnología de reconocimiento centralizado también puede ser un recurso muy valioso en las circunstancias desafortunadas de un niño desaparecido, un paciente de Alzheimer o un animal doméstico perdido. Estas necesidades fundamentales pueden satisfacerse, inicialmente, de forma gratuita e impulsar la conciencia omnipresente y el uso. La tecnología de reconocimiento de la plataforma es tan eficaz con imágenes fijas ya que analiza secuencias de vídeo. Por ejemplo, un niño perdido cuya imagen se ha almacenado en la Plataforma SMCS podría encontrarse si los organismos que cumplen la ley proporcionan al público secuencias de video, etc.

[0062] Un usuario podría optar por almacenar documentos digitalizados importantes, tales como una licencia de conducción, un pasaporte, una tarjeta de Seguridad Social, un

acta de nacimiento, una tarjeta de salud o un registro/seguro de un automóvil, etc., en la Plataforma SMCS y tener estos documentos accesibles en demanda (on demand) en una forma autenticada y digitalizada. En lugar de simplemente almacenar una imagen, el tercero que examina el documento sabe por el proceso de autenticación (Nivel 3 - reconocimiento de imagen) que el documento cargado es auténtico.

[0063] Los comerciantes en línea podrían solicitar una tarjeta de crédito/débito para confirmar una transacción a través de un mensaje de SMCS, lo que elimina la posibilidad de fraude. Los titulares de tarjetas de débito podrían establecer límites diarios sobre las transacciones de manera que solo podría excederse a esa cantidad cuando sea autorizado entonces a través de la Plataforma, por ejemplo, para menores de edad u otras personas dependientes. Los números de Seguridad Social pueden “protegerse” en el caso en el que sólo se pueden utilizar en una transacción si son dados a conocer por el propietario a través de la Plataforma SMCS. Esto eliminaría el robo de identidad. La Plataforma SMCS eliminaría la necesidad de transmitir de hecho detalles de identificación a terceros, que a su vez reduciría las posibilidades de fraude. Por ejemplo, en lugar de solicitar un número de Seguridad Social, el tercero puede simplemente solicitar al usuario que haga que el sistema de autenticación envíe un mensaje al tercero. Debido a que, en un aspecto de la invención, el mensaje por sí solo no contiene información de identificación sino simplemente el resultado de que el usuario ha sido autenticado, no hay oportunidad para que un posible ladrón de identidad intercepte la información.

[0064] Todas las variaciones de fraude y abuso pueden controlarse - bonos alimenticios, votación, control de armas, robo de software de servicios, fraude fiscal, transacciones de valores, etc. La Plataforma SMCS podría deshacer la economía clandestina y convertirse en una nueva arma en la guerra contra el terrorismo con monedas y pasaportes protegidos por imagen.

[0065] Un servicio de autenticación instantáneo, fácil de utilizar, ubicuo y no gubernamental que sobresaldrá en muchos aspectos imprevistos al igual que otras tecnologías masivas en el pasado. Las personas versadas en la materia se darán cuenta de que la presente invención puede adaptarse a casos de uso, aparte de los ilustrados en el presente documento.

[0066] Haciendo referencia ahora a la FIG. 1, donde números similares se refieren a elementos similares, el SMCS incluye una plataforma basada en la nube, centralizada y segura (10). En el primer caso, el usuario se registrará en el SMCS. A la plataforma SMCS se puede acceder a través de una herramienta de red, la cual se encuentra pre-instalada o puede descargarse en el dispositivo inalámbrico del usuario (20). En un aspecto, la funcionalidad subyacente de la herramienta se base en la red en lugar de basarse en el teléfono, al igual que el teclado de marcación, correo de voz o mensajes de texto. Sin embargo, las personas versadas en la materia se darán cuenta de que el software de la herramienta puede almacenarse ya sea en el teléfono o en un servidor de red remota, o cualquier combinación de los mismos.

[0067] Con el fin de iniciar el proceso de registro, el usuario accederá al SMCS a través de la Herramienta de Red en su dispositivo inalámbrico (20). El usuario introducirá su información personal (por ejemplo, nombre y apellido, dirección, código postal, dirección de correo electrónico y los últimos 4 dígitos de su número de Seguridad Social) en la herramienta de red (20). En un aspecto de la invención, la Herramienta de Red (20) es una aplicación de software para el dispositivo inalámbrico.

[0068] La Herramienta de Red (20), a través de una interfaz de programación de aplicación (“API”) específica, transmite esta información personal al Servidor de Aplicaciones de la Herramienta de Red (25). El Servidor de Aplicaciones de la Herramienta de Red (25) almacena los datos introducidos en el Servidor de Archivos de la Herramienta de Red (30) en la plataforma SMCS (10) y transforma la información personal introducida a un formato reconocible para el software y los servidores del Dynamic KBA Partner (35), que se mantiene fuera de la Plataforma SMCS (10), para su revisión. El Servidor de Aplicaciones de la Herramienta de Red (25) transmite la información personal reformateada a través de otra API específica al software y a los servidores del Dynamic KBA Partner (35). Con esa información recibida, el software y los servidores del Dynamic KBA Partner (35) consultan la información disponible al público contenida en su base de datos y obtienen datos específicos establecidos para el usuario que se registra. Con base en la serie de una categoría predeterminada de preguntas establecidas por el SMCS, el Dynamic KBA Partner (35), utilizando su software y servidores, consulta la información disponible al público en su base de datos para obtener respuestas a las preguntas

predeterminadas. Cuando se reciben las preguntas y respuestas, el servidor del Dynamic KBA Partner (35) transmite las preguntas, a través de la API específica, al Servidor de Aplicaciones de la Herramienta de Red (25). El Servidor de Aplicaciones de la Herramienta de Red (25) cambia el formato de los datos y transmite las preguntas a la Herramienta de Red (20).

[0069] Entonces, se le proporciona al usuario una serie de preguntas de elección múltiple (por ejemplo, 3-5) para establecer la posterior autenticación de usuario. Las personas versadas en la materia se darán cuenta de que pueden utilizarse menos o más preguntas. El usuario proporcionará respuestas a las preguntas y enviará las respuestas a través de la Herramienta de Red (20) al Servidor de Aplicaciones de la Herramienta de Red (25). El usuario le indica a la Herramienta de Red (20) que transmita las respuestas introducidas a las preguntas a la Plataforma SMCS (10) pulsando un icono en el dispositivo inalámbrico. Las personas versadas en la materia podrán apreciar que en el dispositivo inalámbrico pueden haber características que pueden utilizarse para dirigir el envío de información desde la Herramienta de Red (20) a la Plataforma SMCS (10). Dentro de la Plataforma SMCS (10), el Servidor de Aplicaciones de la Herramienta de Red (25) recibe la información de la Herramienta de Red (20), transforma los datos introducidos en un formato reconocible por el software y los servidores del Dynamic KBA Partner (35) y transmite dichos datos al software y a los servidores del Dynamic KBA Partner (35). El Dynamic KBA Partner compara las respuestas introducidas con las respuestas almacenadas que fueron previamente determinadas y almacenadas por el Dynamic KBA Partner para establecer si las respuestas del usuario coinciden con los resultados almacenados. Cuando se produce una coincidencia, el resultado de coincidencia positivo de autenticación se transmite de nuevo al Servidor de Aplicaciones de la Herramienta de Red (25), donde se genera un mensaje de autenticación positiva al usuario de la Herramienta de Red (20). El resultado de coincidencia positivo KBA se almacena en el Servidor de Archivos de la Herramienta de Red (30) para futuras referencias. Si no hay ninguna coincidencia, el Dynamic KBA Partner generará entonces otra serie de preguntas y respuestas predeterminadas y el proceso comenzará de nuevo.

[0070] Una vez autenticado a través del proceso de KBA, se le solicitará al usuario entonces que registre una imagen de seguridad biométrica (por ejemplo, 4-5 imágenes de la

mano del usuario) para la autenticación posterior y adicional del usuario. El usuario entonces transmitirá esas imágenes a través de la Herramienta de Red (20) al Centro de Aplicaciones de la Herramienta de Red (25) para almacenamiento y referencia dentro del Servidor de Archivos del Reconocimiento de Imágenes (40).

[0071] Los servidores pueden ser, en un aspecto, ordenadores de propósito general equipados con fuentes de alimentación redundantes y capacidades de almacenamiento en disco y están conectados a internet.

[0072] Una vez registrado, el usuario puede iniciar una transacción utilizando la Herramienta de Red en el dispositivo inalámbrico del usuario (20). El usuario se conectará mediante la presentación de una imagen que sea la misma imagen que se almacena en el Servidor de Archivos del Reconocimiento de Imágenes (40) dentro de la Plataforma SMCS (10). El usuario se autenticará haciendo coincidir la imagen presentada con la imagen de seguridad almacenada del usuario.

[0073] Una vez autenticado, la Herramienta de Red (20) le preguntará al usuario si le gustaría proteger su PII. Por ejemplo, las tarjetas de crédito/débito del usuario (es decir, conservar los números o imágenes reales de las tarjetas), el número de Seguridad Social (o los últimos 4 dígitos del número), los miembros de la familia (es decir, imágenes biométricas de familiares o mascotas que se hayan perdido - pacientes con Alzheimer o niños) u otros documentos importantes, tales como licencia de conducir o pasaporte. Si el usuario elige proteger cualquier PII, la Herramienta de Red (20) le pedirá al usuario que introduzca por tanto los datos específicos. Una vez completado, o si el usuario ha decidido no ingresar PII en el momento, la Herramienta de Red (20) le preguntará al usuario si desea autenticarse a su dispositivo inalámbrico o a un tercero, o enviar un mensaje seguro.

[0074] Si el usuario desea enviar un mensaje de autenticación a su dispositivo inalámbrico (20) o a un tercero (60), el usuario dará instrucciones a la Plataforma SMCS (10) a través de la Herramienta de Red (20) para que envíe un mensaje de autenticación a su dispositivo inalámbrico (20) o a un tercero designado (60).

[0075] Si el usuario desea enviar un mensaje seguro, el usuario entonces deberá diligenciar la información solicitada (por ejemplo, nombre y dirección, incluyendo ciudad y nombre del estado y edad). Una vez realizado, el usuario transmitirá la información a través de la Herramienta de Red (20) a la Plataforma SMCS (10). El Servidor de Aplicaciones de

la Herramienta de Red (25) dentro de la Plataforma SMCS (10) recibe la solicitud transmitida y retransmite además la solicitud al Servidor de Aplicaciones del Mensaje Seguro (45). El Servidor de Aplicaciones del Mensaje Seguro (45) luego busca una coincidencia en su base de datos. El Servidor de Aplicaciones del Mensaje Seguro (45) se actualiza continuamente, preferiblemente sobre una base diaria, con alimentación de datos desde la base de datos del SMCS (50), que contiene los perfiles de usuarios móviles obtenidos a través de fuentes disponibles públicamente, y las bases de datos de proveedores de telecomunicaciones (55), que contienen información de la cuenta del usuario de telefonía móvil. El Servidor de Aplicaciones del Mensaje Seguro (45) transmite los resultados de coincidencia al Servidor de Aplicaciones de la Herramienta de Red (25) que, a su vez, transmite los resultados de coincidencia a la Herramienta de Red en el dispositivo inalámbrico del usuario (20). Con base en los datos contenidos en el Servidor de Archivos de la Herramienta de Red (30), el SMCS podrá proporcionarle al usuario información de identificación adicional, tal como alias, direcciones anteriores y otras personas relacionadas con la Parte que se Busca, pero ningún número de teléfono móvil. El usuario elegirá entonces de los resultados de coincidencia a la persona con la que desea contactar y confirmará que un Mensaje Seguro debe enviarse a ese usuario de telefonía móvil. La transmisión de la solicitud de Mensaje Seguro va desde la Herramienta de red en el dispositivo inalámbrico del usuario (20) al Servidor de Aplicaciones de la Herramienta de Red (25) que, a su vez, retransmite la orden al Servidor de Aplicaciones del Mensaje Seguro (45). El Servidor de Aplicaciones del Mensaje Seguro (45) busca en su base de datos para determinar el proveedor de telecomunicaciones del usuario final y le envía a ese proveedor la instrucción para enviar el Mensaje Seguro a la Parte Receptora (60). Una vez recibida la instrucción del Mensaje Seguro, el proveedor receptor envía el Mensaje Seguro a la Parte Receptora (60). En otro aspecto de la invención, el Servidor de Aplicaciones del Mensaje Seguro (45) envía el Mensaje Seguro directamente a la Parte Receptora (60).

[0076] Con el fin de que la Parte Receptora (60) reciba el Mensaje Seguro, esta tuvo que haber optado por hacer parte del SMCS, lo que significa que dio su consentimiento para recibir mensajes seguros. Si la Parte Receptora (60) no ha optado por hacer parte del SMCS, la Parte Receptora (60) recibirá un mensaje Opt-In notificándole que alguien (por ejemplo, una persona identificada) está intentando contactarle. Una vez que la Parte

Receptora (60) opta por hacer parte del servicio SMCS, recibe el Mensaje Seguro con datos de usuario adicionales (por ejemplo, nombre, número entrante del teléfono móvil y/o un mensaje de correo de voz del usuario). La Parte Receptora (60) tendrá la opción de volver a llamar o enviar un mensaje de respuesta al usuario con el número de la Parte Receptora bloqueado u oculto para proteger la privacidad de la información de contacto de la Parte Receptora. La Parte Receptora (60) también contará con la opción de bloquear todos los mensajes seguros futuros del usuario de contacto.

[0077] En un aspecto de la invención, se almacenará el estado Opt-In y las preferencias del consumidor (por ejemplo, la instrucción del individuo de bloquear a cualquier usuario específico que quiera enviarle un Mensaje Seguro SMCS) en una base de datos específica contenida en el Servidor de Aplicaciones del Mensaje Seguro (45).

[0078] La FIG. 2 muestra una desglose del proceso de registro dentro de la Herramienta de red. El Usuario de la Herramienta de Teléfono Móvil es un usuario primerizo (100). El Usuario de la Herramienta de Teléfono Móvil introduce la información de registro adecuada, que consiste en su nombre y apellido, dirección, correo electrónico y los 4 últimos dígitos del número de Seguridad Social y, una vez completada, el usuario presiona el botón de continuar (101). El Servidor de Aplicaciones de la Herramienta de Red solicita datos de autenticación del KBA Partner después de que el usuario completa su entrada inicial de datos (102).

[0079] El KBA Partner genera preguntas de selección múltiple (por ejemplo, 3-5) para el Usuario de la Herramienta de Teléfono Móvil (103). Las preguntas de KBA se presentan al Usuario de la Herramienta de Teléfono Móvil a través del Servidor de Aplicaciones de la Herramienta de Red (104). El Usuario de la Herramienta de Teléfono Móvil responde a las preguntas de KBA (105). Las respuestas de KBA se transmiten desde el Servidor de Aplicaciones de la Herramienta de Red al KBA Partner (106). Las respuestas de KBA reciben una calificación y la calificación se envía desde el KBA Partner al Servidor de Aplicaciones de la Herramienta de Red (107).

[0080] ¿Las respuestas de KBA eran las correctas? Sí = 108 - No = 110. Si no son correctas, el Usuario de la Herramienta de Teléfono Móvil tiene un segundo intento. Las directivas empresariales dictarán lo que sucederá en el caso en el que falle el segundo intento. Cuando las respuestas son correctas, el Usuario de la Herramienta de Teléfono

Móvil avanzará al siguiente paso en el proceso de registro, tomando fotos (por ejemplo, 3-5) de la imagen de seguridad designada (por ejemplo, la palma de la mano) (109). Las directivas empresariales del sistema de producción se llevarán a cabo si las respuestas de KBA (nivel 2 de autenticación) no fueron correctas después de 2 intentos (110). La Plataforma SMCS almacenará las imágenes biométricas e información de registro (111).

[0081] La FIG. 3 muestra el proceso para el envío de un mensaje de confirmación de autenticación a la Herramienta de Red en el dispositivo inalámbrico. El Usuario de la Herramienta de Teléfono Móvil inicia una solicitud para autenticar su dispositivo inalámbrico (200). El Usuario de la Herramienta de Teléfono Móvil toma su imagen biométrica (si es necesario debido al tiempo de espera) y la envía (201). El Servidor de Aplicaciones de la Herramienta de Red recibe la imagen biométrica transmitida (202).

[0082] ¿Se autenticó la imagen (203)? Sí = 204 - No = 20 y se le solicita al Usuario de la Herramienta de Teléfono Móvil volver a enviar la imagen. Si la coincidencia de la segunda imagen falla, se aplican las directivas empresariales.

[0083] El Usuario de la Herramienta de Teléfono Móvil es notificado de una autenticación exitosa a través del dispositivo inalámbrico, mostrando el nombre del usuario, su dirección, la hora y el lugar de solicitud de autenticación (204).

[0084] La FIG. 4 muestra el proceso para generar una solicitud de autenticación del usuario de la herramienta de red. El Usuario de la Herramienta de Teléfono Móvil inicia una solicitud para autenticar a un tercero (300). El Usuario de la Herramienta de Teléfono Móvil toma su imagen biométrica (si es necesario debido al tiempo de espera) y la envía (301). El Servidor de Aplicaciones de la Herramienta de Red recibe la imagen biométrica transmitida (302).

[0085] ¿Se autenticó la imagen (303)? Sí = 304 - No = 301 y se le solicita al Usuario de la Herramienta de Teléfono Móvil volver a enviar la imagen. Si la coincidencia de la segunda imagen falla, se aplican las directivas empresariales. Se le solicita al Usuario de la Herramienta de Teléfono Móvil que ingrese el código de autenticación del tercero (por ejemplo, un código de 4 dígitos) y lo envíe (304). El Servidor de Aplicaciones de la Herramienta de Red recibe el código de autenticación (305). Se recibe y procesa el código de autenticación y se envía un mensaje de confirmación al Usuario de la Herramienta de Teléfono Móvil (306).

[0086] La FIG. 5 muestra el proceso para la generación de una solicitud de autenticación de un tercero. Un tercero inicia una solicitud de autenticación a un Usuario de la Herramienta de Teléfono Móvil (300a). El Servidor de Aplicaciones de la Herramienta de Red recibe la solicitud de autenticación (301a) y envía la solicitud al Usuario de la Herramienta de Teléfono Móvil. El dispositivo inalámbrico del Usuario de la Herramienta de Teléfono Móvil recibe la solicitud para autenticar, reactiva la aplicación y despliega la pantalla “autenticar a un tercero” con la dirección del puntero del tercero. Si el dispositivo inalámbrico no puede reactivarse, se recibe entonces una notificación de inserción en su lugar (302a).

[0087] El Usuario de la Herramienta de Teléfono Móvil vuelve a tomar su imagen biométrica (si es necesario debido al tiempo de espera) y la envía (201). El Servidor de Aplicaciones de la Herramienta de Red recibe la imagen biométrica y la dirección del puntero del tercero y pasa información a la Plataforma SMCS (304a).

[0088] ¿La imagen se encuentra autenticada (305a)? Sí = 306 - No = 303a y y se le solicita al Usuario de la Herramienta de Teléfono Móvil volver a enviar la imagen. Si la coincidencia de la segunda imagen falla, se aplican las directivas empresariales. El código de autenticación se recibe y se procesa (306a). Se le notifica al Servidor de Aplicaciones de la Herramienta de Red que el mensaje de autenticación fue enviado al tercero y se lo notifica al Usuario de la Herramienta de Teléfono Móvil (307a). Se le notifica al Usuario de la Herramienta de Teléfono Móvil que su mensaje de autenticación fue enviado (308a).

[0089] La FIG. 6 muestra el proceso de envío del Mensaje Seguro. El Usuario de la Herramienta de Teléfono Móvil selecciona la opción “Enviar un Mensaje Seguro” desde la pantalla de inicio y se presenta con una pantalla de búsqueda. El Usuario de la Herramienta de Teléfono Móvil ingresa su búsqueda para localizar a la Parte que se Busca. Ejemplos de los campos necesarios para la consulta son el nombre y el estado; campos opcionales son la ciudad y el rango de edad (400). El Servidor de Aplicaciones de la Herramienta de Red analizará la solicitud de búsqueda y buscará la plataforma (401). La plataforma realiza una búsqueda de su base de datos nacional (402). Si la consulta presenta varias coincidencias, lo que requiere una descripción más detallada, un botón de ‘filtrar’ permitirá que se ingresen otros datos adecuados para mejorar la búsqueda. El Usuario de la Herramienta de Teléfono Móvil introducirá mayores índices y pulsará el icono de búsqueda (403). Una vez se ubica

el registro apropiado, el Usuario de la Herramienta de Teléfono Móvil seleccionará el listado y pulsará el icono de “Continuar” (404).

[0090] El Usuario de la Herramienta de Teléfono Móvil se presenta con un pantalla que le permitirá al Usuario de la Herramienta de Teléfono Móvil escribir o grabar un mensaje (405). El Usuario de la Herramienta de Teléfono Móvil grabará o escribirá el mensaje que se entregará y presionará el icono de enviar (406). El Servidor de Aplicaciones de la Herramienta de Red pasa el mensaje al servidor de la Plataforma SMCS para su procesamiento (407). La Plataforma SMCS envía un mensaje de texto Premium al Usuario de la Herramienta de Teléfono Móvil y espera respuesta de aprobación (408). ¿El Usuario de la Herramienta de Teléfono Móvil aceptó el recargo del texto Premium (409)? Sí = 411 - No = 410. Si el Usuario de la Herramienta de Teléfono Móvil no acepta el cobro del texto Premium, se determinará la solicitud (410).

[0091] Una vez que la Plataforma SMCS recibe la aprobación del cargo del texto Premium, se crea un mensaje Opt-In y se envía a la Parte que se Busca (411). Una vez que la plataforma SMCS recibe la aprobación del cargo del texto Premium, la Plataforma SMCS enviará un mensaje de confirmación al Usuario de la Herramienta de Teléfono Móvil (412). ¿La Parte que se Busca seleccionó la opción Opt-In (413)? Sí = 414 - No = 416. Si se acepta la Opt-In, véase FIG. 8 (414). El mensaje de confirmación se entrega al Usuario de la Herramienta de Teléfono Móvil (415). Si se rechaza la Opt-In, la solicitud terminó (416).

[0092] La FIG. 7 muestra el proceso Opt-In/Opt-Out. La Plataforma SMCS recibe una Solicitud de Mensaje Seguro (500). La Plataforma SMCS revisa su base de datos de preferencias para determinar si la Parte que se Busca ya optó por hacer parte del sistema (501). Sí = 502 - No = 503. La Plataforma SMCS determina que la Parte que se Busca ya optó previamente por hacer parte del sistema y envía el mensaje de contenido a la Parte que se Busca (502). La Plataforma SMCS determina que la Parte que se Busca no ha optado previamente por hacer parte del sistema y, por lo tanto, envía el mensaje Opt-In a la Parte que se Busca (502). La Parte que se Busca recibe el mensaje Opt-In (504). La Parte que se Busca determina si debe o no responder al mensaje (505). Sí = 507 - No = 506. No se necesitan pasos adicionales (506).

[0093] La Parte que se Busca determina si hace parte o no del sistema (507). Sí = 508 - No = 509. La Plataforma SMCS actualiza su base de datos con la preferencia de la Parte que se Busca como no hace parte del sistema (508). La Parte que se Busca determina si debe o no hacer parte del sistema (509). Sí = 510 - No = 505. La Plataforma SMCS actualiza su base de datos con la preferencia de la Parte que se Busca como no hace parte del sistema (510). La Plataforma SMCS responde al Mensaje Seguro (511) - véase FIG. 8.

[0094] La FIG. 8 muestra el proceso para responder a los Mensajes Seguros. El proceso de Opt-In/Opt-Out es el punto de partida (600). La Plataforma SMCS genera un mensaje a la Parte que se Busca. Este mensaje contiene las siguientes opciones:

ANUNCIO GRABADO

- La grabación se coloca en una dirección HTTP segura y está a disposición de la Parte que se Busca para que pueda ser escuchada durante un periodo de tiempo configurable. A la Parte que se Busca se le enviará un código (por ejemplo, 4 dígitos), código que se le solicitará a la Parte que se Busca para ingresar a la grabación.

MENSAJE DE TEXTO

- El mensaje de contenido puede enviarse en forma de un texto o mensaje SMS.

DEVOLVER LLAMADA

- Para devolver la llamada, la Parte que se Busca tendrá las siguientes opciones:
 - Llamar directamente desde la pantalla del teléfono móvil o marcando desde el teclado (entendiendo que su número de teléfono No se mostrará a la Parte que Busca).
 - El *67 puede marcarse antes de que se ingrese el número al que se devolverá la llamada, con el fin de evitar que el número de la Parte que se Busca aparezca en el teléfono de la Parte que Busca.

MENSAJES DE BLOQUEO

- Pueden bloquearse mensajes futuros de las Partes que se encuentra en Búsqueda al:
 - Hacer clic en el enlace proporcionado.
 - Al mensaje enviar texto de respuesta “Bloquear”.

[0095] Después de la expiración del anuncio grabado y/o la opción de privacidad de texto; si la Parte que se Busca intenta utilizar estas opciones, recibirá instrucción acerca de

la expiración de dicha función. En el caso del anuncio grabado, la Parte que se Busca ya no podrá escuchar el mensaje (601).

[0096] La Parte que se Busca recibe el mensaje de contenido con un enlace al correo de voz (602). La Parte que se Busca recibe el mensaje de contenido como un mensaje de texto (603). La Parte que se Busca determina si escucha o no el correo de voz (604). Sí = 606 - No = 605. No se necesitan pasos adicionales (605). La Parte que se Busca ingresa un código para escuchar el correo de voz. A la Parte que se Busca se le proporcionará el código de seguridad con el Mensaje Seguro (606). La Plataforma SMCS accede a la grabación y reproduce la grabación a la Parte que se Busca (607). La Parte que se Busca decide si debe llamar o enviar un texto a la Parte que Busca (608). Sí = 609 - No = 610. La Parte que Busca recibe o bien una llamada anónima o un mensaje de texto con el número de origen oculto de la Parte que se Busca (609). La Parte que se Busca determina si bloquea o no los mensajes futuros de la Parte que Busca (610). Sí = 611 - No = 612. La Plataforma SMCS actualiza su base de datos de preferencias para evitar que el número de la Parte que se Busca reciba mensajes futuros de la Parte que Busca (611). No se necesitan pasos adicionales (612).