(19) OFICINA ESPAÑOLA DE PATENTES Y MARCAS

ESPAÑA

(11) Número de publicación: **2 566 060**

(51) Int. CI.:

G06F 21/34 (2013.01)
G06F 21/40 (2013.01)
G06F 21/42 (2013.01)
G06F 21/10 (2013.01)

(12) TRADUCCIÓN DE PATENTE EUROPEA T3

(96) Fecha de presentación y número de la solicitud europea: **21.09.2007 E 07842933 (9)**

(97) Fecha y número de publicación de la concesión europea: **24.02.2016 EP 2074513**

(54) Título: **Sistemas y métodos de verificación y autenticación**

(30) Prioridad:

10.10.2006 US 545247

(45) Fecha de publicación y mención en BOPI de la traducción de la patente:
08.04.2016

(73) Titular/es:

EQUIFAX, INC. (100.0%)
1550 PEACHTREE STREET, NW
ATLANTA, GA 30309, US

(72) Inventor/es:

COLSON, CHRISTEN, J.

(74) Agente/Representante:

DE ELZABURU MÁRQUEZ, Alberto

DESCRIPCIÓN

Sistemas y métodos de verificación y autenticación

Campo de la invención

Las realizaciones de la invención se refieren a la verificación y autenticación de la identificación de usuarios de red, y en particular se refiere a sistemas y métodos para establecer niveles de riesgo o de verificación, para usar información procedente de una pluralidad de fuentes, y para verificar o autenticar la identificación de pequeñas empresas y directores u otros empleados.

Antecedentes

En la actualidad se usa una diversidad de redes. Las redes de ordenadores incluyen redes de área local (LANs), redes de área metropolitana (MANs), redes de área extensa (WANs), intranets, Internet, y otros tipos de redes. Las redes de comunicación incluyen las de servicio de telefonía convencional, redes celulares de diversas variedades, servicios de radiobúsqueda, y otras. Las redes se usan para muchos propósitos, incluyendo los de comunicar, acceder a datos, y ejecutar transacciones. Con frecuencia se hace necesario, por seguridad y por otros motivos, confirmar y/o verificar la identidad de un usuario antes de permitir el acceso a los datos o que ocurra una transacción en la red. El usuario puede ser una persona individual, aunque también es habitual que las pequeñas empresas accedan a sitios web en los que necesitan tener verificada su identidad.

La “verificación” es el proceso de confirmación de la identidad de una persona, entidad y/o dispositivo en el otro extremo de un canal. Es importante para muchas industrias, por ejemplo proveedores de servicios financieros (FSPs) establecer si el usuario, en el otro extremo, es o no quién dice ser. Los FSPs (banca, seguridad, intermediación e industrias aseguradoras), se han basado tradicionalmente en las comunicaciones cara a cara, pero con la llegada de la gestión de identidad, muestras, biométrica y tecnología de firma digital, las comunicaciones cara a cara como forma de hacer negocios está poco a poco resultando ser la excepción en vez de la norma. Sin embargo, el obstáculo de la distancia en lo que se refiere a la interacción electrónica se solventará solamente cuando se establezca un medio para verificar individuos, entidades y empresas.

El establecimiento de la verificación al comienzo de un proceso online, es una fase particularmente importante y es uno de los problemas de confianza más importantes para el negocio online. Incluso en las organizaciones más robustas, la verificación es un riesgo dinámico y evolutivo del negocio debido a que el fraude sigue amenazando las transacciones online y erosionan la confianza del cliente en servicios online, especialmente los servicios financieros. Más allá de los simples fraudes electrónicos, están apareciendo nuevas amenazas tales como ataques por suplantación de identidad, bots, registro de datos por pulsación de teclas, y herramientas de administrador remoto. Aunque algunas de estas amenazas pueden ser minimizadas o eliminadas con sentido común, otras están disimuladas, son sofisticadas e indetectables. La Comisión Federal del Comercio estima que millones de americanos han sido hurtados y han sufrido abusos en cuanto a su información personal, de una manera u otra, cada año, costando a los consumidores y empresas miles de millones anualmente. Además, algunos pronósticos estiman que el crecimiento del comercio U.S. online se verá materialmente reducido en los años venideros, dado que los proveedores de servicio se esfuerzan por encontrar soluciones de verificación correcta que no creen inconveniencias a los consumidores y que sean baratas de implementar.

Otro motor de verificación son las directrices de Consejo de Examen de Instituciones Financieras Federales (FFIEC) recién constituido, para instituciones financieras. Aunque no son regulaciones, el FFIEC espera que todos los FSPs cumplan con la guía para finales de 2006. Ésta ordena que los FSPs tengan un programa de seguridad eficaz que impida el acceso no autorizado y que solamente permita que los usuarios autorizados accedan a los sistemas y datos. Con las nuevas directrices, los FSPs se han visto obligados a replantearse sus cuestiones de verificación y autenticación. Éstos necesitan aplicar soluciones a través de su organización completa. Necesitan tener la capacidad de definir los requisitos que sean aplicables para la empresa en su conjunto. Necesitan soluciones que les ayuden a ser compatibles y cumplan sus necesidades de negocio de modo que puedan usar totalmente los canales electrónicos y hacer crecer su negocio y sus ingresos.

La verificación de nuevos usuarios es diferente de la autenticación de los usuarios existentes. Confirmar la identidad de un usuario puede ser un aspecto clave para mejorar la seguridad global, no solo en operaciones que requieran la autenticación de los usuarios, sino también cuando se requiera la verificación. Como norma general, la autenticación se refiere más a la confirmación de la identidad de un usuario establecido y/o de un usuario con una cuenta existente, mientras que la verificación se refiere más a confirmar la identidad de un usuario que no esté establecido y/o que no tenga una relación o una cuenta existente. Aunque pueda ser, en alguna medida, una superposición en la definición de verificación y de autenticación, o en el estado de un usuario cuya identidad necesita ser confirmada, también es cierto en general que hasta la fecha, las compañías de seguridad, hardware, software y conteo han estado más enfocadas a la provisión de servicios de autenticación que de servicios de verificación.

Existen algunas soluciones en el mercado que ofrecen verificación, pero son principalmente específicas de la industria. Por ejemplo, las soluciones para los FSPs pueden requerir que el usuario realice una transferencia de

fondos de cuenta a cuenta. Otro ejemplo son las soluciones eID de Equifax, las cuales requieren que el usuario final disponga de un conocimiento profundo de su información financiera y personal. Mientras que ambas opciones mencionadas pueden cumplir las necesidades de las perspectivas de los mercados de destino, no ofrecen una solución que pueda ser usada siempre por todos los mercados. En consecuencia, se necesitan motores adicionales de verificación/autenticación con opciones y funcionalidades más sofisticadas.

Como una cuestión práctica, en la arquitectura o diseño de una solución viable de verificación y/o autenticación, es preferible reconocer que una vez que un usuario ha sido inicialmente verificado, cuando retorna a un sitio web (por ejemplo, para realizar un negocio adicional, acceder a aplicaciones adicionales, plataformas, o realizar transacciones), su identidad necesita ser autenticada o reconfirmada cada vez que retorna, o se necesitará emplear algún mecanismo de seguridad equivalente. Tales visitas repetidas son diferentes de alguna manera respecto a la verificación de un nuevo usuario. Con respecto a una autenticación de red informática, una alternativa son las contraseñas específicas del usuario. Las contraseñas proporcionan algún nivel de protección, pero no son a prueba de fallos. Las contraseñas pueden ser vulnerables debido a que, con frecuencia, los usuarios las comparten o pueden ser fáciles de adivinar. Incluso aunque se conserven privadas, alguien que desee obtener una contraseña puede hacerlo a menudo usando generadores aleatorios, monitores de teclado, u otras técnicas. Además, cuando se trata con usuarios desconocidos tal como gente que desea realizar una transacción electrónica por Internet y que no ha sido aún verificado, las contraseñas ad hoc no son prácticas.

Existen diversos esquemas de no-contraseña que realizan algún nivel de autenticación y/o verificación con anterioridad a autorizar transacciones o permitir el acceso a datos. Estos sistemas requieren por lo general que un usuario proporcione una muestra de información de identificación básica tal como el nombre, la fecha de nacimiento, el número de seguridad social, la dirección, el número de teléfono, y/o información del permiso de conducir. Este tipo de información, conocida a veces como “información de tipo monedero”, se compara con datos conocidos, tal como un archivo de crédito, para determinar hasta donde coincide la aportación del usuario con esa fuente.

Por diversas razones, los esquemas de autenticación de nivel uno no son completamente fiables. En algunos casos, un usuario que proporcione información de identificación precisa puede no ser autenticado. Esto puede ocurrir, por ejemplo, debido a que el usuario introduce un apodo en vez de un nombre propio, y el proceso de autenticación no comprueba ningún apodo ni cualquier otra variación. Como resultado, un usuario que está intitulado para acceder a la información o realizar una transacción, no puede hacerlo. Otras inconsistencias pueden disparar un falso negativo, y con frecuencia el falso negativo (quizás después de un número de intentos) terminará la transacción sin procesamiento adicional ni consulta correctiva.

En otros casos, un usuario que proporciona información fraudulenta puede ser autenticado. Esto puede ocurrir cuando una información de tipo monedero perdida o robada es introducida por un usuario no autorizado. Otras situaciones pueden conducir también a un resultado de falso positivo. Ambos falsos positivos y falsos negativos son indeseables.

Algunos intentos de direccionar estos problemas han incluido la verificación de clientes, por medio de datos estáticos, para aplicaciones comerciales. Un ejemplo de esta alternativa se produce cuando un cliente aplica una tarjeta de crédito de un comercio en el sitio y se conecta por teléfono con la agencia de información crediticia para que responda a una serie de cuestiones que están en el archivo del historial de crédito del cliente para una aprobación o denegación inmediata del crédito del comercio. Otros intentos han incluido proporcionar una autenticación de primer nivel que puede incluir consultas relacionadas con información de tipo monedero, y si esas cuestiones son contestadas correctamente, puede avanzar entonces a una autenticación de segundo nivel que incluye cuestiones relacionadas con información que no sea de tipo monedero tal como información de cuenta de préstamo hipotecario, entidad de crédito, información de cuenta comercial, etcétera. Una vez que el usuario final que intenta acceder a un sistema ha contestado un numero apropiado de cuestiones correctamente, el acceso puede ser concedido o denegado. Un ejemplo de tales sistemas y procesos ha sido descrito en las Patentes U.S. núms. 6.857.073 y 6.263.447, incorporadas aquí por referencia. Tales sistemas y procesos pueden extraerse de uno o más tipos de bases de datos, tal como bases de datos relacionadas con créditos, bases de datos de servicios postales, bases de datos de telecomunicaciones, y otros tipos de datos.

Otros intentos han incluido el uso de datos biométricos, por ejemplo una huella dactilar capturada en forma digital o analógica, un escaneo del iris o de la retina, emparejamiento de la geometría del dedo o de la mano, o reconocimiento de escritura o reconocimiento de voz. Estas soluciones pueden ser útiles en algunos casos, pero puede que no sean siempre prácticas debido a diversas restricciones tecnológicas.

Un problema adicional experimentado por algunas instituciones financieras consiste en la verificación de la identificación de pequeñas empresas. Las pequeñas empresas pueden tener ciclos de vida más cortos que las grandes empresas, lo que puede hacer que sea más difícil para los sistemas acumular, almacenar y acceder a datos acerca del historial de crédito de la empresa. Las pequeñas empresas pueden no tener bienes suficientes sobre los que una institución financiera pueda extender el crédito, de modo que con frecuencia el crédito puede ser extendido al (a los) propietario(s) del pequeño negocio como préstamo personal. Aunque el préstamo sea, efectivamente, parte del panorama financiero de la pequeña empresa, el préstamo no podría ser reflejado como parte del archivo de historial de crédito de la pequeña empresa. Como tal, la entidad crediticia y otras instituciones financieras pueden

tener más dificultades cuando intentan verificar la identidad de una pequeña empresa, debido a que se puede necesitar también que el (los) propietario(s) o director(es) sean también verificados, su historial de crédito y otros datos comprobados, etc. Prestar con esta dificultad podría ser un caso en que estén involucrados varios bancos.

Por ejemplo, un pequeño negocio puede operar con el Banco 1: un propietario del pequeño negocio puede obtener, con el Banco 2, un préstamo personal para invertir en el negocio; y un segundo propietario puede obtener un préstamo personal similar en el Banco 3. El Banco 1 puede querer verificar la empresa, pero la empresa puede no tener un historial de crédito con el que el Banco 1 pueda comprobar y verificar datos fácilmente. En consecuencia, resulta deseable proporcionar un motor de verificación/autenticación que pueda extraer datos desde múltiples fuentes, en este ejemplo desde los Bancos 2 y 3 (en la medida en que puedan compartir información públicamente disponible en sitios web tal como el de Intercambio Financiero de la Pequeña Empresa). Tales sistemas han sido divulgados en la solicitud U.S. Serial núm. 10/021.468, presentada el 29 de Octubre de 2001, titulada “Sistema y Método para Facilitar el Intercambio de Información Financiera Correspondiente de la Pequeña Empresa”, la cual se incorpora aquí mediante esta referencia.

También es deseable dotar a una entidad (en este caso, el Banco 1) con la opción de cambiar, “llamar” o asignar al menos niveles de riesgo o verificación diferentes y fuentes de datos requeridas para la autenticación o verificación de usuarios que pretenden realizar actividades online. Por ejemplo, si el pequeño negocio deseara obtener un préstamo de 50.000 $, las actividades online para realizar esa transacción podrían requerir un nivel de verificación y/o autenticación que esté basado en la presentación y puntuación de preguntas desde un primer conjunto de datos o bases de datos. Sin embargo, un préstamo de diez millones de dólares podría requerir un nivel de verificación y/o autenticación diferente y más alto, basado en la presentación y puntuación de cuestiones desde otro conjunto de datos o bases de datos, con el fin de, entre otras cosas, aplicar un examen más severo, riguroso y/o más difícil de autenticación o verificación.

Puesto que la tecnología está cambiando continuamente, y la necesidad de una seguridad adecuada resulta crucial, resulta necesario un motor de verificación/autenticación que cumpla necesidades específicas del negocio y directrices de cumplimiento de normativas. También es necesario proporcionar un sistema que permita que el negocio establezca sus propias evaluaciones de riesgo conforme a sus prácticas y principios internos. Por lo tanto, existen necesidades de sistemas y métodos adicionales de verificación y autenticación, que puedan ser usados a través de las industrias para múltiples finalidades.

Sumario de la invención

Los motores de servicio de verificación y autenticación conforme a diversas realizaciones de la presente invención proporcionan una solución personalizable, con preferencia para transacciones online, que permite que una organización incremente la seguridad de acceso a sus plataformas y aplicaciones/servicios presentando y puntuando a continuación las respuestas a ciertas cuestiones que pueden ser extraídas desde múltiples fuentes. (A los efectos de esta aplicación, acceder a plataformas, servicios, aplicaciones, o realizar cualquier otro tipo de negocio puede ser mencionado como una “transacción”, lo cual se entiende que significa un intercambio de información, una transacción financiera, acceso a información, o cualquier otro evento donde pueda resultar apropiada la autenticación, verificación u otro control de acceso o medidas de seguridad). Quienes pretendan controlar el acceso a sus plataformas o servicios durante las transacciones, pueden participar en la naturaleza y dificultad de tales cuestiones (a) especificando o ayudando a especificar al menos una o más de las fuentes de datos desde las que se extraen las cuestiones, y (b) especificando o ayudando a especificar la naturaleza y la dificultad de las cuestiones. (Otros parámetros tal como el canal a través del cual accede el usuario a las plataformas y servicios, pueden ser también especificados, según se discute mejor en lo que sigue). Dichos sistemas y procesos permiten que tales clientes modulen la naturaleza de cuestiones y puntuación a efectos de controlar el nivel de dificultad, así como también controlen el nivel de gasto (puesto que el acceso a algunos datos es más caro que el acceso a otros datos). Por ejemplo, para una transacción potencial de baja participación, dicho cliente puede desear gastar una cantidad mínima en la etapa de autenticación, y por tanto desea presentar cuestiones para autenticación o verificación que sean extraídas desde una base de datos modestamente barata como una base de datos de telecomunicaciones o una base de datos del servicio postal. En otros casos, donde la participación es más alta, el cliente puede desear una seguridad extra en la forma de las cuestiones extraídas desde las bases de datos de información crediticia que estén menos sujetas a acceso no autorizado, pero que podrán ser más caras. En este sentido, el cliente puede tener algún control sobre el proceso de autenticación o verificación, similar de alguna manera a la forma en que un teclado en una máquina lavadora proporciona a un usuario opciones para lavar tejidos usando varias temperaturas, cantidades de agua y duración de los ciclos.

Exposición de la invención

Un método de control de acceso por parte de un usuario a sistemas tecnológicos de información de vendedor online usando un motor de verificación/autenticación y un motor de verificación/autenticación para controlar la comunicación y el acceso por parte de un usuario a sistemas tecnológicos de información de vendedor online conforme a la presente invención, han sido definidos en las reivindicaciones.

Un objeto de algunas realizaciones de la invención consiste en recolectar fuentes de datos existentes y soluciones

relacionadas con la identidad, y hacer que sean accesibles como servicios web de una manera en que el cliente tenga alguna aportación en cuanto a la naturaleza y la dificultad de las cuestiones presentadas en tales soluciones. Esto permitirá que un cliente o un vendedor (mencionado también como la entidad que usa el motor de verificación/ autenticación) para verificar y/o autenticar usuarios, clientes y empresas, así como empleados de empresas, que intenten obtener acceso a sus sistemas tecnológicos de información del vendedor de una manera que éstos puedan controlar o modular, al menos parcialmente.

Otro objeto de algunas realizaciones de la invención consiste en permitir a los fabricantes de símbolos de seguridad y a los proveedores de soluciones de autenticación, la capacidad de integrarse con el motor de verificación/ autenticación de modo que la verificación y/o la autenticación de la identidad puedan ser aseguradas con anterioridad a la distribución de dispositivos de seguridad, asegurando su uso a través de múltiples sitios, quizás no relacionados.

Otro objeto de algunas realizaciones de la invención consiste en proporcionar una solución que pueda ser vendida como motor de verificación y/o autenticación o servicio a cualquier industria o negocio, grande o pequeño, que necesite verificar o autenticar un individuo o un negocio con anterioridad a obtener el acceso a un sistema o a datos.

Un objeto adicional de algunas realizaciones de la invención consiste en dotar a las empresas con la capacidad de establecer su nivel de riesgo o verificación y la seguridad de acompañamiento para que coincida con las necesidades de verificación y/o autenticación a través de toda su empresa.

Un objeto adicional de algunas realizaciones de la invención consiste en dotar a la empresa con la capacidad de añadir sus propias fuentes de datos en el motor de verificación/autenticación para reforzar el proceso y su nivel de confianza. Con una infraestructura basada en normas dinámicas, los clientes o los vendedores pueden añadir diversos servicios y datos de verificación y/o autenticación que soporten sus redes de forma fácil y económica.

Un objeto adicional de algunas realizaciones de la invención consiste en proporcionar múltiples ofertas de canales (incluyendo una o más de entre internet, intranet, e-mail, mensajería instantánea u otros canales tales como uno o más de entre los sistemas de telefonía o voz, teléfonos celulares, ATM, kiosco, escáner, punto de terminal de venta, sistemas móviles, blackberry, dispositivos manuales, PC de bolsillo, dispositivos inalámbricos, o cualquier otra plataforma) para servicios de autenticación y/o de verificación.

Otro objeto de algunas realizaciones de la invención consiste en proporcionar una solución única de verificación y/o autenticación que pueda ser personalizada para que cumpla con las necesidades de las pequeñas, medias y grandes empresas, y que pueda reducir los gastos de capital y de operación por usuario.

Un objeto adicional de algunas realizaciones de la invención consiste en proporcionar un sistema que pueda reconocer si el usuario es un individuo o una empresa y (al menos) valore el acceso al motor de verificación/ autenticación de manera correspondiente.

A un nivel más amplio, los sistemas y procesos de verificación y autenticación conforme a algunas realizaciones de la invención reciben una pregunta desde un cliente o un vendedor relacionada con un usuario potencial que está intentando acceder a una aplicación o transacción particular. Dependiendo de la naturaleza de la aplicación o transacción, el nivel de riesgo involucrado y/u otros criterios, el cliente o el vendedor pueden ayudar a seleccionar al menos uno o más de los tipos y/o fuentes de datos que se usarán para la autenticación o la verificación, así como la naturaleza, el número, la dificultad y/u otros parámetros usados para determinar las cuestiones que serán presentadas para la autenticación y/o la verificación. El motor puede puntuar las respuestas a las preguntas, con preferencia conforme a parámetros seleccionados por el cliente, y puede enviar un aviso o una decisión al cliente o al vendedor acerca de si se concede o se deniega el acceso.

Algunos aspectos de la invención se refieren a un método de control de acceso por un usuario (ya sea online o a través de cualquier otro canal) a los sistemas tecnológicos de información del vendedor usando un motor de verificación/autenticación, que comprende:

(a) recibir una pregunta desde un sistema del vendedor para verificar un usuario particular para una transacción, en donde el vendedor ha asignado a la transacción particular un nivel de riesgo;

(b) en donde el vendedor ha especificado un nivel de verificación apropiado para cumplir con el nivel de riesgo asignado, que comprende especificar una pluralidad de fuentes de datos que contienen información acerca del usuario;

(c) preguntar al usuario, usando cuestiones generadas en base a datos procedentes de al menos dos de las fuentes de datos;

(d) determinar el grado en que el usuario responde correctamente a las preguntas, y

(e) determinar si se concede o se deniega el acceso por parte del usuario a los sistemas tecnológicos de información del vendedor en base al grado en que el usuario conteste correctamente a las cuestiones.

Según se ha usado anteriormente y a través de la presente solicitud, el término “cuestión” significa, además del escenario típico de pregunta y respuesta, el uso de verificación de voz, escaneo de huella digital, biométrica, o cualquier otro medio de identificación de datos que puedan ser obtenidos y verificados y/o autenticados o respondidos por un usuario. Por ejemplo, la pregunta en “cuestión” podría ser si la huella digital del usuario coincide o no con la huella digital contenida en el archivo, y la “respuesta” podría ser la propia huella digital, etcétera.

Otros aspectos se refieren a un motor de verificación/autenticación adaptado para controlar el acceso por un usuario online a sistemas tecnológicos de información del vendedor, que comprende:

(a) una opción de establecimiento de riesgo, en donde el vendedor especifica un nivel de riesgo apropiado para verificar y/o autenticar al usuario, y

(b) una opción de establecimiento de fuente de datos, en donde el vendedor especifica al menos dos fuentes de datos para que sean investigadas a efectos de generar cuestiones de verificación/autenticación.

Breve descripción de los dibujos

La Figura 1 es un diagrama de flujo de una forma de flujo de proceso para asignar un nivel de riesgo a aplicaciones particulares en una red de comunicaciones conforme a una realización de la invención;

La Figura 2 es un diagrama de flujo para una forma de procesamiento global para verificar y/o autenticar usuarios conforme a una realización de la invención;

La Figura 3 es un diagrama esquemático que muestra intercambio de información para verificar y/o autenticar usuarios conforme a una realización de la invención.

Descripción detallada de realizaciones de la invención

Se deberá proporcionar, preferiblemente, el nivel de verificación y/o autenticación a los riesgos asociados a la transacción respecto a la que se está buscando la verificación o autenticación; por ejemplo, varios niveles de acceso podrían requerir niveles diferentes de verificación o autenticación. Estos niveles pueden ser preferiblemente dinámicos y coincidir con la petición correspondiente en el momento de la petición. La fuente desde la que se obtiene información de verificación o autenticación puede ser también variada, dependiendo del nivel de riesgo asignado. Esto puede ayudar a mitigar riesgos de extraer todas las cuestiones de verificación y autenticación desde una sola fuente.

Durante el uso, una vez que se ha concedido a un usuario acceso a un nivel de riesgo particular (por ejemplo, el Nivel 2), entonces el usuario podrá tener acceso a todos los niveles que requieran el mismo nivel de riesgo o uno inferior (por ejemplo, el Nivel 1). En este ejemplo, una vez que se ha verificado y/o autenticado un usuario en el Nivel 2, éste deberá tener acceso a todas las aplicaciones, servicios, transacciones que estén en el Nivel 1, así como a otras que estén designadas con el mismo nivel de riesgo en el Nivel 2. Esta característica puede ser configurable, de modo que el vendedor pueda seleccionar esta opción por defecto o requerir que los usuarios sean verificados/autenticados para todos y cada uno de los servicios o transacciones estableciendo sus propios parámetros. De hecho, la mayor parte de las características descritas para los sistemas discutidos en la presente solicitud pueden ser todos ellos configurables, de modo que el vendedor pueda personalizar el sistema según se necesite para usos o usuarios particulares. Esto puede ayudar también a un vendedor o un cliente que usa el motor de verificación/autenticación a valorar apropiadamente el servicio - por ejemplo, una transacción de 10 $ no necesita la misma verificación que una transacción de un millón de dólares, y por lo tanto, no necesitan ser consultadas bases de datos más caras. Por consiguiente, los vendedores pueden desear controlar las fuentes usadas para verificar a sus usuarios por muchas razones, incluyendo el control del precio. Éstos pueden desear extraer información desde sus propias fuentes de datos a costes más bajos. (Se comprenderá que cuando se usa el término “verificación” en la presente solicitud, se pretende hacer referencia al acto de confirmar la identidad de un usuario potencial, y por lo tanto, el término autenticación puede ser igualmente aplicable, y viceversa. Se debe entender también que los términos “vendedor” o “cliente” están destinados a referirse a cualquier entidad que use los servicios de verificación/autenticación descritos en la presente solicitud).

Los motores de servicios de verificación/autenticación conforme a varias realizaciones de la presente invención proporcionan una solución personalizable que puede ser “llamada” en base al nivel de riesgo asignado a aplicaciones individuales o agrupadas a las que se pueda acceder durante una transacción. En algunas realizaciones, el sistema integra un motor basado en reglas de modo que se pueden instituir (“llamar”) reglas apropiadas según el riesgo asignado a una transacción. El motor basado en reglas puede proporcionar también una oportunidad para la personalización local en base al segmento, la localización geográfica y el tipo de servicio requerido. En resumen, la alternativa de “llamar” permite que los clientes accedan a soluciones en cualquier mercado y en cualquier ubicación. Esto permite también que los clientes accedan a productos que se encuentran disponibles en sitios web específicos que están enlazados al sistema (por ejemplo, el sitio web EquifaxDirect, o cualquier otro sitio web que esté enlazado al sistema). También permite que el motor de verificación/autenticación salte al, o marque el, riesgo apropiado y sus requisitos de seguridad/verificación que lo acompañan.

Aunque se han descrito realizaciones como llamada o salto a bases de datos separadas, discretas, es comprensible que una sola base de datos entremezclada pueda contener información compilada procedente de varias fuentes de datos, pero almacenada en una posición. Esta base de datos entremezclada puede estar separada por contenido o por nivel de riesgo.

Realizaciones de la presente invención proporcionan un motor de verificación/autenticación que puede ser usado por todas las industrias. Éstas habilitan una entidad usando el motor para establecer sus propias evaluaciones de riesgo conforme a sus prácticas y principios específicos. Ésta es la opción basada en reglas de algunas realizaciones. En primer lugar, el vendedor (o el cliente o la entidad) asigna un nivel de riesgo a cada aplicación/transacción que éste ofrece. Por ejemplo, el vendedor podría ser un sitio de inversión o de banca que necesite proteger su información y verificar o autenticar usuarios cuando los usuarios intentan acceder al sitio o a determinas plataformas o aplicaciones en el sitio. El vendedor podría entonces especificar un nivel de verificación apropiado que cumpla con el nivel de riesgo asignado. Por ejemplo, para una transacción que requiera un nivel muy alto de certidumbre acerca de la identidad de un usuario, también conocido como alto nivel de análisis (por ejemplo, riesgo bajo), el nivel de verificación podría ser establecido de modo que requiera que los datos sean extraídos desde más fuentes (por ejemplo, X, Y y Z) y que haga más preguntas por cada fuente de datos. Puesto que aplicaciones o transacciones suben la escala de riesgo, las cuestiones presentadas pueden resultar más difíciles y variadas. Esto podría ser un "nivel de verificación" específico que sea especificado por el vendedor. También es posible que el vendedor establezca un nivel de riesgo basado en el canal que esté siendo usado por el usuario. Por ejemplo, si los terminales de punto de venta o los kioscos presentan un riesgo mayor que un acceso online, las transacciones de punto de venta/kiosco pueden estar designadas a un nivel de verificación más alto.

Entonces, cuando el sistema de la entidad consulta el motor de verificación/autenticación sobre una nueva información del usuario, el motor de verificación/autenticación está capacitado para "llamar" al nivel de verificación apropiado que cumpla el nivel de riesgo asociado. En resumen, la "llamada" puede ser establecida también para consultar algunas fuentes de datos, bases de datos, o fuentes de información, y para que pregunte un determinado número de cuestiones desde cada base de datos o cada fuente de información, ejemplos específicos de lo cual se describen más adelante. Estas fuentes de datos y cuestiones son configurables y pueden soportar un cambio en el flujo de trabajo. Dependiendo de la naturaleza del nivel de riesgo asignado, puede existir un número específico de cuestiones que necesiten ser contestadas correctamente a efectos de que un usuario obtenga acceso a un sitio, o la dificultad de las cuestiones puede variar, dependiendo de niveles preestablecidos. Las preguntas y las respuestas pueden proceder de múltiples fuentes de datos, por ejemplo, intercambios de información de pequeños negocios tal como el Intercambio Financiero de la Pequeña Empresa (SBFE) y las bases de datos de Intercambio de Pequeñas Empresas SBX. Otros ejemplos no limitativos incluyen bases de datos de registro de créditos, bases de datos de correo (por ejemplo, MetroMail, PostalSoft), bases de datos de permisos de conducir, guías telefónicas online, sitios web de quién/donde, bases de datos de reunión, colegios o escuelas secundarias, bases de datos de viajeros frecuentes, información de cuentas de inversión y de jubilación, información de compañías aseguradoras, información médica, datos de pasaporte u otra información gubernamental, información de la compañía telefónica o de otra compañía de servicios públicos, sitios de pago de facturas, sitios de registro de automóviles, bases de datos de funerales, bases de datos internas del vendedor, y cualesquiera otras bases de datos internas o comercialmente disponibles.

Si un nivel de riesgo de un producto o servicio requiere datos procedentes de una fuente adicional, el motor de verificación/autenticación puede saltar a esa fuente. En el ejemplo de verificación de una pequeña empresa, si se necesita la verificación de una pequeña empresa y no existe ningún dato dentro de las bases de datos de SBFE y/o de SBX, o si el archivo es demasiado fino, entonces la solución de verificación/autenticación puede volver a las fuentes de datos existentes para complementar el proceso. Las fuentes pueden ser fuentes de datos existentes dentro de una compañía de información crediticia (tal como Equifax), o a través de relaciones, a modo de datos de cuentas de depósito a la vista (DDA), o de terceros tal como Dunn & Bradstreet. Esto asegura una tasa de éxito de verificación automática más alta, y también incrementa el nivel de confianza y la precisión de esa verificación.

Por ejemplo, realizaciones del motor de verificación/autenticación pueden "llamar" a fuentes de datos de terceros proporcionadas por el cliente, por socios y/o por otros, para proporcionar un gran archivo (o "banco de datos") desde el que se elijan cuestiones para probar la propiedad y verificar/autenticar la identidad. La "llamada" habilita cuestiones que son presentadas al usuario para incorporar automáticamente preguntas y respuestas que son aplicables al riesgo asignado a las transacciones. En base al producto y/o servicio al que el usuario está pidiendo acceder, se pueden incorporar múltiples fuentes de datos al proceso de verificación. Por lo tanto, si un archivo no puede proporcionar suficiente información (preguntas & respuestas), el sistema puede saltar automáticamente a fuentes de backup o adicionales. Por ejemplo, el motor de verificación/autenticación puede estar establecido de modo que busque en primer lugar los datos de la agencia de informes crediticios (por ejemplo, titular de préstamo hipotecario y cantidad, pago de coche y cantidad, balances de tarjetas de crédito, qué tarjetas de crédito de establecimientos mantiene, etc.), pero dependiendo del nivel de riesgo que se marque para la transacción particular, se puede entonces seleccionar también y extraer datos desde otras fuentes adicionales, tanto externas como internas. Es posible que las fuentes o bases de datos buscadas durante esta etapa de búsqueda de datos de salto o de backup sean seleccionadas específicamente por la entidad que contrata los servicios de motor de verificación/ autenticación.

Por ejemplo, la verificación/autenticación que se realiza en un punto de venta en un almacén o una gasolinera cuando un usuario pasa una tarjeta de crédito (por ejemplo, con un código postal requerido con anterioridad a la verificación) deberá probablemente ser diferente de la verificación/autenticación que se realiza en una empresa de coches usados antes de que el comprador pueda alejarse con el coche. Puesto que los importes de las compras son diferentes y existe mayor riesgo involucrado, se pueden necesitar más datos del comprador del coche. Adicionalmente, puede ser el caso de que la introducción del código postal no sea una verificación suficiente para algunos almacenes o gasolineras, por ejemplo, si el importe de la compra excede X dólares o si ha existido una racha de usos de tarjetas de crédito falsas en la zona, el vendedor puede desear establecer un nivel de seguridad más alto y requerir la aportación de más información desde fuentes seleccionadas. En esos casos, el vendedor puede desear implementar sistemas tales como los descritos en la presente memoria a efectos de extraer datos desde otras fuentes e identificar ciertos niveles de riesgo tolerados.

Permitir que el vendedor u otra entidad identifique y seleccione las fuentes que desee para verificar y emparejar esas aplicaciones y servicios (colectivamente “transacciones”) frente a niveles de seguridad apropiados previamente establecidos, puede proporcionar a las entidades y a sus usuarios mayor confianza en el proceso de verificación/autenticación. Esto permite también que la entidad use sus propias fuentes de datos que estén enlazadas a sus sistemas, de modo que puede “llamar” a sus propias fuentes internas, o a una mezcla de fuentes de datos tanto internas como externas. Esto permite además que la entidad decida sobre su precio; por ejemplo, ésta puede desear buscar inicialmente motores de búsqueda menos caros para niveles de riesgo más bajos (por ejemplo, quizás bases de datos internas, que sean gratis para el vendedor), y solamente acceder a búsquedas más caras para transacciones en las que el riesgo asignado requiere una certidumbre de verificación y/o autenticación más elevada.

Realizaciones de la presente invención pueden estar dotadas de la capacidad de priorizar elementos de datos, de modo que si una pieza particular de datos puede ser obtenida desde más de una fuente, el motor puede especificar la fuente que puede usarse. Por ejemplo, si un número de permiso de conducir puede ser obtenido desde dos fuentes de datos diferentes, el motor puede ser configurable para especificar la fuente a usar. En algunas realizaciones, el motor puede estar configurado para obtener los datos desde la fuente menos cara.

En resumen, como un usuario aumenta el nivel de riesgo y las transacciones requieren una certidumbre más alta, el motor de verificación/autenticación “sube” el nivel también. Si el riesgo asociado a la transacción pide verificación online en tiempo real, el motor de verificación/autenticación puede proporcionar esto también. Pueden ser casos, aplicaciones o transacciones en las que el vendedor elija usar datos en tiempo real para un nivel de certidumbre particularmente alto. Por ejemplo, si alguien acaba de realizar una compra en la Tienda de Comestibles A, el motor podría extraer esos datos en tiempo real y preguntar sobre cuál ha sido la compra dentro de unos pocos segundos o minutos después de la compra.

En el contexto del comercio electrónico, las transacciones de riesgo más bajo, tal como las compras relativamente pequeñas, puede que no requieran un alto nivel de riesgo asignado. Por otra parte, las transacciones de riesgo más grande o más sensible, tal como grandes compras o acceso a datos sensibles, pueden requerir un proceso de verificación y/o autenticación más exhaustivo a un nivel de certidumbre más alto con relación al riesgo asignado. Las características de las realizaciones de la invención evitan los inconvenientes que podrían encontrarse al requerir que cada transacción sea verificada y/o autenticada en el mismo nivel de certidumbre (por ejemplo, una transferencia bancaria de 10 $ comparada con un préstamo de un millón de dólares) al permitir que se lleven a cabo diferentes niveles de verificación en base al nivel de seguridad deseado, reduciendo costes y el uso innecesario de recursos del sistema.

Como ejemplo, considérese la analogía con una máquina lavadora. Si un cliente está solicitando una transferencia bancaria de 50.000 $, eso podría ser considerado como una “carga completa” para la que se preguntará una serie de cuestiones difíciles desde fuentes x, y, z. Por el contrario, si un cliente está solicitando un pago de 25 $, que podría ser considerado como una “carga ligera” para la que se podría consultar una serie de cuestiones menos difíciles desde fuentes de datos más baratas. La entidad o el vendedor que usan el motor de verificación/ autenticación han sido dotados de la oportunidad de pagar de forma diferente por cargas diferentes en la máquina lavadora. Típicamente, fuentes de datos diferentes tienen costes diferentes. Así, los precios para los servicios de motor de verificación/autenticación serán típicamente diferentes dependiendo de qué fuentes haya identificado el vendedor como parte de la “llamada”. Adicionalmente, otro beneficio del concepto de llamada consiste en que al cliente que solicita el pago de 25 $ no se le da el “tercer grado” antes de que esté en condiciones de completar la transacción.

En algunas realizaciones, la configuración de la llamada puede ser personalizada a nivel de administración, y se basa en los requisitos de seguridad y en los riesgos asociados. Por ejemplo, si un primer FSP quisiera establecer el nivel de riesgo para que un cliente potencial realice una retirada de 1-10.000 $ de una cuenta de Nivel de Riesgo 1, y una retirada de 10.0001-50.000 $ a un Nivel de Riesgo 2, y así sucesivamente, éste puede desear que las cuestiones de Nivel de Riesgo 1 provengan de una base de datos interna y por defecto de bases de datos públicas, gratis, en caso de que sea necesario obtener más cuestiones para completar el proceso, y cuestiones de Nivel de Riesgo 2 que sean extraídas desde un sitio de agencia de informes crediticios. Un segundo FSP puede desear, sin embargo, establecer sus niveles de riesgo de forma diferente, por ejemplo de 1-75.000 $ a Nivel de Riesgo 1 y de

75.000-200.000 $ a Nivel de Riesgo 2. Del mismo modo, también puede seleccionar diferentes fuentes de información desde las que extraer los datos para las preguntas al usuario. La función de establecimiento de llamada permite que el administrador en cada FSP establezca sus niveles de riesgo en el nivel deseado. En este ejemplo, cada FSP estaba también capacitado para personalizar sus fuentes de información adicional deseadas. Adicionalmente a la provisión de mayor personalización, esta opción puede ayudar también a que la entidad controle sus costes.

Otra opción disponible es la de permitir que el vendedor identifique la forma en que son hechas las preguntas, dependiendo del canal de comunicación. Por ejemplo, si la transacción es online con un ordenador, el teclado completo está disponible para que el usuario mecanografíe una respuesta detallada a una cuestión. En esta situación, la forma de la cuestión no es un tema limitativo. Sin embargo, si un punto de terminal de venta solamente tiene un teclado numérico, entonces las cuestiones pueden necesitar que estén enmarcadas de una manera de "sí/no" (¿es su dirección 123 Ivy Lane?) o en un formato numérico (por ejemplo, ¿cuáles son los últimos 7 dígitos de su permiso de conducir?). Por el contrario, si se encuentra disponible un terminal de escaneo de huella digital (por ejemplo, en un terminal de pago táctil), entonces se pueden usar los datos de la huella digital, y así sucesivamente. En resumen, el concepto es que las preguntas y las respuestas (en el sentido más amplio de ambos términos) estarán impuestas por el canal que esté usando el usuario. Si el canal que está usando tiene una gran pantalla con espacio para texto, se puede usar una pregunta más larga, pero si el canal que está usando tiene solamente una pantalla pequeña con espacio limitado, la forma de la pregunta y de la respuesta necesitará probablemente ser modificada de manera correspondiente.

Los diversos canales podrían incluir comunicación a través de internet, de una intranet, de e-mail, de mensajería instantánea o de otros métodos tales como teléfono o sistemas de voz, teléfonos celulares, ATM, kiosco, escáner, punto de terminal de venta, sistemas móviles, blackberry, dispositivos portátiles, PC de bolsillo, o dispositivos inalámbricos. Se pueden usar cualesquiera otros canales de comunicación, y se considerarán dentro del alcance de la invención.

Se podrá apreciar también que si un usuario no puede ser verificado usando el canal preferido (por ejemplo, el usuario está online y ha contestado demasiadas preguntas incorrectamente y por tanto ha sido bloqueado por el sistema), entonces el sistema de verificación/autenticación puede recurrir por defecto a un sistema manual. En el ejemplo anterior, una vez que el usuario ha sido bloqueado, éste podría ser inducido a llamar al vendedor para completar el proceso de verificación/autenticación a través del teléfono. El vendedor podría aún tener las preguntas y las respuestas sobre una pantalla y simplemente preguntar al usuario para que confirme la información o responda a las cuestiones.

La debilidad en alguna de las soluciones existentes consiste en que éstas son estáticas. Por lo tanto, si alguien pretendiera obtener acceso no autorizado a los informes crediticios, la solución completa podría verse comprometida. Sin embargo, puesto que las realizaciones del motor de verificación/autenticación descritas en la presente memoria son dinámicas y no usan simplemente datos de informes crediticios del consumidor, éstas son mucho más difíciles, y quizás imposibles, de quedar comprometidas.

Un ejemplo general del proceso de establecimiento de riesgo y fuente de información, ha sido mostrado en la Figura 1. Un administrador de red de vendedor o de cliente o de servidor, puede asignar niveles de riesgo a varias transacciones. (La autenticación y los permisos que la acompañan pueden ser definidos también durante el proceso de configuración). Por ejemplo, una transferencia bancaria entre cuentas del mismo titular de la cuenta puede ser un Nivel de Riesgo A, mientras que una transferencia bancaria a una cuenta de un titular de cuenta diferente puede ser un Nivel de Riesgo D. En las Figuras se han mostrado otros ejemplos con las cantidades retiradas.

La Figura 2 muestra las etapas que pueden tener lugar una vez que un usuario intenta acceder a transacciones del vendedor (las cuales, según se discute, pueden ser diversas plataformas, aplicaciones y/o servicios relacionados con información, transacciones financieras, acceso a información, o cualquier otro evento en el que puedan ser apropiadas medidas de autenticación, verificación, u otro control de acceso o medidas de seguridad). Cuando un usuario que desea solicitar una transacción online accede a una red de vendedor o cliente/servidor a través de un terminal de cliente, el lado del servidor en la red (o el sitio del vendedor) comunica con un motor de verificación/autenticación. El motor de verificación/autenticación determina el nivel de verificación que deberá ser acorde con la identidad del usuario en base a reglas específicas del vendedor que acepta la transacción.

De ese modo, el alcance del proceso de verificación llevado a cabo depende de la naturaleza de la transacción y de los requisitos específicos del vendedor. El vendedor establece el nivel de riesgo asignado, y el motor de verificación/autenticación localiza preguntas y respuestas apropiadas a partir de fuentes apropiadas que cumplan con el nivel de riesgo asignado. El motor de verificación/autenticación envía varias cuestiones al usuario ya sea a través del sitio web del vendedor o bien el usuario puede ser redirigido a un sitio separado para el motor de verificación/autenticación. En general, el usuario y las credenciales que lo acompañan deben estar capacitados para que sean pasados de la pantalla de inicio de sesión (portlets) a uno o más recursos objetivo (bases de datos) y/o posiciones de verificación. Se prefiere que el motor de verificación/autenticación sirva como portal centralizado común para que pasen las credenciales presentadas hasta la posición apropiada para su verificación, aunque también están disponibles otras opciones y se consideran dentro del alcance de la invención.

En general, el usuario es verificado y/o autenticado en base a su capacidad de responder sucesivas preguntas sobre información personal, y al nivel de coincidencia que se alcanza de comparar la información proporcionada con fuentes de datos fiables. Por ejemplo, se puede pedir inicialmente al usuario que proporcione un primer nivel de información de identificación, tal como el nombre, la dirección, el permiso de conducir u otra información que pueda ser portada normalmente por la persona. Esta información se transmite al motor de verificación/autenticación, el cual lleva a cabo una verificación y/o autenticación de primer nivel sobre esa información comparando el grado de coincidencia entre la información suministrada por el usuario y los datos conocidos sobre el usuario a partir de otras fuentes. Tras la terminación de este proceso de verificación y/o autenticación de primer nivel, el motor de verificación/autenticación determina si son necesarias más preguntas dependiendo del nivel de riesgo asignado.

Con preferencia, algunas de las cuestiones adicionales son información privada que solamente puede conocer el usuario, tal como por ejemplo un prestamista hipotecario, pago del coche, u otra información obtenida de un informe crediticio o de otra fuente. Dependiendo del nivel de riesgo asignado y de la dirección de la entidad que usa el motor de verificación/autenticación, se extraen cuestiones adicionalmente desde otras fuentes, según se ha descrito con anterioridad.

La financiera privada u otros datos obtenidos en el (los) nivel(es) más alto(s) del proceso de verificación pueden ser solicitados usando una pregunta interactiva, tal como múltiples cuestiones opcionales, cuestiones verdaderas/falsas, o cuestiones que requieran una aportación del usuario que son generadas automáticamente en base a la información disponible en las fuentes de datos conocidos. El motor de verificación/autenticación puede acceder a un archivo de crédito para identificar préstamos del usuario que estén aún en estado de devolución. Se pueden seleccionar uno o más préstamos, y la pregunta interactiva podría preguntar al usuario por el nombre del prestador o el importe de pago en el préstamo identificado, y ofrecer un número de opciones entre las que puede elegir el usuario, de las que solamente una es la correcta. Dependiendo de las respuestas, la identidad del usuario puede ser verificada. Si se necesita un nivel de certidumbre más alto, el motor de verificación/autenticación puede extraer cuestiones adicionales desde otras fuentes.

Una característica adicional que puede ser proporcionada consiste en que las credenciales usadas para la verificación pueden estar disponibles para preguntar sobre servicios de perfil externo que contengan información acerca de las preferencias del usuario (preferencias de alertas, intereses, productos adquiridos, direcciones, etc.).

Otra característica opcional consiste en que el motor pueda buscar en múltiples idiomas.

Una característica opcional adicional consiste en que una compañía pueda usar este sistema internamente. Si existen cambios en las políticas de seguridad de una compañía que, por ejemplo, requieran que todos los usuarios sean verificados de nuevo y contesten más cuestiones, el motor basado en reglas puede ser modificado para albergar el cambio. El motor puede habilitar también al usuario para que establezca reglas para los diversos niveles. Por ejemplo, si un empleado puede acceder solamente al sitio de intranet de la compañía, éste puede tener que ser re-verificado solamente una vez al año. Si está accediendo a datos confidenciales, se puede requerir que éste sea re-verificado cada 90 días. Cuando se concede a un empleado acceso a fuentes de información adicionales, ese empleado puede modificar su perfil de manera correspondiente. Éste deberá contestar cuestiones adicionales en base al nuevo nivel de seguridad y se le podrá conceder acceso inmediato.

Una vez que el proceso de preguntas se ha completado, el motor de verificación/autenticación puede proporcionar al vendedor o a la entidad que contrate el motor de verificación/autenticación un nivel de confianza o un porcentaje de seguridad acerca de la identificación del usuario. Por ejemplo, en vez de proporcionar un comando de “aceptar” o “denegar”, el motor de verificación/autenticación podría proporcionar un nivel de confianza o porcentaje de seguridad, por ejemplo, seguridad del “85%” de que el usuario es quién dice ser. Por supuesto, también es posible que el motor de verificación/autenticación proporcione simplemente un comando de “aceptar” o “denegar” (o un comando de sí/no), y esto podría estar basado en un porcentaje de nivel de confort establecido por el vendedor. Por ejemplo, si el porcentaje de seguridad es superior al 85% para un determinado nivel de riesgo, el vendedor puede autorizar que el motor de verificación/autenticación otorgue automáticamente el acceso. La transacción que el usuario está solicitando puede ser llevada a cabo o no (o emprendida otra acción) dependiendo de los resultados de la autenticación.

También es posible que el vendedor marque la clase de servicio de puntuación que prefiera. Por ejemplo, éste puede decidir el nivel de error tipográfico que permitirá en las respuestas del usuario. Por ejemplo, si un usuario potencial tuviera que mecanografiar un código postal incorrecto respecto a su dirección en el archivo, el motor de verificación/ autenticación puede estar establecido en una de muchas opciones, tal como preguntar al usuario (con un número establecido de respuestas incorrectas que pueden ser presentadas con anterioridad a que se bloquee la aplicación o la transacción), o (b) bloqueando directamente al usuario de forma inmediata. Según otro ejemplo, cada aplicación en cada nivel de riesgo puede tener un número establecido de intentos y si se rebasa ese número, entonces el usuario puede ser rechazado de forma permanente (hasta que, por ejemplo, el administrador de la base de datos reconfigure la pantalla). Alternativamente, pueden existir modelos de puntuación más sofisticados que pueden ser usados. El concepto general es que el vendedor pueda identificar sus niveles de riesgo, incluyendo el nivel de confianza y los niveles de puntuación, que prefiera que sean usados durante el proceso del motor de verificación/autenticación.

Una vez que se ha cumplido el proceso de hacer consultas y de verificación y/o autenticación, el motor de verificación/autenticación, u otra fuente, puede generar un certificado digital que registre niveles de verificación y otra información relacionada con el usuario. El certificado digital puede ser presentado después en futuras transacciones para evitar la necesidad de re-verificar al usuario por cada nuevo evento de transacción.

Por ejemplo, si se debe emitir un certificado digital una vez que un usuario completa la verificación, el usuario puede ser dirigido a una compañía de emisión apropiada, junto con la verificación de que el certificado debe ser emitido. Se puede pedir al usuario que introduzca información de identificación y objetivo o contraseña para generar y almacenar un certificado digital. Si el usuario es una pequeña empresa, el certificado digital podrá ser emitido a una persona o a un grupo de personas que estén autorizadas a realizar transacciones en favor de la empresa. En resumen, el motor de verificación/autenticación verifica al usuario y a continuación transfiere el usuario a otra compañía (por ejemplo RSA o VeriSign) para obtener el certificado digital. Se podrá comprender también que pueden estar incluidas otras compañías y/o proveedores de servicio de datos, tal como compañías de biométrica y empresas de símbolos que puedan realizar la verificación a través de verificación de voz, escaneos de huella digital, escaneos de retina, ADN, o cualquier otra característica biométrica o de identificación apropiada. El ejemplo que sigue describe, y está relacionado con, un certificado digital, pero deberá entenderse que se pueden usar también otras características identificativas. El ejemplo es igualmente aplicable a otros métodos.

De forma resumida, un certificado digital contiene típicamente un conjunto de campos que incluyen identificación de usuario, un número de serie de certificado digital, un período de caducidad, así como también información relacionada con el emisor del certificado digital y los datos de huella digital para el certificado digital. Éste se almacena preferentemente de una manera segura en el servidor del cliente y se protege mediante preguntas de identificación y objetivos de usuario o de contraseña antes de que el receptor pueda liberar el certificado digital para otras transacciones. Un certificado digital puede ser un archivo de datos almacenado en un formato común legible con máquina que, tras la liberación apropiada por el usuario, puede ser presentado a otros servidores de autenticación para posteriores transacciones, como prueba de la identidad. Esto ayuda a evitar la necesidad de re-autenticar al usuario para posteriores eventos. Los certificados digitales contienen un campo de caducidad, pero el certificado puede ser generado también de modo que dure indefinidamente.

Los proveedores de autenticación (por ejemplo, RSA, VeriSign, BusinessSignatures, etc.) no tienen la capacidad de proporcionar verificación, solamente distribuyen servicios para autenticación. Por consiguiente, las empresas de este tipo (u otros terceros) pueden desear acceder al motor de verificación/autenticación de modo que se puedan proporcionar dispositivos o símbolos de autenticación y ser usados a través de múltiples sitios (banco 1, banco 2, compañía de seguros 1, correduría 1, etc.), o el motor de verificación/autenticación puede referirse a usuarios que hayan sido verificados para tales empresas. Adicionalmente, se puede emitir un certificado digital que registre un cierto grado de confianza de la identidad del usuario (según se ha descrito con anterioridad), pero para realizar una transacción sensible, el usuario puede necesitar actualizar y mejorar el certificado digital a un nivel de certidumbre más alto en materia de evaluación de riesgos.

También es posible que el motor de verificación se use para verificar individuos o entidades a través de múltiples sitios web, posiblemente no relacionados. Por ejemplo, el Banco A no aceptará un símbolo del Banco B debido a que el Banco A no tiene conocimiento de cómo, y a qué nivel, fue verificado el usuario en el Banco B. El motor de verificación/autenticación podrá ofrecer la capacidad de dejar que los bancos establezcan esas reglas y niveles de riesgo de tal modo que se pueda usar el mismo símbolo a través de múltiples sitios. Esto elimina el síndrome de collar de símbolos. El motor podría verificar a los usuarios en tiempo real y proporcionar una estampilla/sello de aprobación o incluso distribuir un símbolo (por ejemplo, a través de un tercero) para que sea usado en varios sitios.

También es posible que el estado de aprobación de verificación tenga una fecha de caducidad. Por ejemplo, por defecto podría ser establecida en un año desde la fecha de aprobación. Si un vendedor quisiera aplicar una fecha de expiración diferente, ésta puede estar preestablecida.

Diversas organizaciones tienen diferentes objetivos y motivaciones, y sus modelos de negocio para la verificación son diferentes. Un modelo de negocio personalizado para una organización específica puede tener diferentes contenidos y estilos, y puede incorporar diferentes aspectos con énfasis diferente, enfocados a esa organización particular. El diseño de realizaciones del motor de verificación/autenticación que se ha descrito proporciona una solución única que cumple múltiples objetivos y motivaciones. Ésta es lo suficientemente flexible como para modificar y configurar soluciones que cumplan con los requisitos de negocio cambiantes y en curso. Ésta ofrece flexibilidad y facilidad de administración.

Usos de pequeño negocio

Realizaciones de la presente invención proporcionan también un sistema que puede verificar a un usuario en base a información comercial y de pequeño negocio y agregar datos en tiempo real a través de la web para proporcionar una solución de verificación dinámica. El sistema puede incluir cuestiones para los pequeños negocios, y respuestas a esas cuestiones, y las fuentes de datos acompañantes pueden estar identificadas y ser fácilmente disponibles de modo que se genere información suficiente que cumpla con el requisito de la seguridad. Por ejemplo, los archivos SBFE y SBX contienen suficientes datos para generar cuestiones y respuestas en base a muchos requisitos de

seguridad.

Usos de cuenta agregada

Realizaciones de la presente invención proporcionan una solución que proporciona acceso a la información a través de internet y la prueba de propiedad a través de la agregación de cuentas. Las cuentas agregadas, a las que se puede acceder por medio de un inicio único de sesión, son mostradas a otros para verificar la exactitud, autenticidad y titularidad. La intención es proporcionar una vista interior en una o más cuentas seleccionadas. Esto podría ser útil si un usuario desea dar a un asesor financiero acceso a todas sus cuentas en varias instituciones financieras.

Por ejemplo, un determinado servicio puede proporcionar la capacidad de ojear la información de una cuenta en tiempo real online. Esto no compromete la integridad de la cuenta ni divulga la ID del usuario ni la contraseña. Los usuarios de agregación existentes pueden identificar las cuentas que deseen, o están obligados a compartir con el motor de verificación/autenticación. Los usuarios de no agregación pueden necesitar completar y establecer ese servicio con anterioridad a que se complete el proceso de verificación si el vendedor ha seleccionado ésa como una de las fuentes desde la que extraer información.

Mientras que la agregación proporciona la capacidad de agregar cuentas y acceder a las mismas a través de un único inicio de sesión, esto no habilita normalmente al usuario a que permita que otra entidad eche un vistazo dentro de la cuenta seleccionada para proporcionar una prueba de titularidad. Éste es el porqué las aplicaciones de verificación de FSP existentes han dependido de transferencias de cuenta a cuenta, las cuales permiten que el usuario transfiera dinero en tiempo real a una nueva cuenta a efectos de financiación, estableciendo de ese modo una relación instantánea. Resulta deseable proporcionar la capacidad de mirar en una cuenta online sin requerir que el usuario revele su ID de usuario y su contraseña, o que haga un depósito o una transferencia de la cuenta. Ello permitiría un nivel de verificación más alto, sin comprometer la seguridad existente de la cuenta online.

Realizaciones permiten también la visualización en tiempo real sobre la información online existente (financiera, seguridad, médica, etc.) para el cliente potencial, pudiendo ser útil esta capacidad para mirar en cuentas online existentes para verificar la prueba de propiedad y la identificación, y la capacidad para capturar esa información para complementar el archivo. Por ejemplo, un servicio proporciona la capacidad de mirar en cuentas financieras online para proporcionar pruebas a efectos de verificación, y proporciona la oportunidad de capturar esa información. Sin embargo, la limitación de algunos sistemas actuales consiste en que éstos requieren que el usuario “opte por”. En otras palabras, el usuario puede ir a un único sitio web y establecer una única contraseña con el fin de agregar un número de cuentas bajo esa única contraseña (por ejemplo, Yodlee). Sin embargo, a efectos de verificar al usuario, el sitio web que agrega los datos extrae información desde las cuentas que son identificadas por el usuario para su verificación. En otras palabras, la información de cuenta disponible para su verificación es únicamente la información procedente de cuentas identificadas por el usuario a través de optar por. Por el contrario, con los sistemas descritos en la presente memoria, la información no se extrae necesariamente de las cuentas identificadas por el usuario, sino desde cuentas que están ya ligadas al usuario, tal como un informe crediticio. Por ejemplo, un usuario no identifica, u “opta por” el uso de información de identificación que se está extrayendo desde una compañía tal como Equifax.

De forma similar, incluso aunque una entidad particular (por ejemplo, un banco o un almacén) no opte por los sistemas de verificación/autenticación descritos, el motor puede aún tener suficiente información para verificar una cuenta, por ejemplo, la existencia de una tarjeta de crédito del Almacén A o una cuenta en el Banco B. En este ejemplo, los balances reales actuales pueden no ser parte de la información que se pueda extraer, a menos que el Almacén A o el Banco B opten por, y compartan, información con el sistema, pero la existencia de una cuenta puede ser verificada a través de una entidad de informes crediticios.

Algunos productos y servicios pueden requerir verificación más allá de las preguntas y respuestas básicas, o puede que no haya fuentes suficientes de las que obtener información. Por lo tanto, las cuentas que se agregan proporcionan un inicio único de sesión para el acceso a múltiples cuentas online en tiempo real.

Realizaciones del motor de verificación/autenticación descrito pueden desarrollar relaciones con proveedores actuales de agregación para obtener acceso a información con el fin de generar preguntas y respuestas. El sistema puede estar capacitado para capturar esta información, a través de limpieza de pantalla o de alimentación directa para una futura necesidad y/o para hacer crecer el archivo del usuario. Se prefiere que el sistema pueda identificar entre nuevos archivos (datos) y etiquetarlos como tales de modo que los archivos autoinformados, los archivos capturados, y los archivos proporcionados desde fuentes de SBFE y FSP no se mezclen y puedan ser identificados de manera correspondiente.

Acceso a niveles similares

El sistema puede permitir también que el usuario retorne en cualquier momento y pida acceso a soluciones, aplicaciones o servicios adicionales, mientras se requiere que éste conteste solamente aquellas cuestiones adicionales que sean aplicables a las nuevas transacciones. Además, un usuario puede acceder instantáneamente a soluciones que tengan requisitos de verificación similares a las de otros productos y servicios para los que el usuario haya sido ya verificado. Una vez aprobado para uno, por defecto, un usuario puede recibir la aprobación para otros a

niveles similares. El nivel de aprobación, y el acceso a aplicaciones asociadas al mismo, se basan en modelos de riesgo asignados a la aplicación.

El sistema puede otorgar también acceso a otros sistemas y datos que tengan asignado el mismo nivel de riesgo, minimizando el número de veces que un usuario debe ser verificado. Adicionalmente, si se establecen estándares para una industria (por ejemplo, entidades bancarias u otros FSPs), una vez verificado y asignado un símbolo de seguridad, la verificación puede ser utilizada en otras posiciones.

Éste se encuentra también capacitado para proporcionar a un usuario acceso a aplicaciones en diferentes mercados, es decir, a mercados de consumidores y de pequeños negocios, siempre que se alcance los niveles de seguridad apropiados. Por ejemplo, si un usuario ha sido verificado y se le ha concedido el acceso a determinadas aplicaciones, y éste desea obtener acceso a productos y servicios adicionales, el motor de verificación/autenticación puede diagnosticar dónde están los productos adicionales y mostrar preguntas y respuestas apropiadas en base a esas nuevas aplicaciones y al riesgo asociado a las mismas. De igual modo, si un usuario ha sido verificado para una aplicación, esa aprobación puede cubrir otros productos y servicios que estén disponibles para el usuario final (por ejemplo, en ese estante del supermercado o por debajo). Esto elimina la necesidad de obtener una verificación para esos servicios asignados con el mismo nivel de riesgo. Adicionalmente, si el usuario elige añadir servicios adicionales posteriormente, éste puede simplemente seguir adelante desde donde lo dejó.

Requisitos de seguimiento de auditoría y documentación

Puede resultar deseable proporcionar un seguimiento de auditoría de documentos, así como de los productos y servicios que se usaron para la verificación (o que se intentaron usar para la verificación), y de la información que, a preguntas reales, se pidieron. Esta información puede ser útil si el usuario solicita aplicaciones que requieran verificación adicional o re-verificación anual. Por ejemplo, el archivo para cada usuario que está siendo verificado, puede tener una banderola en ciertas cuestiones o tipos de información que puedan ser comprobados, dependiendo de si ese tipo de información fue o no usada en el proceso. El motor puede almacenar después todas las cuestiones de verificación preguntadas.

Con respecto a otros aspectos de la documentación:

- se pueden haber definido y documentado aplicaciones y nivel de riesgo asociado a las mismas;
- si se usa un tercero para la verificación, la documentación para usar el servicio puede ser proporcionada por el vendedor;
- la documentación impresa puede incluir
    - Notas de la Versión de Operaciones del Portal,
    - Guía de Instalación y Configuración,
    - Guía de Implementación, y
    - Guía de Operaciones.
- las soluciones pueden estar documentadas para el proceso de verificación manual.
- Los estándares de verificación pueden estar documentados de modo que las aplicaciones sepan para lo que se han construido, y de modo que las bases y fuentes de datos acompañantes puedan ser identificadas para que cumplan esos estándares.

Otros usos

La alternativa de servicio común minimiza la configuración y el mantenimiento, y proporciona compatibilidad a través de múltiples aplicaciones y de segmentos de mercado. El usuario puede aprovechar las mismas relaciones de datos y trabajar desde una arquitectura y estructura de archivo comunes. Éste puede aprovechar flujos de trabajo comunes, visualizar y generar informes, y lo que es más importante, usar una red de administración común (motor basado en reglas) para la configuración que cumpla las necesidades del mercado específico. Por ejemplo:

Mercado	Aplicación	Controladores
Proveedores de servicios financieros	Acceso a entidad bancaria, correduría, hipoteca, seguros, 401k, etc.	Reducir riesgo financiero, robo de identidad, cumplir directrices establecidas
Venta al por menor	Orden de entrada Servicio personalizado	Reducir fraude Incrementar beneficios (1:1 comercialización)

Mercado	Aplicación	Controladores
Proveedores de soluciones de pago/POS	Verificación de titular de tarjeta/comprobar autor con anterioridad al inicio de la transacción de pago	Reducir fraude, proteger identidad, minimizar gastos de transacción
Empleo/Control de Antecedentes/ Inmigración	Verificación de nacionalidad, estado legal, si las credenciales son legítimas (y no reutilizadas o las de una persona fallecida), antecedentes penales, monitorización	Cumplir requisitos legales (es decir, medidas SB 529), mejorar prácticas de contratación, monitorizar empleados
Empresa/IT Proveedores de Solución de Contraseña	Acceso a Intranet, Extranet, Aplicaciones Corporativas, contraseña/reinicios de PIN	Incrementar la seguridad, reducir costes
Internet	Establecer credenciales, confirmar identidad	Reducir riesgo financiero, robo de identidad, fraude
Asistencia sanitaria	Acceder a información de pacientes, autorizar prescripción de medicamentos, autorizar pagos de seguros	Proteger privacidad personal, cumplir requisitos HIPPA, reducir fraude y robo de identidad
Gobierno/Ejército	Acceder a información guardada, verificación con anterioridad al reparto de beneficios	Incrementar seguridad, reducir costes
Organización de Beneficencia	Validar receptor con anterioridad a la distribución de beneficios	Reducir fraude, malversación de fondos

En general, varias realizaciones descritas en la presente memoria son útiles para verificación del consumidor, verificación de la pequeña empresa (para verificar el principio otorgante de la pequeña empresa), verificación de empleado de negocio (para confirmar la identidad de un usuario como empleado de la empresa), verificación comercial (para establecer la confirmación de empresas comerciales y también de empleados); verificación de dispositivos (para validar que el dispositivo del otro extremo es de hecho propiedad de la persona o la empresa), así como todas las formas de autenticación similares.

Las realizaciones pueden ser usadas también para servicios de inicio rápido, que usen datos para el inicio rápido y servicios de pago de facturas previamente generadas y agregación de cuentas. Específicamente, algunas realizaciones proporcionan la capacidad de generar información para acelerar el proceso de establecimiento de cuenta para agregación de cuentas. El sistema puede verificar el usuario final y permitir a continuación que el usuario seleccione las cuentas que desea agregar. La generación previa de información de cuenta a partir de, por ejemplo, una base de datos Equifax en un proceso de establecimiento de agregación, cuenta por cuenta, puede ser un servicio con un valioso ahorro de tiempo.

Se pueden usar también las realizaciones para verificación en tiempo real, lo que facilita la capacidad de que un usuario final proporcione la prueba de propiedad que le habilita para introducir información para una cuenta online existente. Estas credenciales se hacen pasar a continuación al sitio aplicable donde se garantice el acceso y los datos que residen en ese sitio pueden ser acumulados para ofrecer preguntas como parte del proceso de verificación online. Los datos y la información de credencial de inicio de sesión del sitio web pueden ser también almacenados para su uso posterior.

Se pueden usar también realizaciones para verificación de red social, es decir, para verificar a los usuarios de modo que los usuarios de redes sociales online, es decir MySpace.com, no puedan pretender ser otros. Esto puede ayudar a minimizar los predadores online.

Otro uso potencial para varias realizaciones de los sistemas descritos son para tarjetas de débito o de prepago, tales como las emitidas por la Cruz Roja u otras entidades en situaciones de emergencia (por ejemplo, para ayuda en desastres naturales). Las tarjetas son emitidas con frecuencia a una persona o familia particular, y por lo tanto, confirmar la identidad de esa persona o familia con anterioridad a aceptar la tarjeta puede ayudar a evitar el fraude. La información de identificación podría ser cualquier información práctica, dependiendo del canal en el que se esté

usando la tarjeta. Por ejemplo, si solamente está disponible una interacción de pantalla limitada, la información requerida podría ser "¿Fue emitida esta tarjeta en Alabama?" y el usuario podría responder con una contestación de "sí/no". Si está disponible una mayor interacción con la pantalla, se puede sugerir al usuario que introduzca determinados dígitos de su número de seguridad social, número de reclamación, código postal, etcétera. La Cruz Roja o la entidad emisora puede identificar la información necesaria (o nivel de riesgo) y a partir de qué fuentes (por ejemplo, la fuente en este ejemplo podría ser la propia base de datos de la Cruz Roja, aunque son posibles otras fuentes y podrían ser llamadas si fuera necesario en base al nivel de riesgo) con anterioridad a la aceptación de la tarjeta.

Otras opciones son para tarjetas de regalo que tengan una cantidad prepagada ya asociada a las mismas (por ejemplo, tarjetas de almacenes, tarjetas de restaurantes, etc.). Si tales tarjetas se pierden, pueden ser usadas por alguien distinto del destinatario previsto. Por consiguiente, las tarjetas podrían estar ligadas a un sistema de verificación/autenticación que requiera que se introduzca determinada información con anterioridad a aceptar la tarjeta. Las realizaciones descritas son igualmente aplicables a otras opciones tales como cupones de alimentos u otros cupones emitidos por el gobierno (o de otro modo) a efectos de ayudar a impedir el fraude.

Se pueden usar también realizaciones para una red de verificación que permita que los usuarios intercambien información anónimamente a efectos de verificación. Esto podría permitir a los contribuyentes realizar la verificación intercambiando información en tiempo real, mientras que no se comprometen sus acuerdos con sus usuarios finales (para no compartir información con otros según esté establecido en sus contratos de cuentas conforme al acta de Gramm-Leach-Bliley).

Se pueden usar también realizaciones para verificación de pagos. Con anterioridad al inicio del pago (por ejemplo, mediante cheque, POS o tarjeta de crédito), el sistema puede ser usado para verificar la persona a efectos de establecer la propiedad del instrumento de pago. En resumen, la naturaleza basada en reglas del sistema es una solución dinámica que permite al vendedor (o al usuario inicial del servicio de motor de verificación/autenticación) que establezca el tipo de cuestiones y las fuentes de datos que desea incorporar en el proceso de verificación. El motor puede estar establecido para que se cumplan las necesidades individuales del vendedor y que coincidan las necesidades de seguridad de esas aplicaciones a las que se accede.

Se describen usos adicionales en cada título que sigue. Se puede acceder a cualquiera de esos usos (descritos con anterioridad y en lo que sigue) a través de cualquiera de los canales descritos en lo que antecede (incluyendo uno o más de internet, intranet, e-mail, mensajería instantánea u otros canales tal como uno o más sistemas de telefonía o de voz, teléfonos celulares, ATM, kiosco, escáner, punto de terminal de venta, sistemas móviles, blackberry, dispositivos portátiles, PC de bolsillo, dispositivos inalámbricos). Éstos son solamente ejemplos, y se comprenderá que otros canales son posibles y se consideran dentro del alcance de esta invención.

Uso de FFIEC

La verificación es algo más que la confirmación de la identidad de un individuo, un negocio, o un empleado de un negocio, a efectos de abrir una cuenta. Se pueden usar varias realizaciones de los motores de verificación/ autenticación que se han descrito, para autenticación multiforma y para identificar individuos con anterioridad a iniciar o aceptar un pago o como parte de un proceso de contratación de empleo.

Para fomentar que los FSPs incrementen su seguridad, el Consejo de Examen de Instituciones Financieras Federales (FFIEC) publicó directrices para la autenticación. La guía refleja que la verificación está asociada a la autenticación, pero es un proceso separado. Éste instruye a los FSPs para que usen métodos y fuentes de datos confiables, específicamente de terceras partes, para abrir nuevas cuentas. La sección de "Técnicas de Verificación del Cliente" del documento de "Autenticación en un Entorno de Banca por Internet" del FFIEC, apela a lo siguiente:

- Verificación Positiva – asegurar que los datos proporcionados por un usuario coinciden con los datos procedentes de un tercero de confianza. Verificar la identidad por medio de una interacción de pregunta y respuesta. Se hacen preguntas más específicas y detalladas, incrementando con ello la certidumbre de la verificación positiva.

- Verificación Lógica – asegura que los datos proporcionados son precisos y compatibles. El código postal y la zona postal coinciden con la dirección, etc.

- Verificación Negativa – comparar credenciales contra bases de datos de fraude para asegurarse de que los datos no están vinculados a una actividad fraudulenta.

Uso de POS

Existe también una oportunidad importante para usar los motores de verificación/autenticación descritos dentro del punto de venta (POS) y del área de pagos. Existen cuatro tipos básicos de tarjetas: débito, crédito, inteligente y prepago. Existen tres tipos principales de métodos de autenticación: voz, captura electrónica de datos, y terminales virtuales. La autenticación es el área en que la realización de la presente invención puede añadir un valor significativo al proceso de iniciación del pago. Durante una transacción o un pago, se presenta una tarjeta o un

cheque para el pago, virtual o físico. La información es captada desde la tarjeta o el cheque, mediante escaneo, tecleado, introducción de clave o barrido, y comienza el proceso de captura electrónica de datos (EDC).

Los datos capturados se presentan a un procesador y se devuelve una decisión de pago o no pago. Mientras que éste comprueba la validez básica, no confirma que la tarjeta o el cheque pertenezcan al individuo. Incluso cuando se requiere un PIN o una firma para completar la transacción, esto no valida aún a la persona que presenta el instrumento de pago. Puesto que los consumidores demandan cada vez más opciones de auto-servicio de comprobación y realizan más compras virtualmente, se requerirán medias de seguridad adicionales. Los esfuerzos por minimizar el fraude han sido enfocados, sin embargo, a la detección en el servidor final. Las soluciones tratan de detectar un comportamiento anormal y una actividad inusual. Si la presentación de credenciales tuviera que ocurrir en la interfaz delantera, se podría eliminar una gran proporción del fraude. De hecho, si el usuario no pudiera contestar la pregunta, la transacción no sería enviada. El diseño de motor de verificación/autenticación es tal que el usuario, o el negocio, podrán determinar el umbral de la cantidad de dólares con el que están cómodos y solamente requerirán la verificación sobre compras por encima de esa cantidad. El emisor de la tarjeta puede incluso establecer el tipo de preguntas en base a la cantidad de dólares, asignando el riesgo de manera correspondiente. Tener datos dinámicos y la capacidad de asignar niveles de riesgo asegura que un comprador legítimo tenga una mejor oportunidad de completar la transacción y reciba la seguridad de que su tarjeta no será usada para transacciones fraudulentas.

Este tipo de flexibilidad beneficiará a los emisores de tarjetas, debido especialmente a que el mercado de las tarjetas se ha vuelto muy competitivo. Por ejemplo, algunos emisores de tarjetas tienen una política de “fiabilidad cero” para tarjetas de crédito de pequeños negocios. Esto cubre compras hechas en almacenes, por teléfono, u online. En consecuencia, los motores de verificación/autenticación descritos pueden ser particularmente útiles en esta área. Puesto que el motor es dinámico y no usa solamente datos de informes crediticios del consumidor, no puede resultar comprometido.

Uso de NACHA

La Asociación Nacional de la Cámara de Compensación Automatizada (NACHA) planea probar una nueva solución de pago electrónico que posicione a las instituciones financieras para actuar como intermediarios para transacciones online. Esto es similar a los modelos de pago de PayPal y Verificados por Visa. La diferencia es que, con el PayPal, el usuario final debe presentar información de cuenta personal al PayPal con anterioridad al inicio de una transacción.

Los modelos de NACHA y Verificado por Visa, añaden una contraseña, y en algunos casos un mensaje personal, al proceso de transacción. El titular de la tarjeta introduce la información de su tarjeta en el momento del pago. Se presenta de retorno un recibo con el mensaje personal al titular de la tarjea para que confirme que está en un sitio auténtico. Si es así, el usuario introduce la contraseña y la transacción queda completada. El defecto de este sistema ha sido que la transacción es redirigida a un banco online durante la transacción. Esto obliga al comerciante a ceder el control de la transacción a otra entidad. Esto puede confundir al usuario y ha provocado que los usuarios abandonen la compra antes de que se complete, causando una pérdida de ventas al comerciante.

El motor de verificación/autenticación que se ha descrito podría eliminar todo esto mediante la verificación del usuario en el momento de introducción de la información de tarjeta. La verificación ocurriría en el sitio del comerciante sin ninguna redirección, y ofrecerá mejor seguridad que las opciones anteriores. Puesto que es dinámica, el tipo de cuestión podría ser emparejado con el tipo de transacción y/o con el importe. Esto no requiere que el usuario recuerde una contraseña adicional, y no compromete el flujo de la transacción al que, con frecuencia, el usuario final ha estado acostumbrado.

Uso de dispositivo móvil

Existen nuevas soluciones de seguridad aportadas al mercado a diario. Una que ha cosechado alguna atención últimamente es el fuera de banda (OOB). El OOB es una solución multifactor que se usa junto con dispositivos habitualmente disponibles, como los teléfonos celulares. Esto permite comunicación de dos vías, a través de mensajería de texto o de voz. Puesto que opera fuera de banda, está separado del canal principal (es decir, internet). Éste confirma la identidad del usuario y la validez de la transacción, e impide ataques de solapamiento de identidad.

El fuera de banda tiene una dependencia sobre verificación del dispositivo al usuario. Esta alternativa requiere que el usuario final introduzca en primer lugar información del dispositivo durante el registro. También acepta a ciegas que el número de ese dispositivo pertenece a ese usuario. Lo mejor que los proveedores de la solución de OOB pueden ofrecer actualmente, consiste en comparar los datos del usuario con lo que se conoce acerca de ese dispositivo, por ejemplo, la proximidad geográfica o una combinación de código de zona y de intercambio en relación con un código postal.

Esto, sin embargo, es un débil intento en la detección de fraude. El OOB ha sido usado por compañías para verificar nuevos clientes y titulares de cuentas existentes, y para detectar cuándo se sospecha de fraude o de

comportamiento anormal. También se usa para transacciones específicas como pagos, telegramas y transferencias. Se pueden establecer reglas para determinar cuándo se debe aplicar OOB. Esto puede ser establecido mediante un tipo de transacción o un importe. Esto es compatible con el motor de verificación/autenticación que se ha descrito. Una diferencia principal consiste en que los sistemas de motor de verificación/autenticación pueden verificar que el dispositivo pertenezca al individuo o al pequeño negocio antes de que se envíe el código de acceso. Ésta es la pieza faltante en todas las soluciones de OOB que se están vendiendo actualmente en el mercado. Sin que el dispositivo verifique al usuario, no hay manera de confiar completamente en que el receptor del código de acceso sea la persona a la que está destinado el código.

Uso del empleo

Los legisladores esperan que se promulguen ciertas leyes de inmigración en un próximo futuro. Una está relacionada con la denegación de beneficios públicos a adultos que residan en el país ilegalmente, y a exigir a los contratistas públicos que contraten solamente trabajadores que estén legalmente en el país. Otras leyes podrán requerir que los empleados verifiquen el estado legal y la admisibilidad de de empleados, lo que significa que los empresarios tendrán que verificar si la documentación presentada por los trabajadores es válida o no.

La Administración de la Seguridad Social (SSA) ofrece un servicio gratis. El Sistema de Verificación de Empleados (EVS), que es una manera de verificar los números de seguridad social (SSN) de los empleados. Los usuarios pueden llamar a un número gratis y comprobar hasta cinco SSNs por llamada. Éstos pueden presentar también hasta 50 nombres y los SSNs en la oficina de Seguridad Social local, sobre papel o mediante un listado en cinta magnética. Existen miles de empresarios actualmente registrados para este servicio, y en 2004 solamente, el EVS atendió más de un millón de llamadas. En 2005, la SSA desplegó una aplicación online denominada Servicio de Verificación del Número de la Seguridad Social (SSNVS). Esta solución verifica nombres de empleados y SSNs a través de una interfaz de usuario gráfica de web. En 2005, la SSA procesó 25,7 millones de verificaciones para más de 12.000 empresarios.

La SSA interactúa también con el sistema Piloto Básico del Departamento de Seguridad Nacional (DHS). Éste ayuda a empresarios con la confirmación de idoneidad de empleo para empleados recién contratados. Éste verifica un SSN, ciudadanía de U.S., y situación de trabajo actual, confirmando con ello la autorización de trabajo. El DHS puede confirmar también la autorización de trabajo actual para todos los no ciudadanos. El total combinado de transacciones de EVS, SSNVS y de Piloto Básico en 2004 fue de aproximadamente 67 millones.

Sin embargo, es más probable que las grandes compañías usen estos sistemas que las compañías más pequeñas. Puesto que los costes son fijos, el coste por uso se reduce según se incrementa el número de verificaciones por compañía. Muchos pequeños negocios no tienen conocimiento de estos recursos o no saben cómo o dónde acceder a los mismos. Usando el motor de verificación/autenticación que se ha descrito, se podría hacer que estos sistemas estuvieran disponibles como servicio web y que proporcionen acceso universal a pequeños negocios. Como servicio web, el sistema podría también distribuir e integrar la solución en aplicaciones de terceros, es decir, pago de nóminas, contabilidad y gestión bancaria. El diseño permite que el verificador elija qué soluciones coinciden con las necesidades de su negocio. El sistema puede ser desplegado en cualquier parte, e incluido en aplicaciones que se precisen para hacer que funcione una pequeña empresa o una empresa de cualquier tamaño (pago de nóminas, gestión bancaria online, contabilidad, etc.).

Uso de verificación de antecedentes

Que alguien pueda ser contratado o no para un trabajo o promocionado puede depender de la información revelada en una verificación de antecedentes. Los solicitantes de trabajo y los empleados existentes pueden ser preguntados o requeridos para que presenten una verificación de antecedentes. Con el mayor enfoque sobre seguridad nacional, el número de verificaciones de antecedentes de empleo que se está realizando se ha incrementado anualmente, así como las razones para realizarlas. Ahora están disponibles soluciones que presentan actualizaciones automáticas. Según avanza la tecnología de búsqueda y más registros federales, estatales y locales son digitalizados, la detección continua podría convertirse en una mayor oportunidad de mercado. El motor de verificación/autenticación que se ha descrito es una herramienta que los empresarios podrán usar para minimizar el riesgo financiero y legal. El motor de verificación/autenticación y su capacidad para agregar datos desde fuentes de datos nuevas y existentes, podría ser usado en relación con ofertas de verificación de antecedentes. También podría ser usado para enlazar verificación de empleo y verificaciones y actualizaciones de antecedentes en soluciones de contratación electrónica.

La mayor parte de los segmentos de mercado tendrán principalmente las mismas necesidades y características. La principal diferencia en el diseño del motor de verificación/autenticación será el tipo de transacción y el riesgo asociado a la misma. Por ejemplo, los tipos de transacción podrán incluir lo siguiente:

- Verificación de identidad con anterioridad a la apertura de una cuenta
- Prueba de identidad con anterioridad al inicio de un pago – POS o tarjeta de crédito

- Confirmación de idoneidad de trabajo y/o estado de inmigración
- Reconocimiento de propiedad del dispositivo móvil.

Una diferencia entre los segmentos podrá ser que los clientes de pago y de apertura de cuenta podrá ser que los clientes estarán centrados en la transacción mientras que el empleo y el dispositivo estarán centrados en la información. Es importante apreciar esas diferencias puesto que las mismas podrán tener un impacto sobre los canales móviles/interactivos que estén integrados con el motor de verificación/autenticación y con sus tecnologías acompañantes.

Desde la perspectiva de un cliente, los consumidores esperan que las compañías con las que interactúan protejan no solo sus datos, sino también su identidad. La investigación ha indicado que los usuarios no desean usar símbolos y otros dispositivos para autenticarse a sí mismos en un sitio web. El método preferido es la autenticación basada en el reconocimiento. Este método ofrece una capa de seguridad añadida, así como la capacidad de proporcionar funcionalidad de auto-servicio, tal como reseteo de contraseña. Un objetivo de varias realizaciones de la presente invención consiste en proporcionar una plataforma de utilidad que esté disponible para todos los productos y aplicaciones, permitiéndoles que proporcionen soluciones de verificación a múltiples segmentos de mercado y a sus clientes a través de múltiples canales. Además de hacer que los datos sean más accesibles, esto permitirá a los usuarios personalizar la solución para cumplir con las necesidades de sus mercados individuales.

Se pueden realizar cambios y modificaciones, adiciones y supresiones en los sistemas y métodos definidos con anterioridad y representados en los dibujos sin apartarse del alcance de la invención y de las reivindicaciones que siguen.

REIVINDICACIONES

1.- Un método de controlar el acceso por un usuario a sistemas de tecnología de información de vendedor online usando un motor de verificación/autenticación, que comprende:

(a) recibir una pregunta desde un sistema del vendedor para verificar a un usuario particular para una transacción particular, en donde el vendedor ha asignado a la transacción particular un nivel de riesgo;

(b) en donde el vendedor ha especificado un nivel de verificación apropiado que cumpla con el nivel de riesgo asociado, que comprende especificar una pluralidad de fuentes de datos que contienen información acerca del usuario;

(c) preguntar al usuario, usando cuestiones generadas en base a datos procedentes de al menos dos de las fuentes de datos

(d) determinar el grado en que el usuario contesta correctamente a las cuestiones, y

(e) determinar si se concede o se deniega el acceso por el usuario a los sistemas de tecnología de información del vendedor en base al grado en que el usuario conteste correctamente a las cuestiones,

caracterizado además por:

(f) el motor de verificación/autenticación está habilitado a través de múltiples canales;

(g) en donde el vendedor ha establecido un nivel de riesgo en base al canal que está siendo usado por el usuario;

(h) generar un nivel de confianza y/o una puntuación de la identidad del usuario en base a las respuestas del usuario a las cuestiones, y

(i) proporcionar el nivel de confianza y/o la puntuación al sistema del vendedor, que está configurado para determinar si conceder o denegar el acceso por parte del usuario a los sistemas de tecnología de información del vendedor en base al nivel de confianza proporcionado.

2.- Un método según la reivindicación 1, en donde el vendedor identifica la forma en que se preguntan las cuestiones, dependiendo del canal que se esté usando.

3.- Un método según la reivindicación 1 o la reivindicación 2, en donde el vendedor ha especificado un nivel de puntuación para acomodar los errores.

4.- Un método según cualquiera de las reivindicaciones 1 a 3, en donde fabricantes de símbolos de seguridad pueden integrarse con el motor de verificación/autenticación para distribuir dispositivos de seguridad solamente a usuarios que alcancen un determinado nivel de confianza.

5.- Un método según las reivindicaciones 1 a 4, en donde el motor de verificación/autenticación autoriza la emisión de un certificado digital a un usuario una vez que el usuario completa la verificación.

6.- Un método según cualquiera de las reivindicaciones 1 a 5, en donde los múltiples canales incluyen uno o más de entre internet, una intranet, e-mail, mensajería instantánea, sistemas de telefonía o de voz, teléfonos celulares, ATM, kiosco, escáner, punto de terminal de ventas, sistema móvil, dispositivo portable, PC de bolsillo, o un dispositivo inalámbrico.

7.- Un método según cualquiera de las reivindicaciones 1 a 6, en donde el motor de verificación/autenticación proporciona al vendedor una serie de selecciones y opciones de puntuación en relación con niveles de riesgo, fuentes de datos, precios y canales.

8.- Un método según cualquiera de las reivindicaciones 1 a 7, en donde, una vez que se ha concedido el acceso, un usuario puede volver al sistema de tecnología de información del vendedor y solicitar acceso a transacciones adicionales y responder solamente a las cuestiones que sean aplicables al nivel de riesgo asignado de la transacción adicional.

9.- Un método según cualquiera de las reivindicaciones 1 a 8, en donde el método usa un primer canal para comunicación con el usuario, y en donde, si el primer canal falla, usa por defecto un canal manual alternativo.

10.- Un método según una cualquiera de las reivindicaciones 1 a 9, que comprende además verificar que un dispositivo pertenece a un determinado individuo o negocio antes de que se envíe un código de acceso.

11.- Un método según una cualquiera de las reivindicaciones 1 a 10, en donde las fuentes de datos comprenden una única base de datos entremezclada que tiene información compilada procedente de varias fuentes de datos en una

posición.

12.- Un motor de verificación/autenticación para controlar la comunicación y el acceso por parte de un usuario a sistemas de tecnología de información de vendedor online, en donde el motor de verificación/autenticación está dispuesto para operar mediante el método de cualquiera de las reivindicaciones 1 a 11.

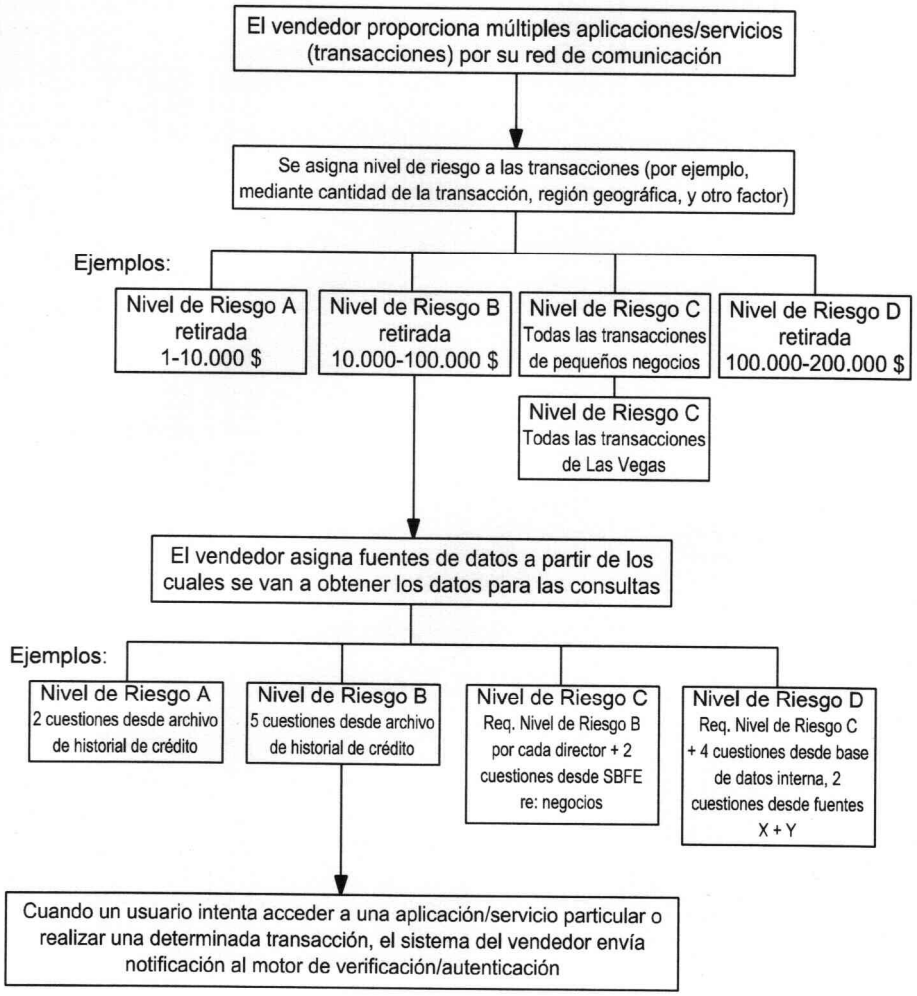
El vendedor proporciona múltiples aplicaciones/servicios (transacciones) por su red de comunicación
Se asigna nivel de riesgo a las transacciones (por ejemplo, mediante cantidad de la transacción, región geográfica, y otro factor)
Ejemplos:
Nivel de Riesgo A retirada 1-10.000 $
Nivel de Riesgo B retirada 10.000-100.000 $
Nivel de Riesgo C Todas las transacciones de pequeños negocios
Nivel de Riesgo D retirada 100.000-200.000 $
Nivel de Riesgo C Todas las transacciones de Las Vegas
El vendedor asigna fuentes de datos a partir de los cuales se van a obtener los datos para las consultas
Ejemplos:
Nivel de Riesgo A 2 cuestiones desde archivo de historial de crédito
Nivel de Riesgo B 5 cuestiones desde archivo de historial de crédito
Nivel de Riesgo C Req. Nivel de Riesgo B por cada director + 2 cuestiones desde SBFE re: negocios
Nivel de Riesgo D Req. Nivel de Riesgo C + 4 cuestiones desde base de datos interna, 2 cuestiones desde fuentes X + Y
Cuando un usuario intenta acceder a una aplicación/servicio particular o realizar una determinada transacción, el sistema del vendedor envía notificación al motor de verificación/autenticación

FIG. 1

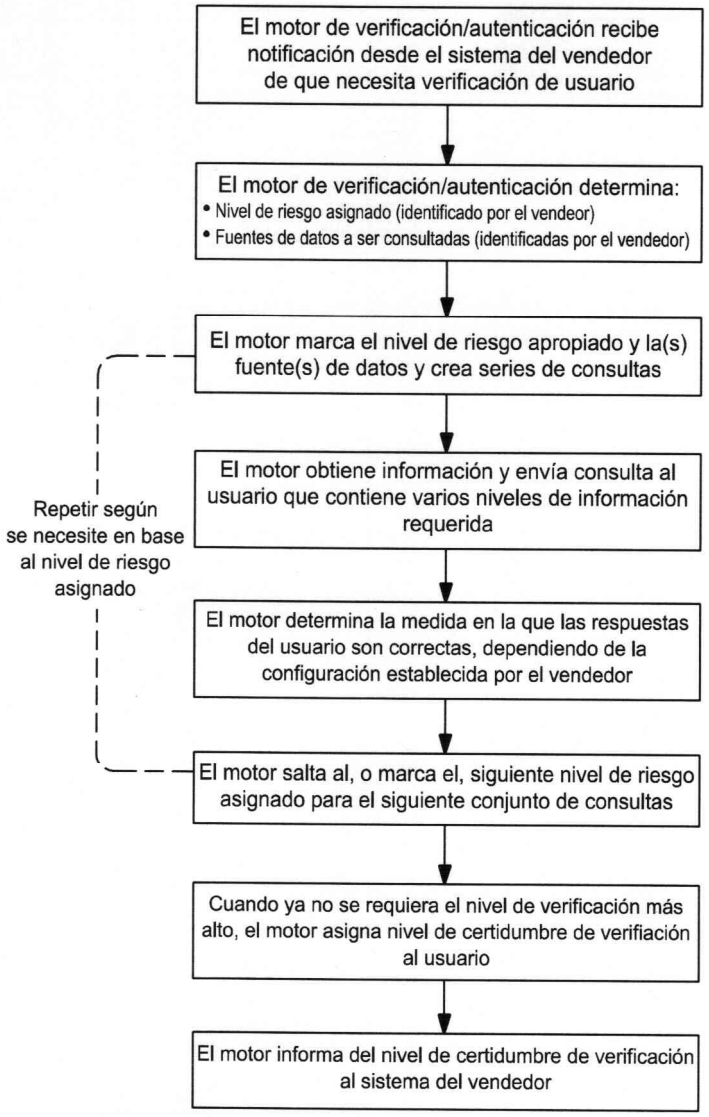
El motor de verificación/autenticación recibe notificación desde el sistema del vendedor de que necesita verificación de usuario
El motor de verificación/autenticación determina:
• Nivel de riesgo asignado (identificado por el vendeor)
• Fuentes de datos a ser consultadas (identificadas por el vendedor)
El motor marca el nivel de riesgo apropiado y la(s) fuente(s) de datos y crea series de consultas
El motor obtiene información y envía consulta al usuario que contiene varios niveles de información requerida
El motor determina la medida en la que las respuestas del usuario son correctas, dependiendo de la configuración establecida por el vendedor
El motor salta al, o marca el, siguiente nivel de riesgo asignado para el siguiente conjunto de consultas
Cuando ya no se requiera el nivel de verificación más alto, el motor asigna nivel de certidumbre de verifiación al usuario
El motor informa del nivel de certidumbre de verificación al sistema del vendedor
Repetir según se necesite en base al nivel de riesgo asignado

FIG. 2

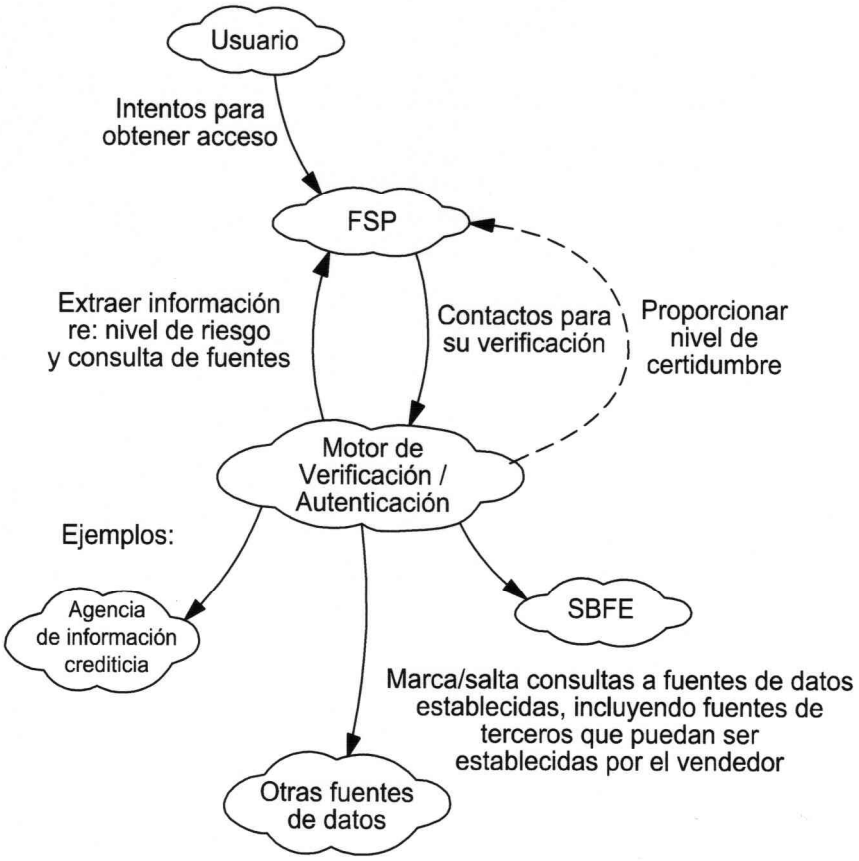
Usuario
Intentos para obtener acceso
FSP
Extraer información re: nivel de riesgo y consulta de fuentes
Contactos para su verificación
Proporcionar nivel de certidumbre
Motor de Verificación / Autenticación
Ejemplos:
Agencia de información crediticia
SBFE
Marca/salta consultas a fuentes de datos establecidas, incluyendo fuentes de terceros que puedan ser establecidas por el vendedor
Otras fuentes de datos

FIG. 3