De la necesidad a la oportunidad: qué manera se posicionan los operadores de redes móviles para beneficiarse de las identidades digitales de confianza

gemalto
security to be free

Índice

1. La identidad en la era de la transformación digital

La transformación digital ya está en marcha. La omnipresencia de los teléfonos móviles, en particular, está impulsando a las empresas y a las organizaciones a repensar básicamente cómo pueden llegar a sus clientes y diseñar sus servicios.

La escala de este cambio es colosal. En 2017, la industria móvil mundial dio la bienvenida a su suscriptor móvil único número 5,000 millones, lo que significa que más de dos tercios de la población del planeta están ahora conectados a un servicio móvil1. La manera en que accedemos a Internet está cambiando del mismo modo. En 2018, se estima que el 73% del uso de Internet se originará en un teléfono móvil2.

En 2018, alrededor del

73% **del uso de Internet se originará en un teléfono móvil**

Al igual que con todas las demás industrias, los operadores de redes móviles (MNO) deben adaptarse a esta atmósfera que cambia rápidamente. Están lidiando con la necesidad de reclamar territorio en el mercado digital y proporcionar servicios cada vez más innovadores para satisfacer la creciente demanda de sus clientes.

Mientras reorganizan su modelo de negocio, los MNO se enfrentan simultáneamente a la necesidad de optimizar sus operaciones y adquirir nuevos clientes. En respuesta a estos diversos desafíos, los MNO pueden comenzar por cambiar la forma en que administran la identidad de sus clientes. Los siguientes impulsores de cambio revelan tanto la necesidad de identidades digitales de confianza como las oportunidades inherentes a la oferta de dichas identidades.

1.1 La necesidad del consumidor en cuanto a conveniencia y seguridad

Las personas se están acostumbrando rápidamente a experiencias digitales fluidas y agradables, y han comenzado a esperar un acceso simple y rápido a una amplia gama de servicios. De hecho, el 66% de los usuarios dice que realizaría aún más transacciones en su teléfono[3]

La conveniencia y la rentabilidad del acceso móvil han trasladado nuestros procedimientos y nuestras transacciones más importantes a nuestro teléfono inteligente. Sin embargo, este cambio se acompaña de una necesidad pronunciada de una verificación de identidad segura. El 43% de los usuarios teme el fraude, el phishing, el hackeo y el robo de su información personal (después de perder el teléfono móvil y sus datos, y de quedarse sin batería)[3].

En resumen, la protección contra el fraude y los métodos de seguridad digital deben seguir el ritmo del aumento de la conveniencia, para que los clientes puedan sentirse seguros al acceder a una nueva generación de servicios.

[1] GSMA Intelligence (2017)
[2] Informe Mobile Forecast de Zenith (2017)
[3] Encuesta de GTO 2017 1,300 entrevistas realizadas en Brasil, el Reino Unido, Sudáfrica, Singapur, los Países Bajos y los EE.UU.

1.2 Iniciativas y reglamentaciones gubernamentales

En todo el mundo, los gobiernos están aprobando leyes para proteger a sus ciudadanos de estafas, fraude y delitos. La verificación de identidad está al frente y en el centro, ya que los delitos como el lavado de dinero y la actividad terrorista, generalmente, involucran identidades falsas o robadas, y cuentas vinculadas a identidades falsas o ausentes.

En respuesta, las regulaciones como Conozca a su Cliente y el registro de la tarjeta SIM requieren que las empresas tengan procesos más rigurosos y sistemas seguros para verificar la identidad de sus clientes. Esto, sin duda, refleja el interés de los MNO, ya que el fraude de suscripción representa el 20% de todos los fraudes de telecomunicaciones[4].

Otras regulaciones tienen como objetivo optimizar y fomentar la compatibilidad entre sistemas y agencias. eIDAS, por ejemplo, está allanando el camino para el mercado europeo digital único, con identidades digitales nacionales aceptadas a través de las fronteras. Las nuevas tecnologías y los nuevos estándares no solo ayudan a multiplicar las iniciativas gubernamentales, como los esquemas de identidad nacional y las fronteras inteligentes, sino que también ayudan a las empresas privadas a acelerar sus propias transformaciones digitales.

El fraude de suscripción representa el

20%

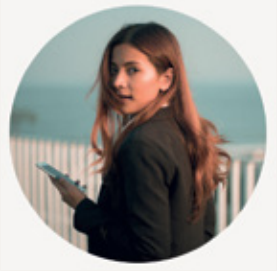
de todo el **fraude** de telecomunicaciones

¿QUÉ ES UNA IDENTIDAD DIGITAL DE CONFIANZA?

Una identidad digital es el equivalente en Internet o en la red de la identidad real de una persona. Se utiliza para la identificación al acceder a un servicio o al realizar una transacción en una computadora, un teléfono celular u otro dispositivo personal.

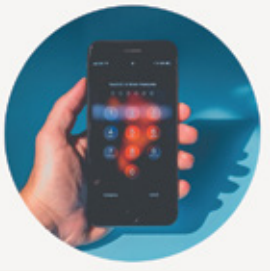
Incluye una colección de atributos de identidad capturados y almacenados electrónicamente, que distinguen a una persona dentro de un contexto dado.

Existe una variedad de atributos que se puede usar, como:



Datos biográficos
(es decir, nombre, edad, género, dirección)

Datos biométricos
(es decir, huellas dactilares, escaneo del iris, impresiones de la mano)



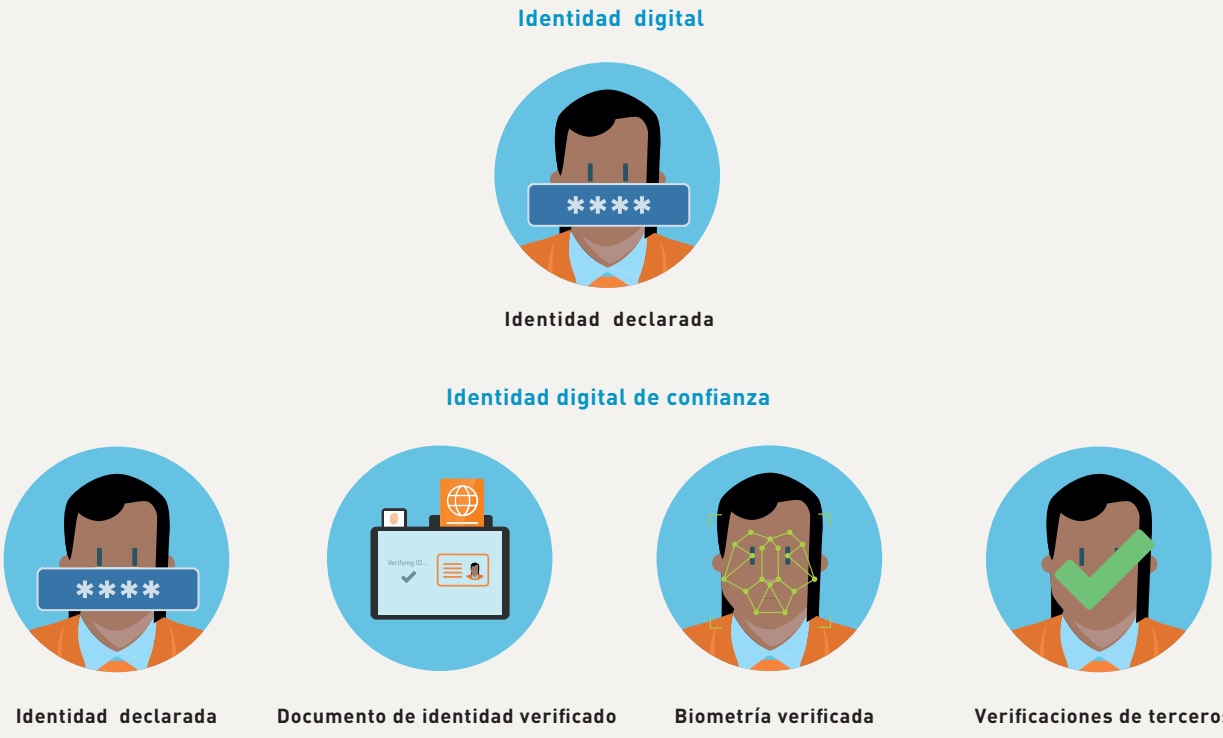
Un objeto que posee la persona
(es decir, un teléfono móvil, un token específico)

Una identidad digital básica puede ser tan simple como una combinación de nombre de usuario y contraseña. Las identidades digitales aumentan la seguridad con el número de atributos agregados.

Las identidades digitales de confianza se crean cuando la información provista se ha verificado o cuando se ha comprobado su autenticidad.

[4] http://www.cfca.org/fraudlosssurvey

IDENTIDAD DIGITAL VS. IDENTIDAD DIGITAL DE CONFIANZA



1.3 Un cambio hacia las identidades digitales de confianza

Una persona promedio ya posee múltiples identidades digitales que se utilizan para acceder a una gama de servicios diferentes. En muchos foros, como los de medios y entretenimiento, estas identidades no necesariamente tienen que reflejar la identidad real de la persona, se puede usar un seudónimo. Sin embargo, a medida que cada vez más servicios importantes se trasladan al canal en línea, como el pago de impuestos o el voto en elecciones, es fundamental que las identidades digitales reflejen identidades reales y verificables.

Cada vez más, numerosas empresas y organizaciones gubernamentales de todo el mundo están adoptando las identidades digitales de confianza como una forma segura de verificar la identidad de sus empleados/clientes/ciudadanos.
empleados/clientes/ciudadanos. A diferencia de una combinación simple de nombre de usuario y contraseña, por ejemplo, se crea una identidad digital de confianza con atributos verificados (como documentos de identidad o datos biométricos verificados), lo que proporciona así un vínculo certificable entre un individuo y su identidad digital. Estos atributos también pueden incluir una verificación de referencia cruzada con terceros, como las bases de datos gubernamentales, los números de tarjetas de crédito, etc.
Los operadores de redes móviles no solo logran este cambio, sino que también tienen un papel importante en la ayuda a otros sectores a hacer el cambio.

2. ¿De qué manera las identidades digitales de confianza pueden cambiar el juego para los MNO?

2.1 Operaciones optimizadas

Las identidades digitales de confianza hacen posible que los MNO simplifiquen y digitalicen sus flujos de trabajo a través de la reducción de la entrada manual, de las fotocopias y del papeleo que puede tardar varios días en procesarse. Esto no solo reduce los costos operativos, sino que también beneficia a los clientes mediante la drástica disminución del tiempo que lleva subscribirse y la activación instantánea de varios servicios.

2.2 Bases de datos de clientes más consistentes

Al crear una identidad digital, la información personal se extrae y se completa automáticamente en el CRM del cliente. Esto crea eficiencias en múltiples frentes. Los representantes de los clientes no necesitan perder tiempo ingresando datos manualmente, y los errores se reducen. La base de datos del MNO se vuelve más consistente y más completa en cuanto a

Las identidades digitales de confianza hacen posible que los MNO simplifiquen y digitalicen sus flujos de trabajo a través de la reducción de la entrada manual, de las fotocopias y del papeleo que puede tardar varios días en procesarse. Esto no solo reduce los costos operativos, sino que también beneficia a los clientes mediante la drástica disminución del tiempo que lleva subscribirse y la activación instantánea de varios servicios.

ENROLAMIENTO
HASTA 5 VECES
MÁS RÁPIDO

2.3 Protección contra el fraude

En pocas palabras: cada año el fraude cuesta caro a los MNO. Y está en aumento. En vista de las grandes pérdidas financieras, así como del daño a la reputación de la marca, controlar el fraude de suscripción es una prioridad clave para los MNO.

Las identidades digitales de confianza abordan eficazmente el problema de las identidades falsas, tanto en los puntos de venta físicos como en los canales en línea.

El fraude de suscripción costó a los MNOs

$5,070

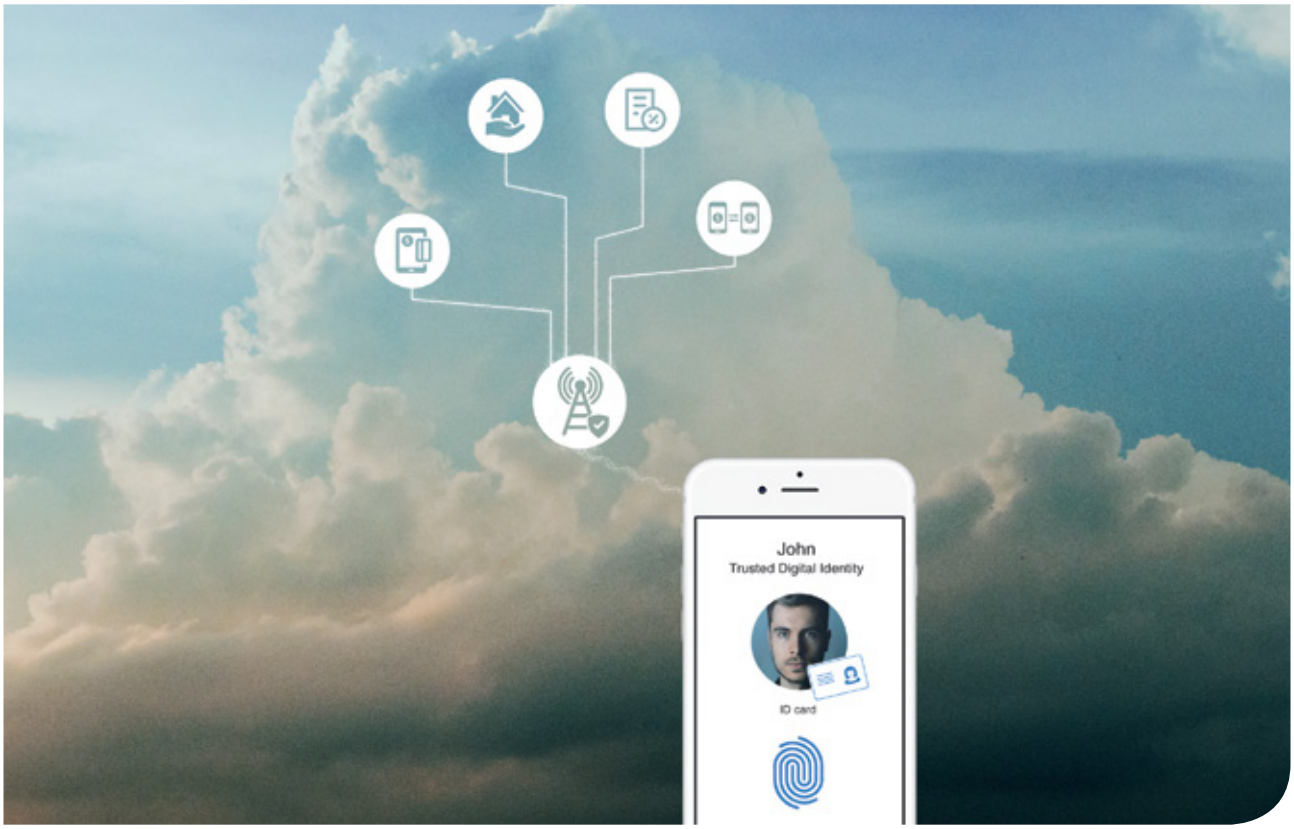
millones en 2016

Si la identidad del posible cliente no puede ser autenticada, no puede continuar. Además, cuando un cliente existente busca, por ejemplo, adquirir otro teléfono y otra suscripción, el uso de su identidad digital única confirma que el cliente no es un impostor. Los equipos de ventas ya no necesitan adivinar intencionalmente o evaluar los documentos de identidad visualmente, las identidades digitales introducen una verificación segura que reduce drásticamente la incidencia del fraude.

2.4 Cumplimiento de las reglamentaciones

Los gobiernos están adoptando medidas más fuertes para prevenir el terrorismo, el lavado de dinero y otros delitos que involucran identidades falsas. La legislación elaborada en respuesta exige la verificación de identidad de alta seguridad, y los requisitos que deben cumplir los operadores de redes móviles continúan cambiando a un ritmo rápido. Por ejemplo, el registro de tarjeta SIM prepaga ya es obligatorio en más de 90 países, según la GSMA. Además, dado que los MNO están ofreciendo cada vez más servicios financieros nuevos, se les exige que cumplan con la legislación contra el lavado de dinero (LMA) y contra el terrorismo (CFT). También están sujetos a cumplir con los procedimientos de verificación de identidad Conozca a su Cliente (KYC).

Las identidades digitales de confianza brindan a los MNO una manera directa de cumplir con dichas regulaciones, sin trasladar la carga a sus clientes (soportar un período de espera, completar formularios extensos, etc.).



2.5 Proporcionar valor a través del acceso seguro a los servicios

Las identidades digitales de confianza pueden cumplir un propósito más allá de la protección contra el fraude y la sistematización efectiva: representan una oportunidad para que los MNO creen un nuevo valor para sus clientes. Dicho valor se centra en la necesidad apremiante de acelerar la seguridad digital junto con la conveniencia. Una identidad digital de confianza puede actuar como una puerta de enlace confiable para que los clientes accedan a múltiples servicios sensibles a la seguridad, incluidos los servicios de operador de telefonía móvil, servicios financieros y servicios de gobierno electrónico.

Servicios de operador móvil: de prepago y postpago, dinero móvil, cambio de dispositivo, servicios IoT.

Servicios financieros: banca, comercio electrónico, pago de facturas en línea, transferencias de dinero.

Servicios de gobierno electrónico: voto electrónico, pago de impuestos, servicios sociales electrónicos, seguros, salud electrónica, seguridad social.

La creación de un nuevo valor comienza cuando el MNO brinda a sus clientes una manera más rápida y fluida de activar sus servicios, iniciar sesión e interactuar. Una identidad digital hace que sea sencillo y conveniente para los clientes suscribirse a servicios adicionales, y que sea más fácil para el MNO obtener una venta cruzada o una venta incremental (upselling y cross selling).

El valor puede extenderse hacia afuera. No todos los sectores y, ciertamente, no todas las empresas crearán su propia solución de identidad digital a medida, sino que buscarán socios. Los MNO están bien posicionados para aprovechar esto. Al servir como un habilitador de ID digital, los MNO pueden explorar nuevos modelos de negocio y aprovechar una fuente de ingresos nueva y estable proveniente de un tercero.

3. ¿Cómo funcionan en la práctica las identidades digitales de confianza?

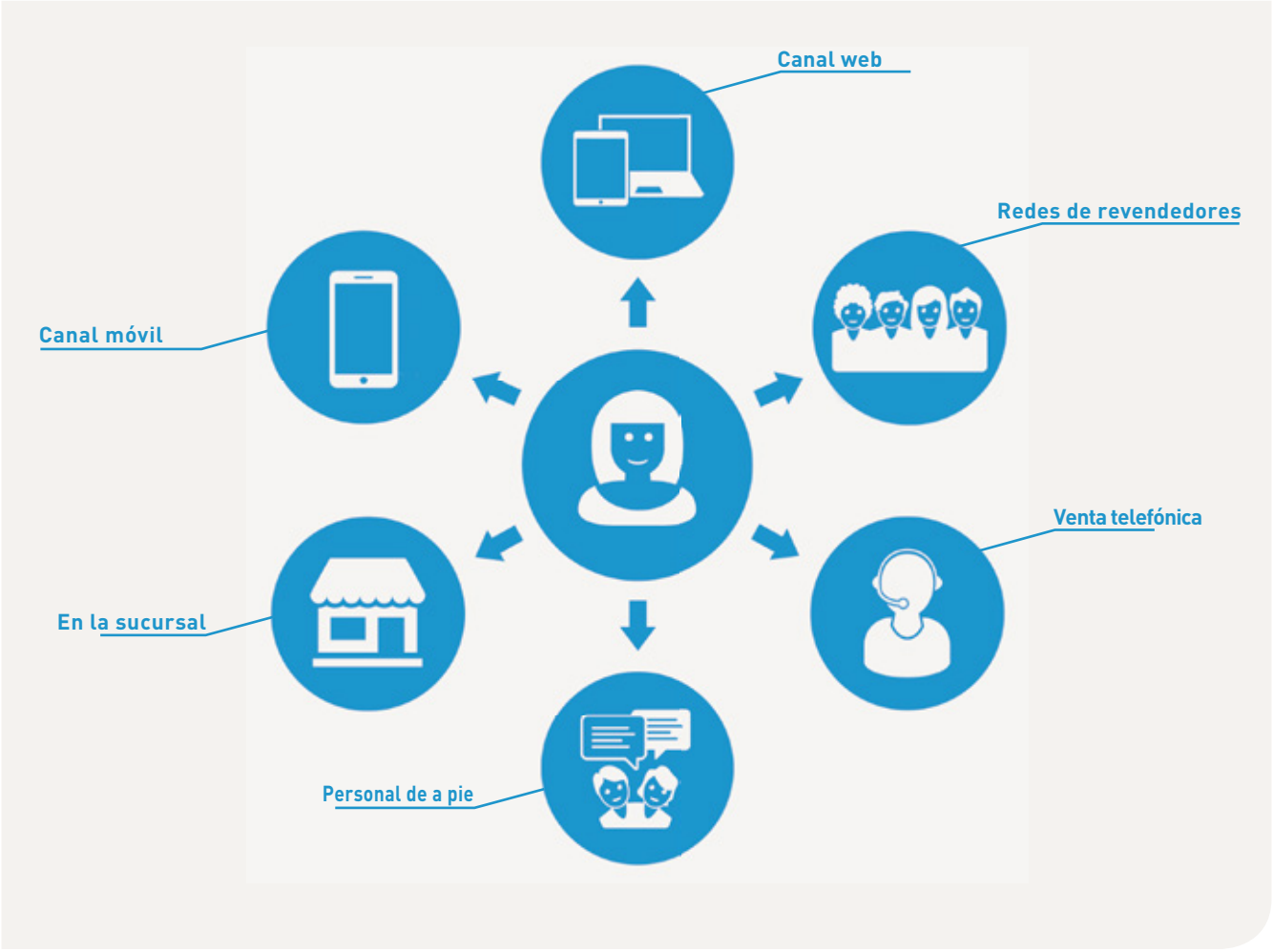
3.1 Un sistema omnicanal es imprescindible

Los MNO incorporan clientes en una amplia gama de escenarios. Las suscripciones y los servicios pueden estar a cargo de personal de a pie, representantes de venta telefónica o representantes de clientes en sucursales, o pueden realizarse en línea sin supervisión.

Muchas soluciones de ID digital solo admiten implementaciones remotas, excluyendo otros canales que son fundamentales para la adquisición de clientes por parte del MNO, como los puntos de venta, las redes de revendedores, etc.

Sin embargo, proporcionar una experiencia omnicanal fluida es de una importancia central para los MNO, ya que los clientes no toleran un proceso pesado.

Ya sea que la incorporación del cliente se realice en persona o de forma remota, la seguridad y la precisión del proceso de creación de la identidad digital de confianza deben ser consistentes. Y el cliente debería disfrutar de la misma experiencia o de una similar, independientemente del canal.



4. El paso a paso en la creación de una identidad digital

Una identidad digital de confianza se crea mediante tres pasos generales: captura, verificación, digitalización. Los detalles de cada paso pueden variar de acuerdo con la extensión de la información que el MNO desea capturar y las regulaciones a las que está sujeto, por ejemplo, en torno a la privacidad de los datos personales.

4.1 Captura (documentos de identidad y biometría)

Aunque los escenarios de incorporación, dependiendo del canal utilizado por el cliente, pueden ser diferentes, el proceso de captura de atributos de identidad debe llevarse a cabo de forma similar. El hardware necesario puede ir desde un teléfono móvil hasta escáneres especializados de alta gama. La elección del hardware tiene implicancias para el nivel de calidad, los tipos de verificación que se pueden realizar y, básicamente, para la precisión de los resultados.

DISPOSITIVOS PARA LA CAPTURA DE ATRIBUTOSDE IDENTIDAD

En la sucursal, atendidos

Escáner
Teléfono inteligente
Tableta

Correo electrónico
Servicio web
Tabletas biométricas

Lectores UV, IR
Lectores biométricos

Remoto, sin atención

Servicio web
Mobile

Tableta
Kiosco

Para comenzar, la información del suscriptor se toma de un documento de identidad (pasaporte, licencia de conducir o documento nacional de identidad, permiso de residencia, etc.). En este proceso, la información, como el nombre y la fecha de nacimiento, se puede extraer a través del análisis de imagen (reconocimiento óptico de caracteres). Esta tecnología ayuda a garantizar que se ingrese información precisa y detallada del cliente en el CRM. De ser necesario, se puede extraer otra información, como la dirección postal del suscriptor de una factura de servicios públicos, para completar el perfil del cliente o habilitar una verificación adicional.

Para capturar la información biométrica del usuario, se utiliza un dispositivo de captura biométrica (como un teléfono móvil, una cámara web, una tableta o un kiosco, o un escáner de huellas dactilares especializado). Los tipos de datos biométricos que se pueden recopilar incluyen información del rostro, la huella dactilar, la huella de la mano o el iris.

4.2 Verificación

La verificación de identidad tiene como objetivo verificar la autenticidad del documento de identidad del usuario final y valida si la persona es quien dice ser. Esto puede requerir una combinación de soluciones, según el nivel de seguridad que se necesite.

a. Verificación del documento de identidad

Una vez capturado, el sistema verifica la autenticidad de un documento de identidad con un software especializado. Comparando con una base de datos de identidades, se pueden usar diferentes métodos para verificar diferentes características del documento de identidad provisto.

En esta fase, también se puede extraer la información personal del tarjetahabiente para llenar automáticamente los campos en los formularios de registro, en el CRM, etc. Esto da como resultado un proceso de incorporación más rápido y simple para los clientes, así como un ahorro de tiempo y mayor precisión de los datos para los MNO.

Existen tres niveles diferentes de verificación de documentos:

LUZ BLANCA

> Verifica elementos de la mayoría de los documentos bajo luz blanca.
> Usado principalmente de forma remota/en línea.
> A menudo utiliza dispositivos de consumo (teléfono inteligente, cámara web...).

LUZ INVISIBLE

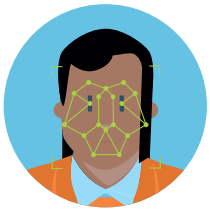
> Verifica elementos de seguridad de la mayoría de los documentos de identidad bajo la luz blanca, ultravioleta e infrarroja.
> Usado principalmente en las sucursales.
> Utiliza escáneres de alta gama.

ELECTRÓNICO

> Verifica información electrónica en el chip de los documentos de contacto o sin contacto.
> Puede usarse en las sucursales o remotamente.
> Usa dispositivos NFC y software especial.

b. Verificación de la biometría

La tecnología biométrica se usa para verificar si la persona que presenta el documento es quien dicen ser. También presenta una oportunidad para su uso posterior como una forma simple y moderna de acceder a los servicios que requieren identificación, y en particular cuando la verificación debe llevarse a cabo de forma remota. Las dos tecnologías más comúnmente utilizadas son el reconocimiento facial y el escaneo de las huellas dactilares.



La tecnología de reconocimiento facial analiza el rostro del usuario por medio de algoritmos que determinan el tamaño relativo, la posición y/o la forma de las características faciales, como los ojos, la nariz, los pómulos y la mandíbula. Estas características se usan luego para compararlas con otra imagen (por ejemplo, la imagen del documento de identidad) para determinar si estas características coinciden. Además, la detección de prueba de vida a través de video, parpadeo u otras técnicas se emplea para asegurar la presencia de una persona real, y no una fotografía o modelo 3D.

La autenticación de huellas dactilares se lleva a cabo mediante el análisis de varias características de las crestas de fricción en la punta del dedo e identificando el patrón de impresión único. Este patrón de impresión se compara con la impresión asociada con el propietario de la tarjeta de identidad. Esto se puede hacer localmente comparando la huella dactilar con datos en el chip, o remotamente, con una base de datos de terceros.

4.3 Digitalización de la identidad

Después de que se establece una coincidencia entre los datos biométricos y el documento de identidad, se puede crear una identidad digital. En el futuro, la identidad digital del usuario se puede utilizar para iniciar sesión fácilmente en el servicio. El usuario puede obtener acceso simplemente presentando el atributo biométrico solicitado, como la huella dactilar.

Esta función permite a los usuarios acceder más libremente a los servicios del MNO al reducir la fricción con la que, de lo contrario, se encontrarían durante la autenticación. El MNO también puede proporcionar este método de verificación conveniente a los servicios de terceros que requieren la identidad verificada de sus usuarios.

5. Nuestra experiencia central: la identidad digital

En Gemalto, trabajamos con algunas de las empresas y de los gobiernos más importantes del mundo y les brindamos soluciones tecnológicas flexibles que les ayudan a satisfacer la necesidad de mayor seguridad y conveniencia simultáneamente.

150+
programas de
gobierno electrónico

Nuestra tecnología sirve como base para más de 150 programas de gobierno electrónico, y nuestra tecnología de pasaporte electrónico biométrico es utilizada por más de 80 países, con más de 200 implementaciones biométricas y contando. La identidad digital sigue siendo el núcleo de nuestra experiencia, a medida que ayudamos a cientos de nuestros socios a implementar soluciones avanzadas de autenticación y seguridad.

Hemos trabajado como un socio de confianza para diferentes MNO desde los inicios de nuestra empresa. Proporcionamos tarjetas SIM y servicios gestionados a más de 700 millones de suscriptores, y suministramos a los MNO productos y servicios de última generación, que cumplen con las últimas especificaciones de la GSMA. Nuestros productos cumplen con los estándares internacionales más exigentes, como los que exigen el Departamento de Comercio de los EE.UU., el FBI, Interpol y el Instituto Nacional de Estándares Americanos.
Al combinar nuestra experiencia en identidad digital con nuestras asociaciones de larga data con diferentes MNO, buscamos ayudar a los MNO a brindar la mejor experiencia posible a miles de millones de personas.

700
millones
de suscriptores

6. Gemalto: un socio en transformaciones digitales

Con cada nueva generación de tecnología que llega más rápido que la anterior, la evolución de la tecnología sigue una curva exponencial. En este entorno rápidamente cambiante y altamente centrado en el cliente, las empresas constantemente necesitan mejorar sus ofertas y mantenerse al día con las últimas tendencias.

Aquí es donde entra Gemalto. Nuestra misión central es estar varios pasos adelante de los desarrollos tecnológicos.
Trabajamos como socio de las empresas que buscan hacer avances importantes, y les ofrecemos la tecnología, así como la orientación en cuanto a su integración. Esto permite que nuestros socios continúen centrándose en sus competencias centrales, a la vez que diversifican y fortalecen su oferta.

En lugar de simplemente ser un imperativo de seguridad, las identidades digitales constituyen una gran oportunidad de monetización y un futuro emocionante para los operadores de redes móviles. Al igual que con nuestras otras soluciones para los MNO, que van desde el IoT pasando por la conectividad y hasta las tarjetas SIM y los elementos seguros, estamos preparados con tecnología de identidad digital fácilmente implementable.

Para obtener más información acerca de nuestra cartera de tecnología de identidad digital de confianza, consulte nuestro folleto: **Tecnología de identidad digital de confianza de Gemalto para operadores de redes móviles.**

ACERCA DE GEMALTO

Gemalto (Euronext NL0000400653 GTO) es el líder mundial en seguridad digital, con ingresos anuales de €3,000 millones en 2017 y clientes en más de 180 países. Llevamos confianza a un mundo cada vez más conectado.

Desde software seguro hasta biometría y cifrado, nuestras tecnologías y nuestros servicios permiten a las empresas y a los gobiernos autenticar identidades y proteger datos para que permanezcan seguros y habilitan servicios en dispositivos personales, objetos conectados, la nube y entre ellos.

Las soluciones de Gemalto están en el corazón de la vida moderna: en la seguridad de los pagos, la seguridad empresarial y el Internet de las Cosas. Autenticamos personas, transacciones y objetos, ciframos datos y creamos valor para el software, lo que permite a nuestros clientes brindar servicios digitales seguros a miles de millones de personas y de cosas.

Nuestros 15,000 empleados operan en 114 oficinas, 40 centros de personalización y de datos, y 35 centros de investigación y desarrollo de software ubicados en 47 países.

Para más información,
visite: https://www.gemalto.com/mobile
https://www.gemalto.com/mobile/id-security

© Gemalto 2016. Todos los derechos reservados. Gemalto, el logotipo de Gemalto, son marcas comerciales y marcas de servicio de Gemalto y están registradas en ciertos países.

GEMALTO.COM/MOBILE

gemalto
security to be free