MailTeck CUSTOMERCOMMS

WhitePaper

Verificar y autenticar la identidad de tu cliente

La implementación de un sistema adecuado de verificación en la autenticación de la identidad legal de un cliente es una necesidad que comparten cada vez más empresas de varios sectores. Las técnicas de verificación, combinadas, ofrecen una solución segura y confiable para identificar y autenticar a tus clientes, que además pueden vivir una *user experience* atractiva.

TABLA DE CONTENIDOS

01

Beneficios de la verificación de la identidad digital

En 2019 se presentaron alrededor de 3.000 demandas por suplantación digital de identidad en España. País que, para la Comisión Europea, es uno de los estados miembro en los que más porcentaje de población se ha visto afectada por este problema. Esto supone contratiempos importantes para las empresas (que a veces se traducen en pérdidas económicas relevantes) y también para los usuarios o clientes.

La implementación de un sistema adecuado de verificación de identidad digital es una garantía a la hora de evitar este fraude y ofrece grandes beneficios tanto para tu empresa como para tus clientes:

Para la empresa

- Reduce el fraude
- Evita posible sanciones y pérdidas económicas
- Mejora su imagen corporativa

Para el cliente

- Mejora su experiencia como usuario o cliente
- Incrementa su seguridad en las transacciones
- Reduce el riesgo de suplantación de su identidad

En MailTecK & Customer Comms podemos ayudarte a conseguir estos beneficios, por ejemplo, en procesos de comunicaciones fehacientes, contratación electrónica y *onboarding* digital, como en los casos siguientes:

- Nuestro servicio de **identificación digital certificada**.
- El **check-in digital con biometría digital** en colaboración con Mitek.
- **Validación de la identidad del firmante en un proceso de firma electrónica** en colaboración con OneSpan.

02

Diferencias entre identificar y autenticar

Antes de conocer las principales técnicas de verificación de identidad digital es importante diferenciar dos términos:

Identificar

Una persona se "identifica" cuando dice quién es aportando los datos y pruebas de su identidad que permitirán verificar que es quien dice ser. Estos datos de identificación se asocian de manera única a la persona (nombre, dirección postal, email, teléfono móvil, contraseñas, preguntas y respuestas, biometría...) en un formato electrónico.

El Reglamento eIDAS (artículo 3.1) la define así: *"Proceso de utilizar los datos de identificación de una persona en formato electrónico que representan de manera única a una persona física o jurídica o a una persona física que representa a una persona jurídica"*.

Autenticar

Una persona se "autentica" con la utilización de sus datos de identificación, incluyendo una posible verificación de identidad, en un proceso digital que garantiza el origen y la integridad de los datos en formato electrónico.

La definición de autenticación incluida en el Reglamento eIDAS (artículo 3.5) es la siguiente: *"Proceso electrónico que posibilita la identificación electrónica de una persona física o jurídica o el origen y la integridad de datos en formato electrónico"*.

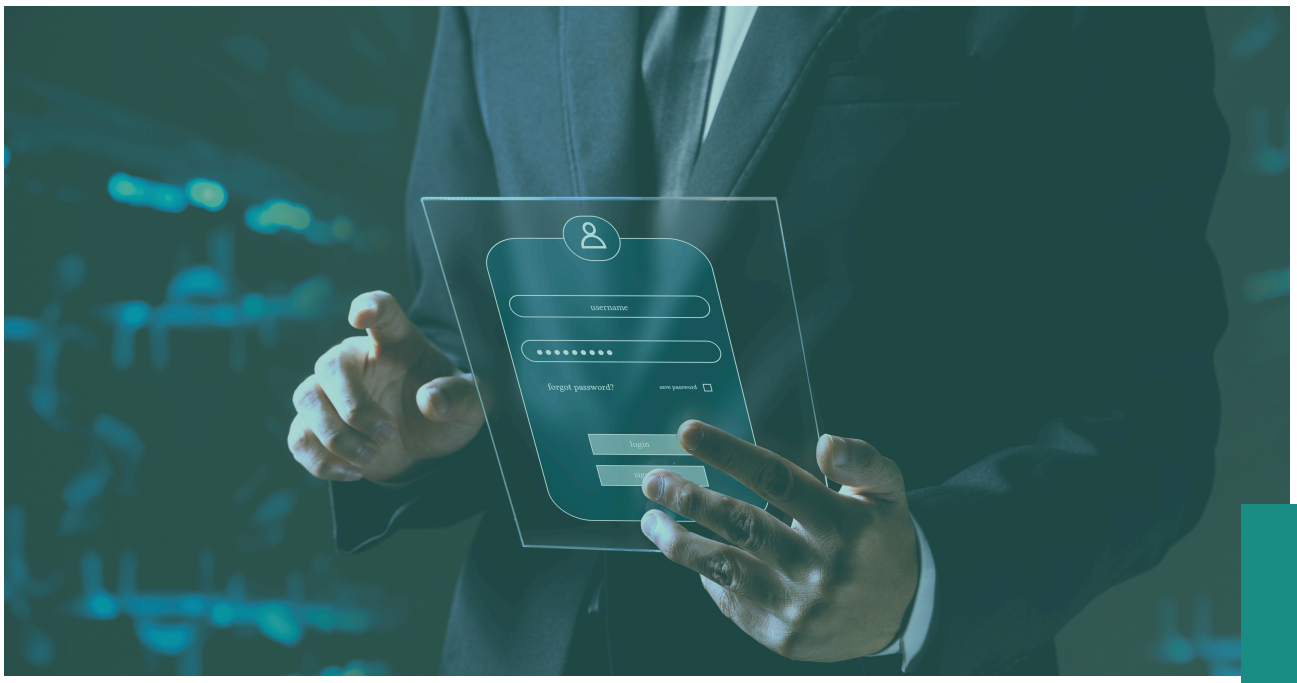
03

Tipos de sistemas de autenticación

Los sistemas de autenticación se pueden agrupar en tres grandes categorías:

- Los que se basan en **algo que la persona sabe.**
  Una contraseña o preguntas de control con respuestas predefinidas.
- Los que se basan en **algo que la persona tiene.**
  Un dispositivo generador de códigos, una tarjeta de coordenadas y el documento de identidad son opciones en esta categoría. Una de las soluciones más utilizadas es la OTP (contraseña de un solo uso, por sus siglas en inglés) que llega por SMS al teléfono móvil.
- Los que se basan en **lo que la persona es.**
  Son los sistemas de autenticación biométrica y usan rasgos únicos y medibles de las personas: reconocimiento de iris, biometría de huella dactilar, biometría facial, escritura y firma, voz... Su seguridad es máxima. Una contraseña se puede robar, el iris no, ni tampoco falsificar.

A todas ellas hay que añadir una opción, que la persona tiene, con máximo valor jurídico y extendida sobre todo en las relaciones con las administraciones públicas: el uso de un **certificado electrónico cualificado**.



04

Características de los sistemas de autenticación

La mayoría de los sistemas de autenticación tienen que mantener una serie de características básicas comunes que permitan garantizar la seguridad del proceso:

Seguridad

Es decir, que ningún ciberdelincuente pueda corromper el sistema y utilizarlo para obtener datos sensibles o hacerse pasar por quien no es.

Fiabilidad

A prueba de fallos.

Usabilidad

Clave para ofrecer una experiencia de usuario atractiva.

05

Principales técnicas de autenticación

A la hora de autenticar a usuarios y clientes, las empresas usan una serie de técnicas, a menudo de forma combinada. A continuación te detallamos las más habituales:

- **Validación de documento de identidad.**
  Se trata de una acción, doble ya que hay que probar que el documento es auténtico y que se corresponde con la persona que lo aporta. Se hace a través de las medidas de seguridad que integra el documento, de la lectura automatizada de sus campos de texto y su cotejo con bases de datos oficiales de sustracción de documentos de identidad.

- **Identidad física (biometría).**
  La autenticación biométrica es fundamental para cualquier empresa que quiera asegurarse que una persona sea quien dice ser. Por ejemplo, a través de reconocimiento facial con un selfie que se compara con la fotografía del documento de identidad. Incluye prueba de vida mediante movimiento facial para asegurar que la foto es real.

- **Identidad digital.**
  La dificultad se encuentra en conectar la identidad digital de alguna persona con su identidad real. Aquí entran en juego algoritmos sofisticados que, además de validar el teléfono y el email del usuario, utilizan otras técnicas como la geolocalización y el análisis de redes sociales.

06

La autenticación biométrica

Se trata de una de las técnicas de autenticación más seguras y cómodas para el usuario, y también de las más fiables para las empresas.

Podemos destacar dos tipologías dentro del mundo biométrico:

Biometría estática

Utiliza **características físicas únicas que se interpretan a través de soluciones tecnológicas**. En esta categoría entran el reconocimiento facial, de huellas dactilares, de iris, de voz o de la geometría del dedo.

Esta es una forma segura de autenticar clientes, pero siempre tiene que incluir una detección de vida para evitar fraudes.

Biometría de comportamiento

Aquí se incluyen **hábitos y movimientos que forman patrones distintivos y muy seguros**. Entre ellos están la dinámica de escritura (forma, velocidad y presión), la forma en la que se sostiene un teléfono (mano dominante, ángulo, cómo se desliza el dedo en la pantalla...) o hasta la manera de caminar. Incluso la hora y la ubicación de inicio de sesión pueden conformar un patrón de comportamiento.

Con la biometría de comportamiento se monitoriza continuamente la sesión de un usuario, y este hecho no solo permite verificar su identidad en momentos concretos. Va más allá. Si la sesión se interrumpe o es secuestrada, **el sistema puede reconocer el peligro y tomar las medidas adecuadas** para prevenir el fraude antes de que se produzca.

Si quieres profundizar más sobre este tema puedes consultar nuestro artículo sobre biometría, publicado en el blog, donde describimos de una manera amplia esta técnica y sus diferentes elementos.

07

Autenticar al cliente con verificación de identidad en una firma electrónica

Existen variadas maneras de autenticar, con verificación, la identidad de un cliente. Te mostramos, a continuación, y de forma resumida, el paso a paso de un servicio de autenticación por validación de documento de identidad en un proceso de firma, ofrecido a través de nuestro *partner* **OneSpan**. Podrás leerlo con más detalle en esta entrada del blog: Validación de la identidad de un firmante mediante la **herramienta de verificación de identidad OneSpan Sign**.

Se trata de un escenario de acuerdo mediado que parte del envío de un formulario de apertura de cuenta por parte de un agente.

- El agente que lanza la firma inicia el proceso sobre una plantilla prediseñada.
- Introduce los datos del destinatario que tiene que firmar electrónicamente.
- Elige la opción de autenticación. El sistema permite varias, como correo electrónico, SMS, preguntas y respuestas, solo verificación de documentos de identidad y verificación de documentos de identidad con comparación facial.
- Envía el formulario para su firma.
- El cliente recibe el correo con la petición y comienza la validación. Acepta las condiciones y elige el país de expedición de su documento de identidad.
- El cliente fotografía su documento de identidad y, a continuación, se hace un selfie para demostrar que es la misma persona que aparece en la foto del documento de identidad.
- Tras verificar con éxito la identidad, lo que ocurre en segundos, continua con la firma.
- Una vez completado el proceso se crea una traza de auditoría que captura los detalles y crea un registro que asegura el cumplimiento normativo.

08

Sectores en los que más se aplica la autenticación por verificación de la identidad digital

Las empresas tienen que asegurarse de que las personas que contratan con ellas son quienes dicen ser. Esto es así en general, tanto en procesos presenciales como a distancia. Pero algunos sectores operan bajo una normativa más férrea. La directiva europea PSD2 sobre servicios de pagos electrónicos, que entró en vigor a finales de 2019, es una de ellas.

Las **entidades financieras**, muy volcadas en el onboarding digital, forman parte de un sector innovador en cuanto a identificación legal (por normativa) y rápida (por experiencia de usuario). Pero también las **aseguradoras**, las **inmobiliarias** o incluso las **administraciones públicas** se enfrentan al mismo reto.

Por no hablar de las **telecos** y de las **compañías energéticas**, cuyo negocio generado a distancia crece de manera imparable, o las empresas turísticas. En este caso, la identificación digital gana enteros no solo a la hora de comprar sino, sobre todo, para hacer el check-in digital en **establecimientos hoteleros**. Nuestra plataforma CertySign permite a los hoteles verificar la identidad antes de la entrada del huésped, gestionar el formulario electrónico con sus datos, facilitar la gestión de la tasa turística y el cumplimiento de normas como la ORDEN INT/1922/2003. Lo explicamos con detalle en este artículo: Check-in digital con Certysign, el comienzo de la transformación digital en tu hotel.

¿Quieres saber cómo podemos acompañar a tu empresa en la identificación y la autenticación de sus clientes? Visita nuestra web.

Te ofreceremos soluciones personalizadas, adecuadas a tu actividad e integrables con tus sistemas.