Santander X Innovation Xperts

Ciudadanía & tecnología:
Identidad digital

FEBRERO 2023

By Santander

Índice

01 Introducción: **¿Dónde estamos?**

La identidad digital es un mercado en auge y su potencial de crecimiento seguirá aumentando en los próximos años. El cambio hacia procesos digitales, tanto para fines públicos (impuestos, subvenciones, servicios públicos, votaciones o ciudadanía digital, entre otros) como para diversos servicios privados (servicios financieros, comercio electrónico, acceso y uso de instalaciones, redes sociales, juegos, meta/multiversos, etc.), es definitivo y, tras la aceleración y la expansión provocadas por pandemia, se ha vuelto irreversible. Esto constituye el punto de partida más obvio para el crecimiento previsto del mercado de la identidad digital, y sin duda sienta las bases para el desarrollo del sector. Pero algunas tendencias, más complejas y cargadas de desafíos, están también anunciando una profunda transformación del mercado, que requerirá y conllevará una mayor sofisticación de las soluciones de identidad digital, los actores implicados y las necesidades de los usuarios. A la hora de afrontar e interiorizar estos retos, las rutas que se pueden tomar y los ámbitos que se pueden explorar son diversos y múltiples. Por lo tanto, las respuestas innovadoras y estratégicas serán las que marquen la diferencia.

Este informe se estructura en tres partes, además de esta introducción. La segunda parte (*¿Hacia dónde vamos?*) revela las principales tendencias — la extensión de la «vida digital», las necesidades de la identidad en los contextos híbridos y la multiplicación de nuestras «vidas digitales» (en metaversos y realidades extendidas/aumentadas) —, que abren el camino a soluciones de identidad digital que cada vez tienen más capas, están mejor definidas y son más versátiles y escalables. La tercera parte (*¿Hacia dónde podemos ir?*) esquematiza las principales opciones organizativas, tecnológicas y políticas que se pueden considerar de acuerdo con cinco factores: el control (quién tiene el control), los actores (quiénes están implicados), los inputs (qué atributos), los outputs (qué soluciones se aportan) y el entorno (con qué propósito). La cuarta parte (*¿Hacia dónde deberíamos mirar?*) analiza las oportunidades menos evidentes pero más prometedoras, que están guiadas por cinco impulsores clave con capacidad de desarrollar definitivamente el potencial de la identidad digital en los próximos años. Las principales conclusiones se resumen en el último apartado.

02 ¿Hacia dónde vamos? Identidades digitales: las oportunidades más evidentes

La identidad digital es un mercado floreciente y su potencial seguirá aumentando mucho en los próximos años. Nuestra creciente **"vida digital"**, las **urgentes necesidades relacionadas con la identidad en contextos híbridos físico-digitales**, y la **multiplicación de nuestras "vidas digitales" (en metaversos y realidades extendidas/aumentadas)** están muy supeditadas a un marco de identidad digital global y aspiracional, sólido, versátil y fiable, y dependen mucho de él.

Más allá del evidente punto de inflexión que supone el paso de procesos cara a cara y en papel a procesos totalmente digitales, hay otras tendencias complejas que están produciendo un extraordinario aumento de las necesidades relacionadas con la identidad digital, llevando a una sofisticación de las situaciones que requieren demostrar y verificar la identidad y a una reinterpretación de la identidad digital bastante alejada de la mera "equivalencia funcional" de las fórmulas de identidad tradicionales.

Las principales tendencias identificadas, que guiarán el ejercicio de análisis y de detección de oportunidades prometedoras que pueden aprovecharse, son las siguientes (se desarrollarán con mayor detalle en los siguientes apartados):

II.2.1. La expansión y proliferación de contextos híbridos en los que la identidad tiene que fluir de manera fiable de los entornos físicos a los digitales y viceversa.

La consolidación definitiva del teletrabajo y el trabajo a distancia, la cada vez más frecuente participación a distancia en diversas situaciones sociales, políticas y profesionales (eventos, órganos decisorios, reuniones, comités deliberativos, negociaciones empresariales, contextos de aprendizaje, etc.), la demanda desbordada de procesos de incorporación (onboarding) totalmente remotos/digitales a una diversidad de servicios (contratación de personal, contratación de servicios bancarios, procedimientos de admisión, matriculación, etc.) reclaman soluciones de identidad fluidas y versátiles.

Como se detalla más adelante, esta tendencia se está abordando desde diferentes frentes, a menudo opuestos, y existen varias respuestas posibles, todas ellas con oportunidades igualmente prometedoras. Algunas soluciones pueden coexistir, o incluso complementarse; otras representan paradigmas enfrentados sobre la interpretación y el desarrollo de la identidad digital del futuro.

II.2.2. El fascinante aumento previsto de la vida digital en los metaversos y las realidades extendidas/aumentadas.

El sector privado se está embarcando seriamente en la planificación y concepción de estrategias de negocio para tener presencia en el/los metaverso/s y otras realidades extendidas/aumentadas: las universidades y escuelas de negocios, las tiendas y zonas comerciales, los organizadores de actos sociales, los bufetes de abogados, los bancos y proveedores de servicios financieros, los museos, las casas de subastas, etc. Con diferentes niveles de fiabilidad, las soluciones de identidad digital serán necesarias para fines educativos, profesionales, de entretenimiento, comerciales o incluso para aspectos relacionados con el ejercicio de la ciudadanía.

II.2.3. En lugar de identidades "monolíticas" los usuarios demandan identidades más granulares y con fines específicos, con una exposición mínima de la privacidad y un sentido del anonimato responsable.

Existen multitud de contextos en los que solo es necesario verificar y autenticar un atributo (o unos pocos, por ejemplo: edad legal, nacionalidad, vacunación, si se es un estudiante matriculado o un trabajador empleado, el cumplimiento de las obligaciones fiscales, que no existen pagos pendientes o retrasados, etc.) para completar una transacción, permitir el uso o acceder a un servicio. Exponer la privacidad y todos los atributos de la identidad en estos escenarios recurrentes es indeseable, innecesario e ineficiente.

Los usuarios estarían dispuestos a preservar su identidad y confiar en terceros fiables para, en cada situación, confirmar a la contraparte que se cumple determinado requisito, se ha verificado un atributo o incluso se ha autentificado la identidad. Esto implica el desarrollo de un modelo de identidad con una finalidad específica en el que debería ser esencial el papel del sector privado.

Por ejemplo, una institución bancaria podría desempeñar este papel aprovechando su posición y su experiencia en procesos de "conozca a su cliente" (KYC, por sus siglas en inglés) y contra el blanqueo de capitales (AML, por sus siglas en inglés). Si el usuario tiene que demostrar su edad legal, su nacionalidad o domicilio, el banco podría hacer de intermediario, limitándose a confirmar el cumplimiento de determinado requisito sin revelar otros datos innecesarios relacionados con la identidad.

II.2.4. La proliferación de modelos distribuidos y descentralizados de generación/verificación de atributos, para crear una auténtica DeSoc (sociedad descentralizada), a modo de transición revitalizadora desde unas DeFi (finanzas descentralizadas) puras.

Hay varias soluciones que operan en el mercado cuyo desarrollo puede permitir alcanzar modelos de privacidad con una finalidad específica, descritos anteriormente. En concreto, las soluciones basadas en sistemas distribuidos, o tecnología de registros distribuidos (DLT, por sus siglas en inglés) están ganando popularidad y relevancia.

Los tokens Soulbound, tokens intransferibles (no fungibles) que representan la identidad de una persona mediante el uso de la tecnología blockchain, están captando también una atención significativa.

Asimismo, los tokens de un solo uso emitidos por terceros fiables/de confianza (desde registros hasta instituciones bancarias) para demostrar la identidad en relación con uno o varios atributos con una exposición mínima son soluciones y proyectos en curso que merecen consideración.

En el marco de estas tendencias, los modos de asignación y acumulación de atributos crecerán —avatares, carteras, tokens de un solo uso, tokens Soulbound, cuentas como entrada única, wearables, el comportamiento en metaversos u otras realidades extendidas/aumentadas— y la identidad digital será cada vez más **definida, multicapa, versátil y escalable.**

¿Dónde nos encontramos?

Identidad digital en entornos privados y públicos y para una infinidad de propósitos

Identidades definidas con una finalidad específica →

Modelos centralizados muy fiables y de gran alcance, modelos distribuidos y descentralizados de generación/verificación de atributos →

¿Hacia dónde nos dirigimos?

La identidad digital para contextos híbridos, vida digital, metaversos y realidades extendidas/aumentadas

Santander X Innovation Xperts

By Santander

Con las tendencias actuales, la identidad digital será cada vez más definida, multicapa, versátil y escalable.

03 ¿Hacia dónde podemos ir? Principales retos y opciones de política legislativa y regulatoria

El futuro de la identidad digital (ID) debe abordar tres retos principales que gravitan en torno a tres modelos en tensión:

- **El modelo centralizado dirigido por el Gobierno; frente a los modelos de identidad federados[1]; frente a los modelos de identidad soberana.**
- **La integración de soluciones frente a la descentralización competitiva.**
- **La identidad fiable frente al anonimato aspiracional y la privacidad autogobernada.**

1. La identidad federada permite a los usuarios autorizados acceder a múltiples aplicaciones y dominios utilizando un único conjunto de credenciales que las organizaciones federadas, basándose en acuerdos/convenios, se comprometen a reconocer.

Para encontrar un equilibrio estable, los reguladores, los agentes del mercado, los productores de tecnología y los desarroladores de soluciones innovadoras tienen que jugar con cinco factores: el **control** (quién tiene el control), los **actores** (quiénes están implicados), los **inputs** (qué atributos alimentan el sistema de ID), los **outputs** (qué soluciones se aportan) y el **entorno** (dónde se utilizará el sistema de ID y con qué propósito):

Control	Actores	Inputs	Outputs	Entorno
Mayor control público de la identidad digital (ID)	Gobiernos	Atributos verificados	Reconocimiento transfronterizo	En espacios públicos y con fines públicos
Bancos y otros proveedores de servicios	Entidades privadas que cooperan con los Gobiernos para ofrecer soluciones de ID integradas y multicapa	eKYC Calificación crediticia AML	Pasarelas con ID de uso específico y multicapa	Espacios privados — obligación de las empresas de aceptar herramientas de ID
Modelos autosoberanos	Individuo al mando	Datos generados por avatares	Reconocimiento en todos los metaversos	Metaversos

04 ¿Hacia dónde deberíamos mirar? Las oportunidades más prometedoras en el

El pleno potencial de la identidad digital podrá desarrollarse si los retos relacionados con las políticas descritos antes se abordan con soluciones efectivas, innovadoras y pensadas para el futuro: **las oportunidades más prometedoras, y menos visibles, están ahí.** Según nuestro criterio y de acuerdo con nuestro análisis, **hay cinco impulsores clave con capacidad para alimentar el potencial de la identidad digital en los próximos 4-7 años.**

IMPULSOR 1: El reconocimiento transfronterizo y la identidad digital global: el papel del sector privado

El reconocimiento global de la identidad digital es fundamental. Este implica varios retos: interoperabilidad tecnológica, un marco legal habilitante, la cooperación mutua entre Estados, consideraciones lingüísticas, armonización normativa y de estándares, e infraestructuras compartidas, entre otros[2].

Aunque el reconocimiento transfronterizo es un concepto que se apoya en el Estado, ¿cómo pueden las entidades privadas añadir valor a la experiencia de su usuario y proporcionar soluciones rentables sin socavar la fiabilidad y la seguridad? Identificamos tres oportunidades que conviene explorar:

1. Facilitadores de la expansión de una identidad digital pública aceptada a escala global

2. Interfaces para la autenticación

3. Verificadores fiables

2. Naciones Unidas (CNUDMI) adoptó en julio de 2022 una Ley Modelo sobre la Utilización y el Reconocimiento Transfronterizo de la Gestión de la Identidad y los Servicios de Confianza.

Los Gobiernos están invirtiendo mucho en servicios de identidad digital (Australia, Alemania, Francia en el marco de NextGenerationEU, etc.). Estas iniciativas sientan las bases de un marco mundial para la identidad digital, pero no son suficientes. De hecho, los proyectos promovidos por Gobiernos pueden llevar a un escenario de identidad digital fragmentario y escasamente armonizado. Por lo tanto, garantizar el reconocimiento transfronterizo (o, para ser más precisos, internacional) de los servicios de identidad digital es decisivo. El establecimiento de un marco legal uniforme como el propuesto por la Comisión de las Naciones Unidas para el Derecho Mercantil Internacional (CNUDMI) en 2022 (Ley Modelo sobre la Utilización y el Reconocimiento Transfronterizo de la Gestión de la Identidad y los Servicios de Confianza) es sin duda un importante avance.

La actual revisión del reglamento eIDAS[3] (las siglas en inglés de "identificación electrónica, autenticación y servicios de confianza", que se refiere a una serie de servicios que incluye la verificación *online* de la identidad de individuos y empresas y la verificación de la autenticidad de documentos electrónicos) establecerá el escenario para el desarrollo futuro de la identidad digital en Europa y señalará las innovaciones y soluciones necesarias para la implementación del marco revisado. En el discurso sobre el estado de la Unión, la Comisión fue invitada a presentar una propuesta de firma digital interoperable a mediados de 2021. Con un respaldo tan firme y decisivo, las perspectivas del mercado de la identidad digital en Europa son enormemente prometedoras. De hecho, según la comunicación de la Comisión "Brújula Digital 2030: el enfoque de Europa para el decenio digital", se ha fijado el objetivo de que el 80% de los ciudadanos de la Unión Europea utilicen una solución eID digital en 2030; y en el horizonte, la estrategia para configurar el futuro digital de Europa prevé una identidad electrónica pública universalmente aceptada.

El 22 de febrero de 2022, el grupo de expertos eIDAS adoptó el documento *European Digital Identity Architecture (EUDI) and Reference Framework - Outline*[4], que proporciona una descripción sumaria del concepto de cartera de identidad digital europea (EUDI *Wallet*) (las siglas en inglés de Identidad Digital Europea): su objetivo,

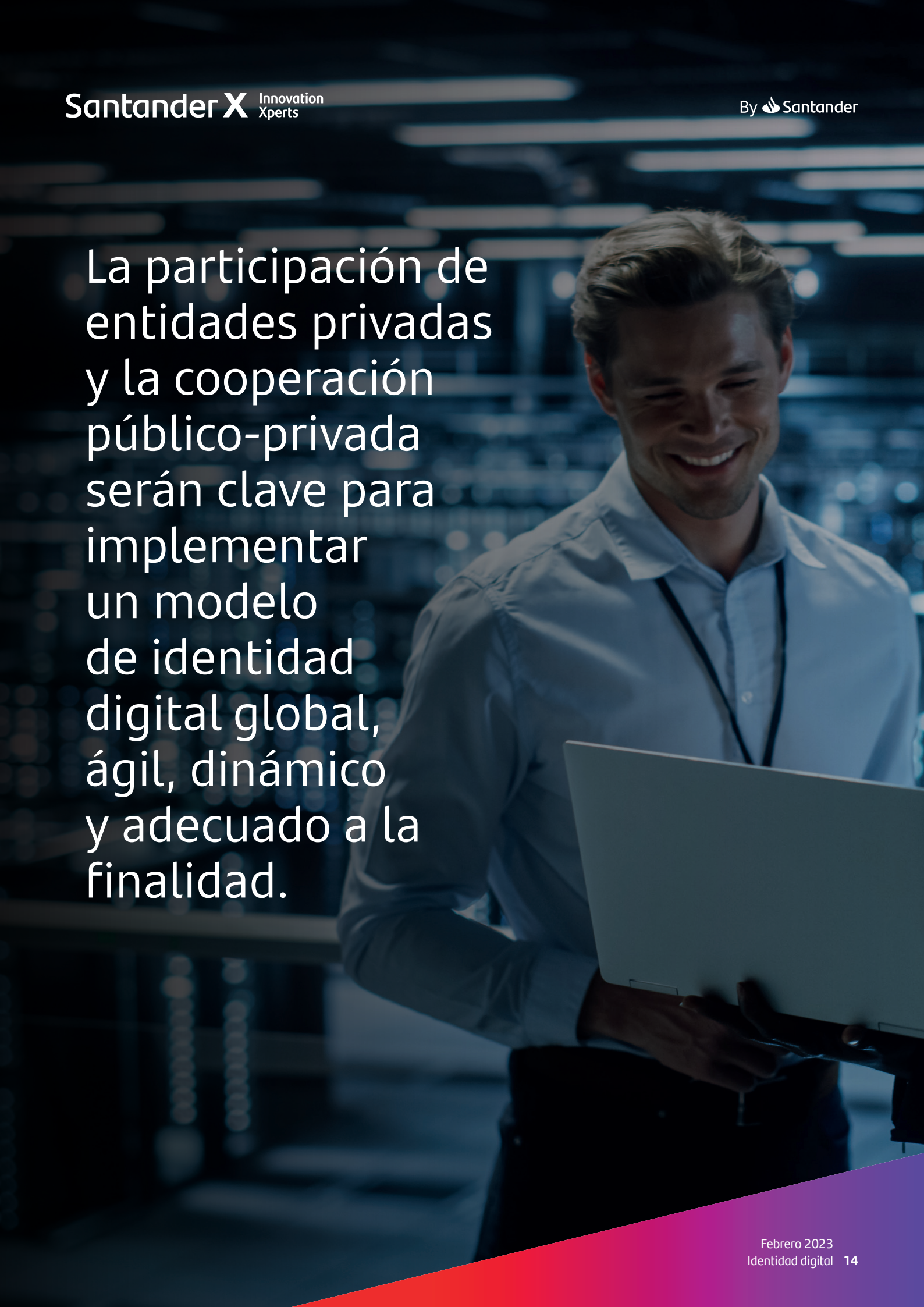
3. Reglamento (UE) n.º 910/2014 del Parlamento Europeo y del Consejo, de 23 de julio de 2014 , relativo a la identificación electrónica y los servicios de confianza para las transacciones electrónicas en el mercado interior y por la que se deroga la Directiva 1999/93/CE. OJ L 257, 28.8.2014, p. 73-114.

4. https://digital-strategy.ec.europa.eu/en/library/european-digital-identity-architecture-and-reference-framework-outline

los roles de los actores del ecosistema, los requisitos funcionales y no funcionales de la cartera y sus potenciales componentes. El documento señala algunas cuestiones clave que deben incluirse en la "caja de herramientas" (*toolkit*) y el marco técnico de referencia y arquitectura (ARF, por sus siglas en inglés), un conjunto de estándares y especificaciones técnicas comunes; así como un conjunto de directrices comunes y mejores prácticas.

La oportunidad para el sector privado: más allá de un modelo centrado en el ciudadano y un sistema de Gobierno a Gobierno. Dado que un sistema estrictamente de Gobierno a Gobierno no es aconsejable ni óptimo para el objetivo, la participación de entidades privadas y la cooperación público-privada serán clave para implementar un modelo de identidad digital global, ágil, dinámico y adecuado a la finalidad. Además, hay que señalar que la propuesta contempla, ambiciosamente, el requisito de que cada Estado miembro emita una cartera de identidad digital europea en los doce meses posteriores a la entrada en vigor del reglamento. En este contexto, el papel del sector privado como acelerador del marco eIDAS será crucial y así se señaló de manera explícita en el informe de evaluación[5].

5. Informe de la Comisión al Parlamento Europeo y al Consejo sobre la evaluación del Reglamento (UE) n.º 910/2014 relativo a la identificación electrónica y los servicios de confianza para las transacciones electrónicas en el mercado interior (eIDAS). COM/2021/290 final.



La participación de entidades privadas y la cooperación público-privada serán clave para implementar un modelo de identidad digital global, ágil, dinámico y adecuado a la finalidad.

In focus

Razones para apoyar un marco cooperativo público-privado

Existen varias razones que desaconsejan un modelo dirigido únicamente por el Estado y que avalan un marco de cooperación público-privada.

1. Las iniciativas dirigidas por Gobiernos tienden a implementar **modelos centrados en el ciudadano.** Este enfoque supone que, en el caso de los viajeros, los visitantes, los migrantes o los turistas el reconocimiento no siempre es lo suficientemente fluido. El papel del sector privado puede ser crucial para reducir estas carencias. Desde certificados sanitarios para viajar hasta títulos profesionales y certificados educativos, la identificación y la autenticación de los no ciudadanos son necesarias en multitud de contextos en los que las entidades privadas pueden tomar la iniciativa.

2. Un número creciente de contextos que requieren identificación digital refieren a **situaciones de un único atributo**: el usuario tiene que demostrar, por ejemplo, que ha sido invitado a un acto, su edad legal, la vacunación adecuada, el permiso de acceso o su matriculación en un curso. La identificación completa y la autenticación oficial no es lo que precisa ni son aconsejables en tales circunstancias. No solo es costoso más allá de lo razonable, sino desproporcionado para su objetivo y arriesgado para la privacidad.

En esta línea, la evaluación del reglamento eIDAS[6] reveló la aparición de un nuevo entorno que transita desde la provisión y utilización de identidades digitales rígidas a la provisión de y confianza en atributos específicos relacionados con esas identidades.

El sector privado está en condiciones de proporcionar e implementar modelos de identificación y autenticación adecuados a la finalidad, muy eficientes y respetuosos con la privacidad para estos contextos. Con ese objetivo, el sector privado puede desarrollar una segunda capa en la autenticación digital que se superponga a los marcos de identificación digital dirigidos por el Estado.

3. En tercer lugar, los intentos de garantizar el reconocimiento transfronterizo y la aplicabilidad global de las credenciales de identidad fracasarán si no existen **credenciales de identidad digital estandarizadas.** Los Estados deben promover la estandarización, pero eso requiere una cooperación intensa, extensa y profunda a escala mundial. Cuestiones de soberanía, razones políticas o, simplemente, obstáculos prácticos pueden poner en peligro la estandarización o dificultar una colaboración plena. El sector privado encontrará una brecha importante que reducir y un nicho en el que centrarse. Si las credenciales de identidad oficiales no se estandarizaran, podrían estandarizarse los datos.

6. Informe sobre la evaluación del Reglamento (UE) n.º 910/2014 relativo a la identificación electrónica y los servicios de confianza para las transacciones electrónicas en el mercado interior (eIDAS), 3.6.21, COM (2021) 290.

Las oportunidades para las empresas, tanto para los actores emergentes como los existentes, apuntan a las siguientes oportunidades de negocio e inversión:

A. Como proveedores de servicios vinculados a la identidad (certificaciones electrónicas de atributos).

B. Como interfaces "intermediarias", recopilando los datos pertinentes de las credenciales oficiales de identidad y proporcionando plantillas estandarizadas a la parte que solicita la identificación para cada finalidad específica (por ejemplo: credencial sobre estado de salud para poder viajar, edad legal, si un paciente está asegurado, etc.).

C. Como verificadores fiables que atestigüen en cada circunstancia que la credencial oficial de una jurisdicción es válida y aplicable en otra jurisdicción (una especie de comparador de credenciales).

Estas oportunidades están totalmente alineadas con los posibles roles de los agentes del ecosistema de la identidad digital europea (EUDI)[7]. Por lo tanto, el sector privado está en situación de ampliar su presencia en la Unión Europea a una escala mundial.

Para desarrollar e implementar las funcionalidades de la cartera EUDI, algunas tecnologías ya disponibles pueden cumplir el papel previsto. Las funcionalidades que debe prestar la cartera EUDI pueden agruparse en cinco componentes: interfaz de usuario, almacenamiento de datos, funciones complejas/protocolos criptográficos, material criptográfico sensible y módulo de medios eID[8].

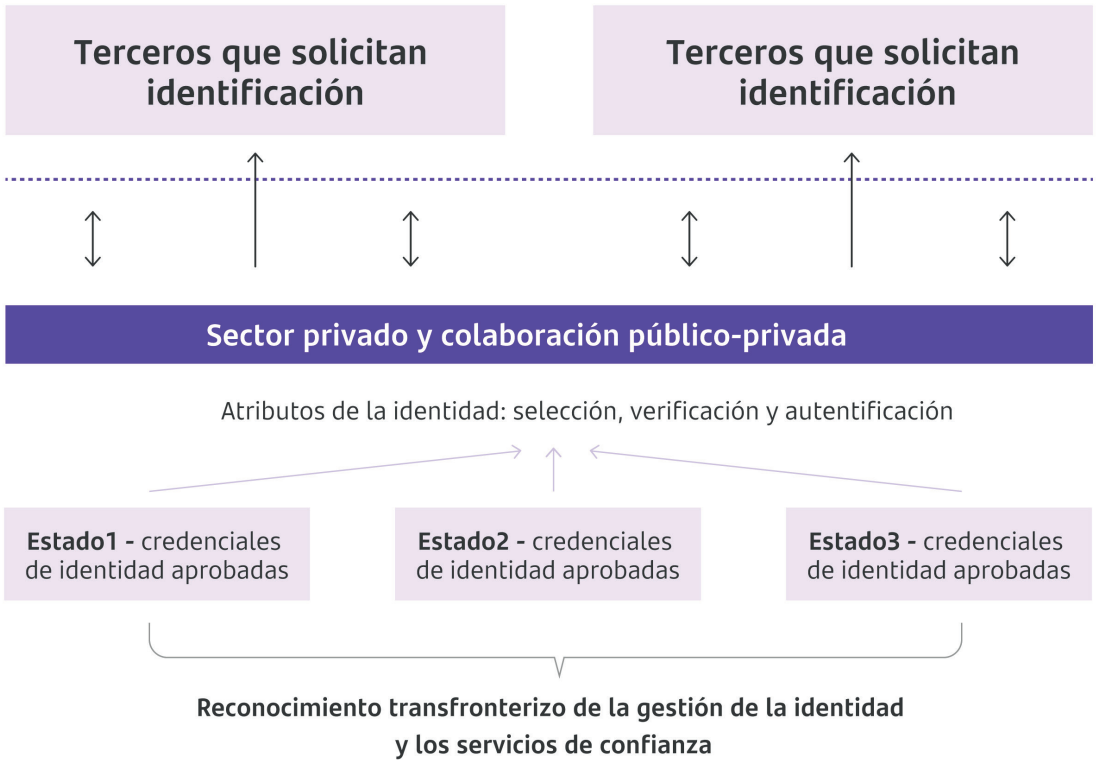
---

7. Grupo de expertos eIDAS, Marco de Referencia y Arquitectura de la Identidad Digital Europea. Resumen, 22 de febrero de 2022.

8. El grupo de expertos eIDAS enumera las funcionalidades requeridas como sigue:

1. Realizar la identificación electrónica, almacenar y gestionar la declaración electrónica cualificada de atributos (QEAA, por sus siglas en inglés) y la declaración electrónica de atributos (EAA, por sus siglas en inglés) de forma local o remota.
2. Solicitar y obtener de las declaraciones provenientes de proveedores, la declaración electrónica cualificada de atributos (QEAA) y la declaración electrónica de atributos (EAA).
3. Proporcionar o acceder a funciones criptográficas.
4. Autenticación mutua entre la cartera EUDI y las entidades externas.
5. Seleccionar, combinar y compartir con las partes dependientes los datos de información personal (PID, por sus siglas en inglés), la QEAA y la EAA.
6. Interfaz de usuario compatible con la concienciación del usuario y un mecanismo de autorización explícita.
7. Datos que se firman mediante firma/sello electrónico cualificado (QES).
8. Provisión de interfaces a las partes externas.

Por un lado, las aplicaciones móviles, las aplicaciones web y/o las aplicaciones seguras en dispositivos de escritorio pueden implementar los factores de forma. Por otro, los componentes de apoyo necesarios pueden basarse en: un servidor *backend*, documentos de identidad electrónicos oficiales, un token de *hardware* externo seguro, un proveedor de servicios criptográficos, un entorno de ejecución de confianza (TEE, por sus siglas en inglés).



IMPULSOR 2: Los modelos de identidad digital autosoberanos y de uso específico

Las carteras de identidad digital sintetizan dos rasgos clave del futuro de la identidad digital: la identidad digital se centra en el usuario y es este quien la controla. La identidad de los usuarios se evaluará y verificará solo cuando sea necesario (pertinencia), en la medida adecuada para la finalidad (adecuación al fin) y de forma que se revele exclusivamente la información esencial (minimización); por ejemplo, la comprobación de la edad no exige que se revele la fecha de nacimiento, ni la de la elegibilidad de un candidato revelar detalles específicos sobre las condiciones requeridas, ni la ubicación de un usuario revelar la dirección personal. Los actores existentes y los emergentes pueden añadir un valor significativo al actuar como "centros de identidad" o emisores de tokens de identidad/atributos (de un solo uso). Varias razones y algunos factores concurrentes (que se enumeran más adelante) refrendan que las instituciones bancarias se encuentran en una posición especialmente favorable para desempeñar con eficacia este papel.

Como se ha explicado con anterioridad, **la necesidad de identificar y verificar la identidad de individuos y organizaciones está ganando en definición, transversalidad y versatilidad.** Nuestra vida digital, cada vez más activa, no solo da lugar a infinidad de situaciones que requieren una identificación —compras *online*, banca *online*, pago de impuestos—, sino también a contextos o transacciones híbridas en las que una identificación *online* previa conlleva el ejercicio de derechos o el cumplimiento de obligaciones en persona (por ejemplo, en la economía *gig* o colaborativa, el hecho de confirmar que eres el pasajero esperado y que el conductor tiene un carnet de conducir válido; o a la hora de comprar un medicamento prescrito por un médico en una cita *online* o a través de una aplicación de diagnóstico automatizado). Estos diferentes contextos con frecuencia comparten ciertas características específicas:

A. Una baja sofisticación, pero una gran necesidad de confianza. En muchos de estos contextos, el nivel de sofisticación tecnológica es relativamente bajo, por ejemplo, en las transacciones P2P (entre pares), pero la necesidad de fiabilidad sigue siendo alta, al igual que lo son las expectativas privadas.

B. Situaciones dispersas. Las situaciones en las que se requiere la identificación son esporádicas, normalmente informales y suelen concluirse con rapidez; por ejemplo, los usuarios de una aplicación P2P para compartir coche tienen que identificarse antes de iniciar el viaje.

C. Identificación de atributos específicos. En estas situaciones, la identificación puede requerir tan solo la verificación de un atributo de identidad.

En la medida en que nuestras vidas digitales se amplían y los contextos híbridos físico-digitales se multiplican en una gran variedad de sectores y entornos sociales, los medios de identificación y verificación digital, cada vez más numerosos, inundan las relaciones cotidianas. La confusión, los errores, los costes y la frustración desaniman a los usuarios[9] y ahogan con ineficacias los procesos empresariales y sociales.

9. https://d2qcmozihn2auk.cloudfront.net/whitepapers/SG-Battle-to-onboard.pdf. La incorporación (onboarding) es una de las áreas cruciales en las que los proveedores están fallando. El abandono de aplicaciones por parte de usuarios frustrados que son incapaces de completar el proceso de incorporación es ahora más alto que nunca, llegando al 70% en algunos países.

Case in point

El proyecto TISA

Barclays, Signicat, OneSpan y Daon son algunas de las importantes empresas que se han unido al programa de identificación digital TISA (las siglas en inglés de La Alianza para la Inversión y el Ahorro). El objetivo del proyecto TISA es crear un sistema de identidad digital que permita a los consumidores establecer y reutilizar una identidad para interactuar con las instituciones financieras. Esto puede utilizarse cuando se solicitan productos y servicios financieros, como la apertura de una nueva cuenta bancaria, la transferencia de una pensión o la solicitud de una hipoteca. Los proveedores de servicios financieros pueden verificar con facilidad y luego autenticar la identidad digital de un cliente.

Case in point

ID reutilizable

Existe una oportunidad de negocio en proporcionar verificaciones reutilizables del tipo "conozca a su cliente" (KYC). Los principales objetivos son reducir la duplicación y la redundancia en el proceso de autenticación, y facilitar la incorporación. Las empresas están desarrollando soluciones basadas en blockchain para facilitar el KYC reutilizable. Cuando una entidad ha verificado a un usuario, otras empresas pueden aprovechar este KYC. El reconocimiento mutuo se basa en la confianza entre las entidades de autenticación y las que importan el KYC. Los incentivos para compartir el KYC y permitir su reutilización son económicos y estratégicos. A las entidades de autenticación se les compensa por sus verificaciones y además consiguen y retienen la relación con el cliente.

En el caso de las instituciones financieras, las oportunidades de negocio consisten en **actuar como un punto de identidad único para los usuarios.** Los puntos de identidad únicos pueden operar en los dos extremos de la línea de comunicación:

- Por un lado, el usuario se beneficia de una interfaz única y el proveedor del servicio gestiona, selecciona e interactúa con el tercero que solicita la identificación. Por ejemplo, la aplicación de reconocimiento biométrico desarrollada por Apple para sus iPhones proporciona al usuario un único punto de entrada a múltiples servicios de terceros. De media, una persona tiene alrededor de cien contraseñas, una cifra en solo en 2021 aumentó un 25%[10]. La interfaz de reconocimiento biométrico permite al usuario gestionar una cartera de contraseñas y credenciales con mucha facilidad y una interacción mínima.

10. https://tech.co/password-managers/how-many-passwords-average-person

- Por el otro, las aplicaciones centradas en la empresa pueden ayudar a compañías y autoridades a facilitar la identificación de usuarios en múltiples contextos, para múltiples fines y con una mínima exposición de la privacidad. Se estima que en 2025 estarán en uso más de 6.200 millones de aplicaciones de identidad digital, lo que agravará los problemas existentes generados por la fragmentación del mercado[11]. Además, se prevé que las empresas digitales que ofrezcan a sus clientes una mejor experiencia durante la corroboración de la identidad conseguirán un aumento de ingresos del 20% en comparación con sus competidores[12].

11.https://www.biometricupdate.com/202010/digital-identity-apps-to-outnumber-cards-by-2023-juniper-research

12. https://www.gartner.com/en/documents/3697317

In focus

Un argumento sólido en favor del papel de los bancos como "centros de identidad seguros"

El esfuerzo de los bancos por implementar obligaciones de KYC y AML les ha colocado en una posición incomparable para actuar como un tipo de **"centro de identidad seguro"** respaldado por las credenciales del sector público. El aprovechamiento de estas capacidades podría permitir nuevos servicios de identidad fiables y con posibilidad de elección por parte del usuario.

A. Confianza

Varios estudios internacionales han demostrado que los consumidores confían a los bancos la recogida y el tratamiento de sus datos personales. Un informe reciente del Banco de Pagos Internacionales (BPI)[13] destacó esta preferencia por los bancos frente a otros posibles actores en todos los segmentos demográficos. Por motivos de privacidad y protección de datos, quizá los consumidores prefieran que sean empresas del sector privado las que gestionen los atributos de datos sensibles que componen su "identidad", así como el historial de transacciones de lo que compran y con quién interactúan[14].

13. Olivier Armantier, Sebastian Doerr, Jon Frost, Andreas Fuster y Kelly Shue, "Whom do consumers trust with their data? US survey evidence", BIS Bulletin, n.º 42, 7 de mayo de 2021.

14. M. Baradaran, (2015), How the Other Half Banks: Exclusion, Exploitation, and the Threat to Democracy, Harvard University Press; I. Fu (2021), "The Freedman's Bank and the Persistence of Mistrust", mimeo; y E. Vaportzis et al. (2017), "Older adults' perceptions of technology and barriers to interacting with tablet computers: a focus group study", Frontiers in Psychology, n.º 8(1687).

B. Minimización y finalidad específica

La autenticación bancaria es fundamental para minimizar la exposición de la privacidad y garantizar una identificación/autenticación adecuada a cada finalidad. En función de cada transacción o de las situaciones que requieran autenticación, se decide qué datos del consumidor hay que aprobar[15].

Los modelos de "prueba de conocimiento cero" (ZKP, por sus siglas en inglés)[16] son muy prometedores, en la medida en que no revelan información adicional. ZKP es un método de verificación entre un probador y un verificador. El probador es capaz de demostrar al verificador que conoce determinada información sin revelar la información en sí. En la práctica, el probador puede demostrar que una afirmación concreta es cierta sin transmitir información adicional, más allá del hecho de que la afirmación es realmente cierta. Cabe destacar que la minimización de los datos y el control del usuario están integrados en el diseño. Gracias a su diseño, estas soluciones respetan la privacidad y cumplen el objetivo de identificación para una finalidad específica[17].

C. Terceros de confianza centrados en el usuario: las ventajas de los terceros de confianza centralizados para prevenir la desintermediación.

Existe una oportunidad estratégica muy prometedora en el aprovechamiento de la dinámica entre dos factores: la confianza y

15. Los estándares de la Fundación OpenID para las API financieras: este modelo prevé que el consumidor (o el usuario final de una pequeña empresa) pueda decirle a una de sus contrapartes de confianza existentes (como un banco, una empresa de telecomunicaciones o un minorista de energía) que verifique su identidad. https://openid.net/

16. El concepto ZKP fue descrito por primera vez por Goldwasser, Micali y Rackoff (1989) en su artículo "The Knowledge Complexity of Interactive Proof Systems", SIAM Journal on Computing, vol. 18, n.º 1, pp. 186-208, febrero de 1989. En el artículo, las ZKP se definen como "aquellas pruebas que no transmiten conocimiento adicional, más allá de si la proposición en cuestión es correcta".

17. Global Assured Identity Network (GAIN), https://gainforum.org/. "En lugar de iniciar la sesión directamente, el usuario pide a un proveedor regulado y de confianza (por ejemplo, su banco, proveedor de telecomunicaciones u otra entidad regulada) que verifique que él es la persona y/o cuenta con las credenciales que afirma tener".

el alcance. Si bien las grandes empresas tecnológicas han obtenido una escala mundial y han aprovechado su presencia en la economía digital proporcionando una experiencia muy sencilla como "centro de identidad" (alto alcance), la adopción generalizada de estas soluciones sencillas es inestable, porque no está respaldada por altos niveles de certeza y fiabilidad. Las soluciones de autenticación que ofrecen estas plataformas son cómodas para los usuarios, pero no proporcionan seguridad ni la verificación de la identidad detrás de una cuenta o nombre de usuario[18].

Por el contrario, las instituciones financieras se encuentran en una situación muy favorable en términos de confianza, como se ha explicado antes, y han desarrollado en profundidad habilidades, prácticas y experiencias fundamentales en KYC, AML y autenticación que pueden extrapolarse de manera efectiva a soluciones de autenticación de gran alcance. El alcance debe basarse en acuerdos de cooperación y modelos de colaboración entre instituciones financieras y con otras entidades[19]. La confianza es una fortaleza, mientras que el alcance limitado sigue siendo una debilidad: la oportunidad estratégica está en reforzar ambos.

D. La necesidad de unificar el fragmentado mundo de la identidad

Las instituciones financieras están en posición de aprovechar una ventana de oportunidad, catalizando una red de identidad descentralizada, colaborativa a escala mundial y técnicamente interoperable que supere las limitaciones de los modelos centrados en el ciudadano y dirigidos por el Gobierno, y que gane en escala y alcance acumulando confianza.

18. Foro Económico Mundial, A Blueprint for Digital Identity. The Role of Financial Institutions in Building Digital Identity, agosto de 2016.

19. Ejemplo de proyecto de colaboración: ID2020 Alliance, https://id2020.org/alliance

Case in point

GlobaliD

Uno de los principales retos de la identidad digital es que sea completa. Por lo tanto, hacer posible que sea completa y trazable es una oportunidad de negocio que conviene estudiar. GlobaliD[20] está trabajando en este objetivo, operando una especie de "DNS para la identidad". Las verificaciones de la identidad están vinculadas a un nombre incluido en el espacio de nombres público de GlobaliD. Aunque los usuarios tienen derecho a tener varios nombres y, por lo tanto, a satisfacer sus expectativas de preservación de la privacidad, GlobaliD permite la trazabilidad para crear una visión completa del usuario. Al actuar como red troncal (backbone) de la identidad, GlobaliD se conecta a los verificadores de identidad a través de silos, incluyendo las identidades autosoberanas.

IMPULSOR 3: La identidad digital como una recuperación del anonimato responsable

Las herramientas de identidad digital deben satisfacer una creciente demanda de "anonimato responsable" en los entornos digitales. Hay que encontrar un equilibrio delicado: una identidad fiable y cierta con unos estándares más altos de protección de la identidad y una demanda cada vez mayor de minimizar la exposición de la privacidad.

20. https://www.global.id/

Puede observarse cómo, conjuntamente, varios de los impulsores identificados explican la aparición de determinadas soluciones, y cómo se conciben y evolucionan ciertos modelos en respuesta a varios de estos impulsores. En concreto, la inversión en anonimato responsable está generando soluciones, aplicaciones y oportunidades de negocio que refuerzan simultáneamente la identidad autosoberana y proporcionan soluciones de identidad con una finalidad específica (impulsor 2), mientras exigen soluciones centradas en el usuario y llevadas a cabo por actores privados, más allá de las soluciones centradas en el ciudadano dirigidas por Gobiernos y autoridades públicas (impulsor 1).

En el marco de este impulsor, llaman la atención dos modelos prometedores:

A) Tokens soulbound

Los autores de un artículo reciente sobre la sociedad[21], que han acuñado el concepto de token Soulbound (SBT, por sus siglas en inglés), sintetizan este incipiente paradigma en la siguiente descripción:

> *En lugar de la privacidad como un derecho de propiedad transferible, un enfoque más prometedor es tratar la privacidad como un conjunto de derechos, programables y poco acoplados, de permiso de acceso, modificación de la información o beneficio derivado de ella. Con este paradigma, cualquier SBT —por ejemplo, un SBT que representa una credencial o el acceso a un almacén de datos— tendría idealmente un derecho de propiedad programable implícito que especifica el acceso a la información subyacente que constituye el SBT: los titulares, los acuerdos entre ellos, la propiedad compartida (por ejemplo, los datos) y las obligaciones con terceros (p. 15).*

Los tokens Soulbound permiten a los usuarios demostrar quiénes son sin desvelar su identidad y sin que una autoridad central responda por ellos. De este modo, hacen posible una herramienta de identidad respetuosa con la privacidad, así como el ejercicio del anonimato responsable. Los usuarios, al utilizar los tokens Soulbound,

21. Eric Glen Weyl, Puja Ohlhaver y Vitalik Buterin, "Decentralized Society: Finding Web3's Soul", 10 de mayo de 2022. Disponible en SSRN: https://ssrn.com/abstract=4105763 o http://dx.doi.org/10.2139/ssrn.4105763

pueden tener múltiples identidades, anónimas pero verificables, conocidas como souls.

Los tokens Soulbound se guardan en souls. Una soul es la cuenta o cartera de un usuario que puede tener tokens Soulbound. Una soul puede ser una persona, una institución o cualquier entidad. En principio, como un usuario puede tener varias carteras para guardar criptoactivos, NFT o cualquier tipo de activo digital, también puede tener varias souls. Sin embargo, y curiosamente, solo se puede tener un token Soulbound específico en una soul y no se puede transferir a otra soul.

A diferencia de los sistemas centralizados y burocráticos para conferir identidad propios de la economía actual (un "permiso de conducir"), el nuevo paradigma de la sociedad descentralizada se basa en declaraciones sociales horizontales ("entre pares") con tokens Soulbound. Así, los tokens Soulbound son tokens permanentes, intransferibles y no fungibles (NFT). Los tokens Soulbound, como catalizadores esenciales de la transición de las DeFi (finanzas descentralizadas) a la DeSoc (sociedad descentralizada), no tienen un valor financiero significativo, pues el valor que aportan es la acreditación del historial de las souls o de las comunidades conectadas.

Entre sus posibles aplicaciones, los tokens Soulbound pueden aportar soluciones centradas en el usuario para los siguientes fines: identidad y autenticación, calificación crediticia, requisitos KYC, DAO (las siglas en inglés de Organización Autónoma Descentralizada) y varias formas cooperativas, contribuyentes verificados o votaciones. Los tokens Soulbound serán múltiples y variados, porque pueden ser emitidos bajo diversas modalidades o en diferentes condiciones. Algunos ejemplos pueden ilustrar diferentes posibilidades que interesa estudiar:

- Algunos emisores optarían por hacer totalmente públicos los tokens Soulbound.
- Algunos tokens Soulbound, como un pasaporte o un historial de salud, serían privados en un sentido autosoberano, con derechos unilaterales de divulgación para la soul que tiene esos tokens Soulbound.
- Otros, como los tokens Soulbound que reflejan la pertenencia a una cooperativa de datos, tendrían permisos de votación multifirma o comunitarios más sofisticados, en los que todos o una mayoría cualificada de los titulares de los tokens deben dar su consentimiento a la divulgación.

In focus

¿Quién está emitiendo tokens Soulbound?

Binance está emitiendo tokens Soulbound como credenciales de identidad para los usuarios que completaron la verificación KYC. Se llama Binance Account Bound (BAB). Binance es un ecosistema blockchain y proveedor de infraestructura de criptomonedas que incluye el mayor mercado para activos digitales por volumen. El token Soulbound, BAB, se muestra en la cartera para acreditar que el titular ha sido evaluado por Binance según los requisitos KTC.

Según ha anunciado Binance, sus tokens Soulbound (BAB) tienen las siguientes características. En primer lugar, los BAB son intransferibles. Por lo tanto, los usuarios no pueden transferir tokens BAB a otros usuarios. En segundo, los BAB son revocables. Así, los usuarios pueden revocar sus tokens BAB. En tercer lugar, los BAB son únicos. Así, un ID de usuario de Binance verificado permite al usuario acuñar un token BAB solo en una cadena determinada.

Tras el anuncio de la emisión, catorce destacados proyectos web3 han adoptado los tokens Soulbound y ofrecen a los titulares de tokens BAB incentivos exclusivos. Por ejemplo, los titulares de BAB tendrán un derecho de voto especial para mejorar la gobernanza de la DAO y la gestión de las disputas; los titulares de BAB están exentos de KYC y se les conceden derechos de voto; y se indicará en el perfil del usuario que es un usuario real (no un bot).

B) Tokens de identidad y/o ciertos atributos de un solo uso emitidos por entidades fiables

Este modelo combina la oportunidad de negocio que supone actuar como un "centro de identidad seguro", el objetivo de minimizar la exposición de la privacidad con soluciones específicas para atributos y los beneficios de la sociedad descentralizada con los NFT.

Un tercero de confianza (registrador, entidad financiera, actor fiable, etc.) emite, a petición del usuario, un token de un solo uso relacionado con la identidad del usuario y/o uno o varios atributos. El usuario emplea ese token para identificarse, acceder a un servicio o acreditar un atributo requerido (edad legal, matriculación, pago de impuestos, estar empleado, etc.).

IMPULSOR 4: La identificación biométrica y los servicios de autenticación para una vida físico-digital

La biometría facial impulsará un mercado de la identidad digital innovador y prometedor. Una serie de contextos híbridos físico-digitales se beneficiarán de una identificación y autenticación biométrica facial sencilla y fiable. Varios factores convergentes predicen una notable expansión del sector.

A. Sin interacciones cara a cara. Como consecuencia de la limitación de las interacciones sociales adoptada para contener la pandemia de COVID, se han implementado muchos dispositivos "*contactless*" o sin contacto, que mantienen la distancia personal, para la identificación y autenticación en entornos físicos. El uso del reconocimiento biométrico se ha generalizado, desde el control de acceso de los empleados a edificios públicos, universidades o empresas privadas, hasta el control de pasaportes.

B. El crecimiento sin precedentes del teletrabajo y el trabajo a distancia genera muchas situaciones profesionales y laborales en las que es necesario una identificación inmediata y eficaz de las personas. El reconocimiento facial puede utilizarse para calcular las horas de trabajo, verificar la asistencia a programas de formación, garantizar la admisibilidad a reuniones, a espacios protegidos o datos confidenciales o restringidos.

C. La popularidad de las aplicaciones para dispositivos móviles (y otros

dispositivos de mano) ha permitido la implementación generalizada del reconocimiento facial para desbloquear dispositivos, acceder a aplicaciones, expresar consentimiento en diversas transacciones (por ejemplo, confirmar una transferencia de fondos, modificar datos personales relevantes, firmar o descargar contenido digital) o realizar pagos.

D. Los procesos de incorporación tradicionales aspiran a convertirse en actividades puramente digitales: la apertura de una cuenta, la verificación de KYC, los procesos de ALM (las siglas en inglés de gestión del ciclo de vida de las aplicaciones), la solicitud de un préstamo, etc.

E. En la economía de plataformas, la verificación está ganando escala y relevancia. Resulta interesante que el Reglamento de Servicios Digitales[22] recientemente adoptado estipule el requisito KYBU (las siglas en inglés de "conoce a tu usuario profesional") para los mercados B2C[23]. En este sentido, las plataformas *online* "que permiten a los consumidores cerrar contratos a distancia con comerciantes deberán garantizar que estos últimos solo puedan utilizar dichas plataformas *online*" si, con anterioridad, estas han obtenido determinada información del comerciante y hacen lo posible para garantizar que sea completa y fiable.

En todos estos escenarios, el reconocimiento facial, sumado a la identificación y autenticación por vídeo, puede permitir desbloquear muchos de los obstáculos en los procesos de incorporación, optimizar los procesos de identificación recurrentes en entornos profesionales, políticos o educativos (votaciones, empleados autorizados, estudiantes matriculados, etc.), y mejorar la seguridad y la certeza en muchos contextos empresariales y sociales (reuniones de negocios, actos sociales, seminarios, etc.).

22. Reglamento (UE) 2022/2065 del Parlamento Europeo y del Consejo de 19 de octubre de 2022 relativo a un mercado único de servicios digitales y por el que se modifica la Directiva 2000/31/CE (Reglamento de Servicios Digitales). OJ L277/1, 27.10.2022.

23. Reglamento de Servicios Digitales, Art. 30, Trazabilidad de los comerciantes.

Según el ciclo de sobreexpectación de Gartner más reciente (2022), la biometría de terceros está pasando ahora por la fase de la desilusión. Eso significa que hay que estimar que tardará entre dos y cinco años en alcanzar la meseta de productividad. Dentro de ese marco temporal, las soluciones relacionadas con la biometría seguirán despertando interés. En concreto, las modalidades de la videoidentificación más intensivas en biometría puede seguir suscitando grandes expectativas y proporcionando, en determinadas circunstancias sociales y tecnológicas, soluciones eficaces en las economías en desarrollo; conjuntamente con la alta penetración de los dispositivos móviles para servicios financieros y de contratación (dinero móvil y comercio móvil).

In focus

¿Hacia dónde mirar? Las posibilidades y las limitaciones de la identificación por vídeo

La incorporación del cliente es un proceso clave que supone importantes trabas para muchos sectores (y resulta especialmente crítico para algunos, como el financiero, la banca o los seguros). Es una tarea compleja, costosa, que requiere tiempo y normalmente se inicia o completa con interacciones cara a cara. Sin embargo, una economía digital próspera no puede depender de los procesos presenciales.

La videoidentificación es una solución en crecimento y que conviene tener en cuenta. Se trata de un proceso de identificación y verificación de la identidad basado en un vídeo de alta definición grabado que muestra a la persona y su documento en directo, con gran detalle. El vídeo se graba y se sella electrónicamente para mantener su integridad, al igual que se hace con datos primarios como la dirección IP, el dispositivo y la ubicación, como prueba electrónica principal de la identificación.

Una variante del reconocimiento facial que resulta tentadora es el "Smile ID". La identidad del usuario se autentica mediante el reconocimiento y la verificación de su sonrisa. Es un método rápido, sencillo y efectivo que puede suponer una minimización de la exposición de la privacidad. Puede reducir el alcance y la cantidad de datos biométricos que se recogen y almacenan. De este modo, se limita el riesgo de ciberseguridad de un acceso autorizado o de una clonación.

En este ámbito, algunas empresas están aprovechando la combinación de la biometría con los teléfonos móviles para permitir la autenticación en economías en desarrollo de África y el Sudeste Asiático, mientras que otras están aprovechando igualmente la biometría, y otras técnicas avanzadas, para permitir la autenticación móvil a escala mundial.

IMPULSOR 5: La identidad digital en las realidades extendidas/aumentadas

La identidad digital se convertirá en un conjunto de identidades digitales que acompañarán nuestra "vida digital" en los metaversos y otras realidades extendidas/aumentadas. El concepto y las herramientas de la identidad digital deben evolucionar para acoger y hacer posible el fenómeno, prometedor y complejo, de las identidades digitales múltiples, y poder innovar en él: la portabilidad, la reputación generada por avatares, la manifestación de derechos privados, la ampliación de datos personales, la realidad extendida y aumentada. Las nuevas tecnologías inmersivas no funcionarán ni prosperarán sin una identidad digital sólida y fiable. Todavía no ha surgido, ni se ha expandido, una manera efectiva de implementar una identidad digital de uso general.

En el metaverso, las soluciones de identidad tienen que proporcionar mecanismos eficaces y sencillos para acceder y crear conexiones significativas entre la identidad del usuario, sus dispositivos y sus avatares. La portabilidad será crucial. Las empresas que deseen atraer a más usuarios tendrán que permitirles llevar su identidad digital a todo el metaverso, con independencia del punto de entrada o la plataforma; por ejemplo, implementando un estándar universal similar al de la tecnología de estudio virtual (VST, por sus siglas en inglés) para los avatares de audio.

Case in point

¿En qué soluciones están trabajando las empresas?

Las herramientas que abrevian el oneroso proceso de gestión de claves hacen posible que los usuarios finales inicien sesión en dApps (aplicaciones descentralizadas) sin necesidad de utilizar software de terceros. Las dApps son aplicaciones descentralizadas que se ejecutan en una blockchain o una red de ordenadores entre pares en lugar de depender de uno solo. Así, las dApps están fuera del ámbito de una única autoridad y libres de las interferencias de esta. Las soluciones desarrolladas permiten al usuario integrar fácilmente su aplicación con la blockchain de Ethereum, tanto si el usuario ya tiene una dApp integrada con web3 como si empieza desde cero.

Los navegadores que preservan la privacidad o los navegadores compatibles con un sistema de identidad tokenizado están diseñados específicamente para trabajar con diversas aplicaciones descentralizadas, o dApps, así como para proporcionar una funcionalidad más profunda que un navegador tradicional con un complemento básico de cartera web. El navegador también incluye una nueva cartera cripto nativa no custodiada que te permite acceder a tu cripto o firma en dApps directamente desde el navegador, sin necesidad de instalar una extensión.

In focus

Retos en el metaverso... que pueden ser una oportunidad estratégica

1. Asegurar los dispositivos de internet de las cosas

(IoT, por sus siglas en inglés): Nuestra "inmersión" en el metaverso y nuestra interacción con diversas realidades extendidas/aumentadas dependen de un universo de dispositivos y están "interconectadas" con ellos: gafas de realidad aumentada (RA), auriculares de realidad virtual (RV), guantes de RV, bandas de muñeca, etc. Estos dispositivos interconectados son fundamentales para garantizar una experiencia inmersiva segura, fiable y de calidad en el metaverso y las realidades aumentadas/extendidas. Los riesgos asociados son numerosos y variados, desde la seguridad de los dispositivos de *hardware*, hasta la protección contra las vulnerabilidades y exposiciones del *firmware* y el *software*.

¿Qué soluciones se están desarrollando?

- Soluciones para "monitorear el tráfico entre los dispositivos y los entornos de la nube, con el fin de detectar anomalías de comportamiento o patrones de tráfico que puedan ser indicativos de una amenaza o de una exfiltración de datos".
- Soluciones para proteger los dispositivos IoT/OT de los problemas de seguridad del *firmware*, las vulnerabilidades y exposiciones comunes (CVE, por sus siglas en inglés), los secretos comerciales y muchos otros problemas de seguridad en complementos (*plugins*) de dispositivos IoT y el *firmware* integrado.

- Soluciones y servicios sobre descubrimiento de activos, gestión de vulnerabilidades y monitorización continua de amenazas.

2. Datos y privacidad

La exposición de la privacidad es un riesgo al que hay que hacer frente en el metaverso y en las realidades aumentadas/extendidas. Las características inmersivas y sensibles de estas experiencias pueden agravar la importancia de la exposición de la privacidad y/o la gravedad del impacto en caso de infracción. Por otro lado, en ausencia de mecanismos de identificación sólidos y fiables (soluciones de identidad digital) en estos escenarios, aumentan los riesgos de suplantación, fraude, usos no autorizados o transacciones no rastreables. En consecuencia, surgen oportunidades de negocio tanto en el ámbito de las soluciones para proteger la privacidad como en aquellos dedicados a la verificación de la identidad.

¿Qué soluciones hay en el mercado?

- Software de investigación que conecta las transacciones de criptomonedas con entidades del mundo real y analiza actividades delictivas como el movimiento de fondos robados, así como actividades legítimas como los préstamos flash y las transferencias de NFT.
- Soluciones para prevenir la apropiación de cuentas y el fraude: recopilación de datos recapturados de infracciones, dispositivos infectados con malware y otras fuentes ocultas.

05 Consideraciones finales

La identidad digital es un mercado floreciente. Identificamos cinco impulsores que alimentan su potencial de crecimiento y expansión en los próximos años, y la creación de valor y las oportunidades de innovación e inversión gravitan en torno a las tendencias trazadas (o señaladas) por estos cinco impulsores.

La identidad digital está virando hacia modelos granulares, más definidos y con fines específicos. Las soluciones más prometedoras giran en torno a proporcionar, verificar y autenticar la identidad digital o atributos específicos para un fin concreto (edad legal, vacunación, elegibilidad, etc.), con una reducida exposición a la privacidad y una gran versatilidad. Como se ha explicado, hay dos modelos que pretender abordar esta tendencia. Por un lado, los modelos centralizados con un "centro de identidad seguro" (terceros de confianza), pero también agregadores, interfaces y tokens verificados de un solo uso. Por otro lado, soluciones descentralizadas o distribuidas como los tokens Soulbound y soluciones funcionalmente equivalentes.

En este contexto, **en los próximos años los modelos de identidad digital transfronteriza van a ser fundamentales.** El modelo EUDI ofrece una oportunidad incomparable para probar soluciones y descubrir áreas atractivas para la inversión. Hay que prestar mucha atención a los estándares y requisitos técnicos que señalará la implantación de la cartera EUDI y el desarrollo de su caja de herramientas (*toolkit*).

El potencial de la identificación biométrica sigue ampliándose y demuestra ser una solución versátil para entornos *online, offline* e híbridos. A pesar de que algunas soluciones, como la videoidentificación, parecen haber perdido impulso, las aplicaciones biométricas impregnan una gran variedad de situaciones en las que son necesarias la verificación de la identidad y la identificación y verificación de atributos.

Una estrategia con visión de futuro debe integrar y abordar otros retos planteados por una vida digital "multiplicada" en las realidades extendidas/aumentadas. Una protección integral y completa de la identidad digital en el metaverso y las realidades ampliadas/extendidas requiere una combinación de soluciones para asegurar los dispositivos, proteger el *firmware/software* y preservar los datos y el contenido digital.

Autora

Teresa Rodríguez de las Heras Ballell

Profesora de Derecho Mercantil en la Universidad Carlos III de Madrid, España

Visitante académica en la Facultad de Derecho de la Universidad de Cambridge, 2022-2023; Sir Roy Goode Scholar en UNIDROIT, 2021-2022. Árbitro de la Corte de Arbitraje de Madrid y de España. Miembro de los siguientes *Grupos de Expertos de la UE* que asisten a la Comisión: *Expert Group on Liability/Technologies formation*, elaborando el *Informe Liability for AI and other emerging technologies; Expert Group to the EU Observatory on Platform Economy; Expert Group on B2B Data Sharing and Cloud Computing.*

esade

Santander X Innovation Xperts

www.santander.com/santander-x-innovation-xperts-es

By Santander