COLADE 2026 · CONFERENCIA MAGISTRAL

La Identidad Soberana ante la Frontera de los Neurodatos y la IA

Redefiniendo la propiedad del "yo" en la banca

Marcos Allende López
CEO y Cofundador, Blerify

San Salvador · 15 de octubre de 2026




RÉPUBLIQUE FRANÇAISE
DUPONT
Chloé Marie
F
FRA
12 07 2031
PARIS
X4RTBPFW4
12 07 2031
Signature
384213


Face Selection
Local Upload

LA PREGUNTA DEL MILLÓN

¿Hasta cuándo podremos seguir confiando en la biometría remota para verificar a nuestros clientes?

Con la IA, la biometría remota por sí sola ya no es un factor de alto nivel de confianza

ÍNDICE

Recorrido

01 El KYC tradicional ya no sirve

02 Ante la IA, dos opciones para verificar clientes

03 La identidad se vuelve digital y criptográfica

04 Esto ya está pasando

05 El marco regulatorio habilitante

06 Estándares, comparativa con cripto wallet y desafíos

07 Agentes IA, el siguiente paso

08 La dimensión cuántica

Cierre · reflexiones para llevarse

01

El KYC tradicional ya no sirve

La IA está invalidando la forma en que la banca verifica a sus clientes.

EL PROBLEMA

La IA está jubilando los dos factores clásicos de autenticación

"Algo que sabes"

26 mil M

intentos de credential stuffing al mes

Las contraseñas como autenticación primaria están estructuralmente rotas.

Fuente: Akamai / Okta threat reports

"Algo que eres"

1 de 5

intentos de fraude biométrico ya involucran deepfakes con IA

La biometría facial remota, método dominante de onboarding en LAC, deja de ser un buen factor único.

Fuente: Entrust, Identity Fraud Report 2025

EL PROBLEMA

El gran desafío: una identidad biométrica robada se usa mil veces, sin rastro y sin correlacción

1 → **1.000** → **0**

biometría robada o sintética
comprada o generada con IA

cuentas abiertas en paralelo
cada apertura pasa el liveness y face match

rastros del hacker
nadie correlaciona ni persigue

Sin unicidad

Cada verificación es un evento aislado sin correlacción: nadie puede decir "esta persona ya tiene una identidad activa diferente".

Sin trazabilidad

La evidencia no queda firmada ni vinculada a un dispositivo: el fraude no deja rastro forense.

Sin revocabilidad

Una biometría filtrada no se puede cancelar: tu cara “robada” sigue siendo tu cara para siempre.

02

Ante la IA, dos opciones para verificar clientes

IA contra IA, o confianza criptográfica.

LA BIFURCACIÓN

Dos caminos: cada vez más datos o cada vez más verificabilidad

CAMINO A · MÁS DATOS - IA BUENA VS IA MALA

- Lo que tienes · código por SMS
- Lo que eres · rostro, huella
- Cómo te comportas · tecleo, voz, gestos
- **Lo que sientes · estrés, emoción**
- **Lo que piensas · neurodatos**

CAMINO B · MÁS VERIFICABILIDAD – CRIPTOGRAFÍA

"Algo que tienes SOLO TÚ"

Un documento de identidad digital firmado por el Estado o proveedor de identidad certificado, en el dispositivo del ciudadano.

La certeza viene de la criptografía, no de acumular datos sobre la persona.

Más certeza · menos datos · más control

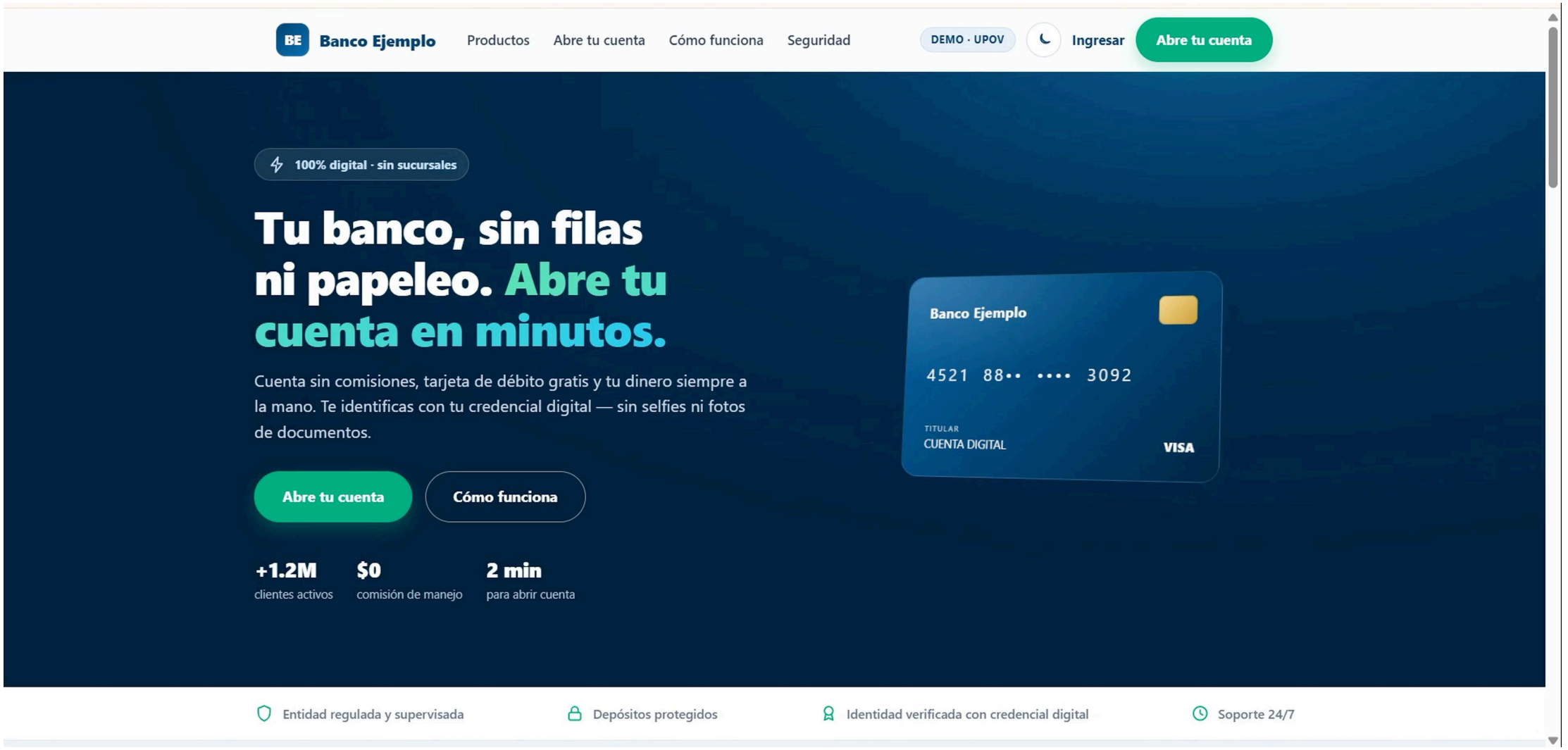
03

La identidad se vuelve digital y criptográfica

Y eso cambia la relación entre el ciudadano, el Estado y el banco.

UN NUEVO PARADIGMA BASADO EN DOCUMENTOS DIGITALES Y CRIPTOGRAFÍA

Así se ve el futuro de la verificación de identidad de clientes



EL PRODUCTO · ENROLAMIENTO Y AUTENTICACIÓN

Lo que experimenta el ciudadano en cuatro pasos

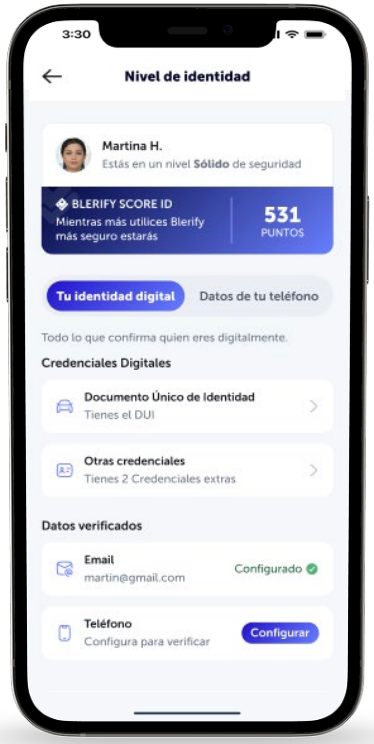
1 Crea su cuenta

Descarga la ID Wallet y se verifica en persona o contra el motor biométrico del estado de manera remota.



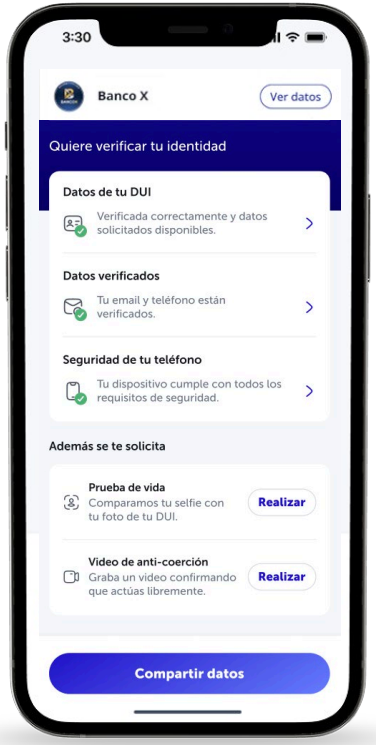
2 Obtiene su identidad digital

Crea una pareja de llaves criptográfica y recibe su ID digital.



3 Aprueba y comparte

Da consentimiento explícito a cada entidad que le solicita datos, verificando previamente quién es y si está autorizada.

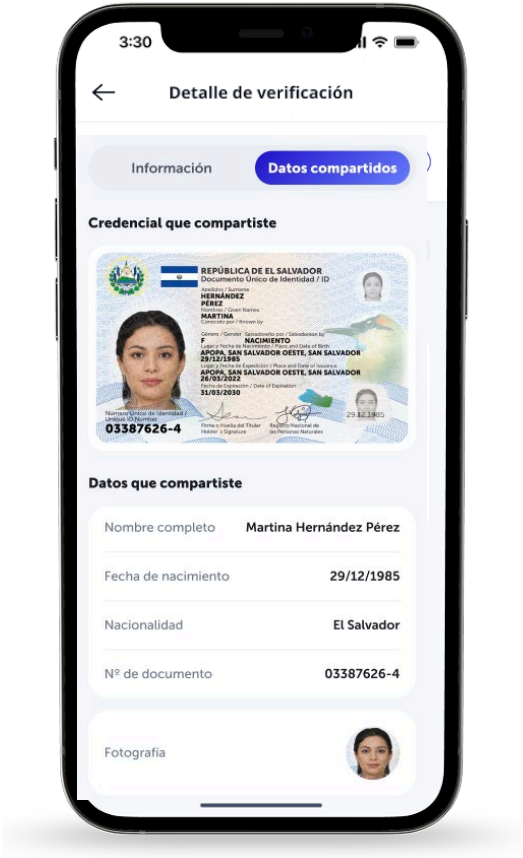


4 Monitorea su historial

Cada verificación es trazable en su historial local, consultable en el tiempo.



La ID Wallet y ID digital, mecanismo ideal de KYC y AML



Apertura de cuenta remota

Identidad completa del registro civil, sin foto del documento ni selfie que interpretar.

Certeza del emisor · Vínculo al titular

Autenticación reforzada

Login de alto riesgo o cambio de dispositivo con la llave del teléfono, sin SMS.

Vínculo al titular

Firma de contratos y créditos

El cliente firma con su identidad verificada; queda evidencia con valor probatorio.

Trazabilidad

Transferencias de alto valor

Confirmación y atestación del dispositivo en el momento.

Vínculo al titular · Trazabilidad

Prueba de datos aislados

Mayoría de edad o residencia sin copiar el documento completo.

Minimización

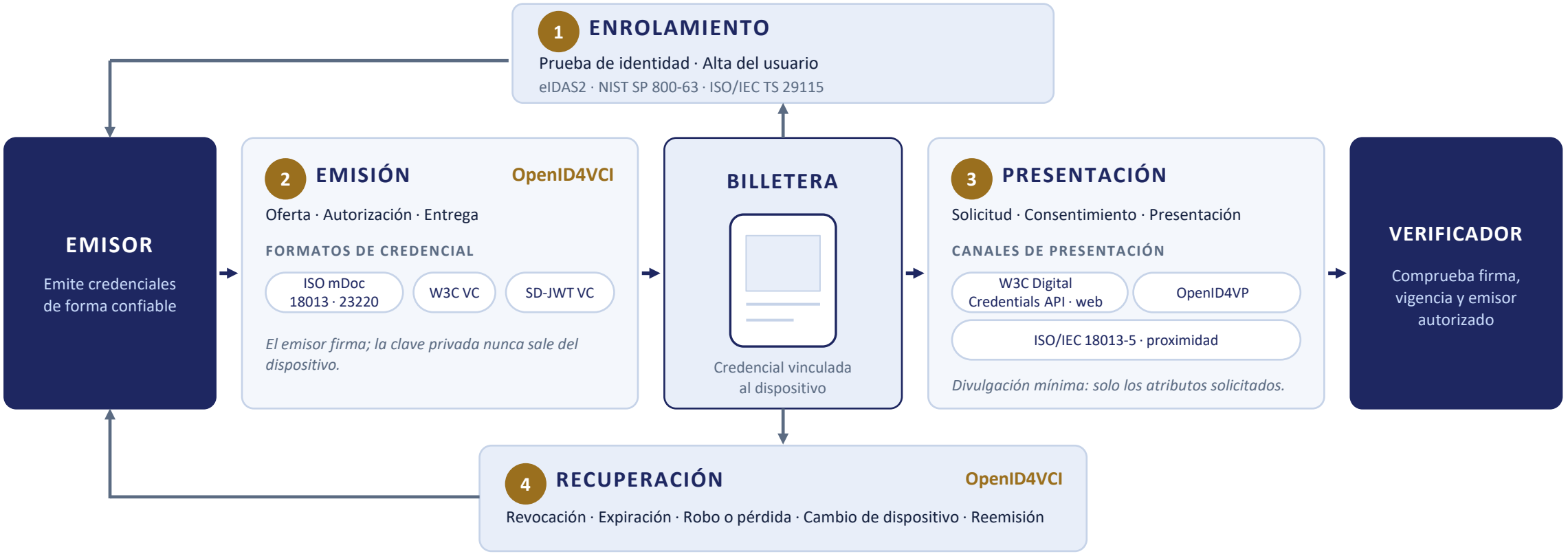
Recuperación de acceso

El cliente recupera su cuenta presentando su credencial de identidad digital.

Reutilización · Revocabilidad

EL FLUJO · ENROLAMIENTO, EMISIÓN, PRESENTACIÓN, RECUPERACIÓN

El ciclo de vida de un ID digital criptográfico



CONFIANZA TRANSVERSAL

Tres planos independientes, cada uno con su propia vía de revocación

1 · Autenticación

¿Quién es este participante?

- ISO/IEC 18013-5 · IACA y VICAL
- ETSI TS 119 612 y TS 119 602 · listas de confianza
- OpenID Federation 1.0 · W3C DID

2 · Autorización

¿Está autorizado a actuar?

- ETSI TS 119 475 · atributos del verificador
- ETSI TS 119 411-8 · certificados de acceso
- ARF EUDIW · registro nacional de verificadores

3 · Estado

¿La credencial sigue vigente?

- IETF Token Status List · en cola de publicación
- W3C Bitstring Status List
- RFC 5280 CRL y RFC 6960 OCSP · capa PKI

Contenido derivado de obra del BID y CDPI bajo licencia CC. No distribuir sin consentimiento

ATRIBUTOS Y EVIDENCIAS

El banco decide qué exigir según el riesgo de cada operación: atributos que se revelan y evidencias que se verifican

ATRIBUTOS · LO QUE SE REVELA

- Nombre y apellidos
- Tipo y número de documento
- Fecha de nacimiento, o solo "mayor de 18"
- Nacionalidad y dirección
- Retrato verificado

Divulgación selectiva: cada regla pide solo lo que necesita.

EVIDENCIAS · LO QUE SE COMPRUEBA

- ✓ Firma del emisor y estado de vigencia
- ✓ Firma del titular con llave del dispositivo
- ✓ Nivel de garantía del enrolamiento
- ✓ Atestación de la llave en hardware
- ✓ Integridad de la app y del dispositivo
- ✓ Señales anti-fraude y anti-coerción

EL CAMBIO DE PARADIGMA

Siete propiedades de la nueva identidad que la biometría sola no puede dar

1

Certeza del emisor

El documento es auténtico, de una autoridad reconocida.

2

Vínculo al titular

Firma con una clave que nunca sale de su dispositivo.

3

Unicidad

Una sola identidad activa por persona, a la vez.

4

Revocabilidad

Si se pierde o se roba, se cancela y se re-emite.

5

Trazabilidad

Cada uso deja evidencia firmada, útil como prueba.

6

Reutilización

El documento digital criptográfico se usa ilimitadamente en vigencia.

7

Minimización

Se revela solo el atributo necesario; el banco no custodia biometría.

Comparativa de document físico, digital y biometría

Certeza que se obtiene	DOCUMENTO FÍSICO PRESENCIAL	BIOMETRÍA REMOTA	DOCUMENTO DIGITAL CRIPTOGRÁFICO
¿El documento es válido?	~	?	✓
¿Lo emitió una entidad confiable?	~	?	✓
¿Está vigente, no revocado?	~	?	✓
¿Quien lo presenta es el titular?	~	?	✓

✓ Certeza plena

~ Comprobación visual o manual

? Sin forma de comprobarlo

TRAZABILIDAD

Cada verificación deja una huella auditable

1

Qué se verificó

Atributos, evidencias, tipo de documento y regla aplicada.

2

Cómo se verificó

Protocolo de presentación, canal, sellos de tiempo y firmas criptográficas.

3

Dónde y quién

Operador, sucursal o canal digital, dispositivo y momento exacto.

Para el derecho financiero

La verificación deja de ser un "aprobado" en un log y pasa a ser un expediente firmado: útil ante el supervisor, en una auditoría de cumplimiento y como prueba en un litigio.

GARANTÍAS NIST SP 800-63

Las billeteras de identidad los ID digitales impactan en las tres dimensiones de la verificación digital

		BIOMETRÍA DE UN SOLO USO	DOCUMENTO DIGITAL EN BILLETERA
IAL	**Garantía de identidad** ¿Es quien dice ser? Rigor del enrolamiento.	✓ IAL-2	✓ hasta IAL-3
AAL	**Garantía de autenticación** ¿Es la misma persona en cada sesión posterior?	—	✓ AAL-3
FAL	**Garantía de la prueba compartida** ¿La prueba es del titular y no una copia?	—	✓ FAL-3

Se pueden cubrir los tres ejes donde hoy se cubre uno.

04

Esto ya está pasando

No es una promesa: hay estándares, plazos y países en producción.

CONVERGENCIA GLOBAL

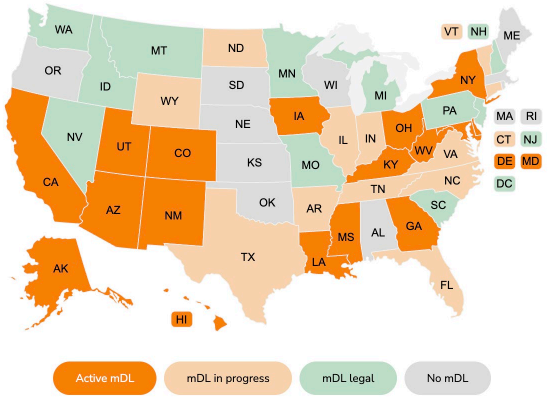
El mundo converge hacia billeteras de identidad interoperables

Unión Europea



eIDAS2 obliga a los Estados a ofrecer una ID Wallet (~dic 2026) y al sector privado a aceptarla (~dic 2027).

Estados Unidos



~30 estados ya implementan licencia de conducir móvil (mDL) en wallets, con aprobación de TSA para viajar nacionalmente.

América Latina y Caribe



7 países en 2026: Panamá, El Salvador, Uruguay, Rep. Dominicana, Perú, Costa Rica y Honduras con proyectos activos sobre ISO/IEC 18013-5.

Mismos estándares: ISO 18013-5, OpenID4VCI, OpenID4VP.

ESTADO DEL ARTE · UNIÓN EUROPEA

eIDAS2

Unión Europea

20 MAY 2024

En vigor

Reglamento (UE) 2024/1183

6 DIC 2026

Estados miembro

≥1 billetera certificada por país

6 DIC 2027

Sector privado

Aceptación obligatoria (banca, energía, telecom…)

2030

Meta política

80% de ciudadanos con billetera

Relevancia para LAC: la separación explícita emisión / operación de billetera / verificación es un modelo de capas directamente transferible; el ARF es público y reutilizable.

450 M

ciudadanos potenciales

Dic 2026

billetera obligatoria por Estado

80 %

meta de uso activo en 2030

mDL

Estados Unidos



Aceptado por la TSA (21 + PR)

Programa en desarrollo

Sin iniciar (4)

21 + PR

estados con mDL aceptado por la TSA en puntos de control (ene 2026)

solo 4

estados sin iniciar programa: Alabama, Maine, Massachusetts y Nebraska

~30

jurisdicciones proyectadas con mDL para 2026

NY 200k+ · GA 500k+

inscripciones reportadas; sin registro nacional único de adopción

Caso de uso inicial: viajes nacionales.

REAL ID en vigor desde may-2025 y TSA ConfirmID ($45) desde feb-2026. Emisión multicanal: app estatal, Apple, Google o Samsung Wallet.

ADOPCIÓN REGIONAL

LAC sigue el mismo camino

Costa Rica
Cédula digital desde 2025

El Salvador
DUI digital, 2026

Panamá
Licencia y cédula, 2026

Honduras
DNI y licencia digital

Perú
Cédula y licencia, 2026

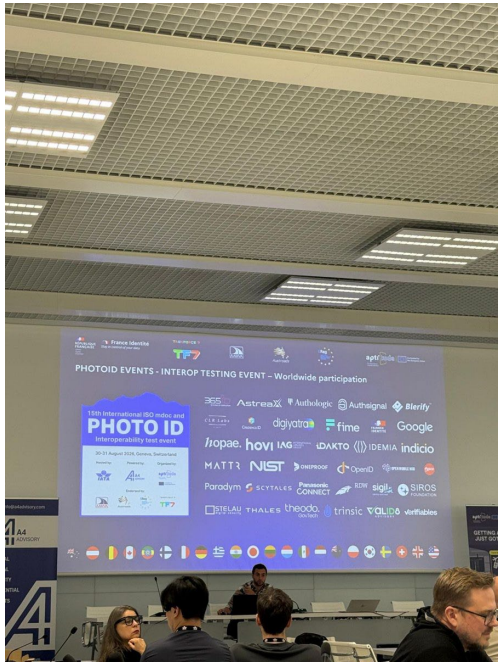
R. Dominicana
Cédula y licencia, 2026

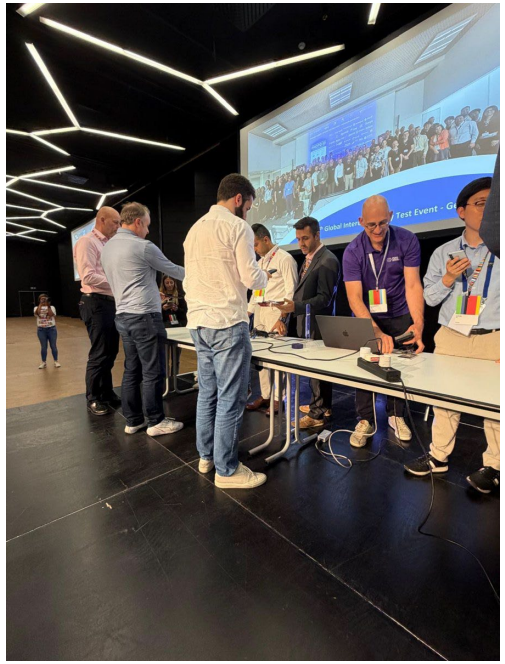
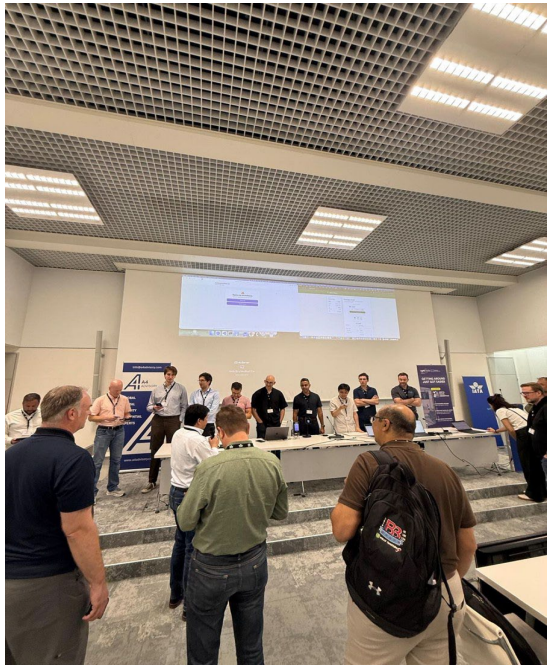
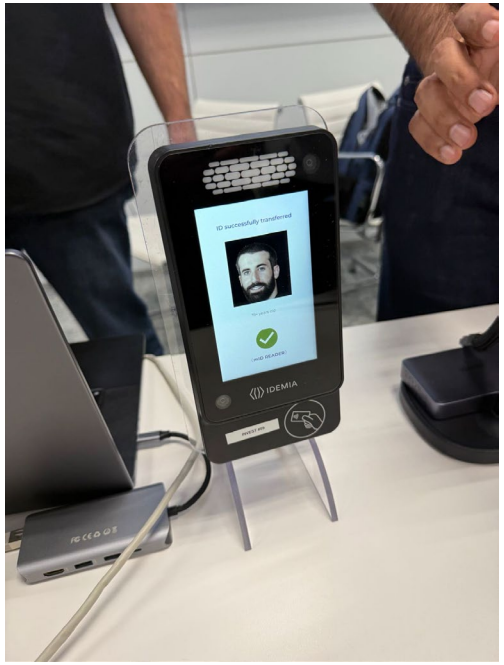
Uruguay
DNI digital, dic. 2026

+ Brasil, Colombia, Argentina, Ecuador y T&T en otros casos

IdLAC: doce países construyendo un marco federado de identidad transfronteriza, con el BID, el Banco Mundial, la Red GEALC, la OEA y Co-Develop.

Ginebra, Junio 2026: Test de interoperabilida Global



Pruebas cruzadas de interoperabilidad ISO en Ginebra: emisores, billeteras, lectores y gobiernos y empresas de todo el mundo.

Primera billetera de identidad de LAC en interoperar globalmente: Blerify.

05

El marco regulatorio habilitante

Cómo Europa y Estados Unidos están adaptando el KYC, y qué debería regular la región.

Dos modelos, una misma dirección

UNIÓN EUROPEA

Mandato

El Estado emite la billetera, la regulación obliga al sector privado regulado a aceptarla y la normativa antilavado la reconoce como vía de verificación.

eIDAS2 · AMLR

ESTADOS UNIDOS

Habilitación

Sin mandato federal: los estados emiten la licencia móvil, NIST fija las garantías y los reguladores confirman que el banco puede usarla para KYC si su programa lo permite.

NIST SP 800-63-4 · FinCEN CIP

EIDAS2 + AMLR

Europa: el calendario que obliga a la banca

20 may 2024

eIDAS2 en vigor

Reglamento (UE) 2024/1183

24 dic 2026

Billetera disponible

Cada Estado miembro ofrece al menos una billetera certificada

10 jul 2027

AMLR aplica

El art. 22(6) reconoce la identificación electrónica eIDAS de nivel sustancial o alto, incluida la billetera, para verificar clientes

24 dic 2027

Aceptación obligatoria

Art. 5f(2): bancos y servicios financieros deben aceptar la billetera si el usuario la elige

Excepción: micro y pequeñas empresas. La billetera es voluntaria para el ciudadano y nadie puede negarle el servicio por no usarla.

OBLIGACIONES EN DETALLE

Qué significa el artículo 5f(2) para un banco europeo

Aceptar, no imponer

El banco debe aceptar la billetera cuando el usuario la elige; puede seguir ofreciendo otros métodos.

Registrarse como verificador

Antes de integrarse, se registra en su Estado y declara qué datos pedirá y para qué.

Pedir solo lo registrado

No puede solicitar atributos fuera de lo declarado: la minimización se vuelve exigible.

La billetera no cierra todo el KYC

Verifica la identidad; la diligencia debida (beneficiario final, PEP, perfil de riesgo) sigue siendo del banco.

Encaje con PSD2

Aceptar la billetera para autenticar convive con los requisitos de autenticación reforzada de pagos.

Sin registro, sin acceso

La propia billetera comprueba que quien pide está autorizado antes de mostrar datos al titular.

NIST + FINCEN

Estados Unidos: el regulador confirma lo que la tecnología ya permite

JULIO 2025

NIST SP 800-63-4

La nueva versión de las guías de identidad digital admite evidencia digital, como la licencia móvil, entre las vías para alcanzar IAL2, e incorpora las billeteras controladas por el usuario.

8 SEP 2026

FinCEN + Fed, FDIC, OCC y NCUA

Una credencial digital verificable emitida por el gobierno, como la licencia móvil, cuenta como identificación oficial bajo la regla CIP, presencial o remota.

EN PARALELO

Estados y TSA

Más de 20 estados emiten licencia móvil y la TSA la acepta en controles de aeropuerto.

Los matices: no es obligatorio aceptarla, el banco debe tener sistemas para extraer y validar los datos, y cualquier señal de fraude en la credencial cuenta en su análisis.

PROPUESTA PARA LAC

Qué debería regular la región

Equivalencia legal

El documento digital verificable vale como el físico para KYC, presencial y remoto.

Como FinCEN

Niveles de garantía

Definir niveles de enrolamiento, autenticación y presentación, y mapearlos al riesgo de cada operación.

Como NIST y eIDAS

Registro de verificadores

Quién puede pedir qué atributos y para qué; la billetera lo comprueba antes de mostrar datos.

Como eIDAS art. 5b

Certificación

Requisitos para billeteras, dispositivos y proveedores: hardware seguro y atestaciones.

Como el ARF europeo

Responsabilidad clara

Si el banco verifica bien una credencial válida, queda protegido; el emisor responde por lo que firma.

Puerto seguro

Aceptación escalonada

Primero habilitar, luego obligar a quienes ya exigen autenticación fuerte.

Como eIDAS art. 5f

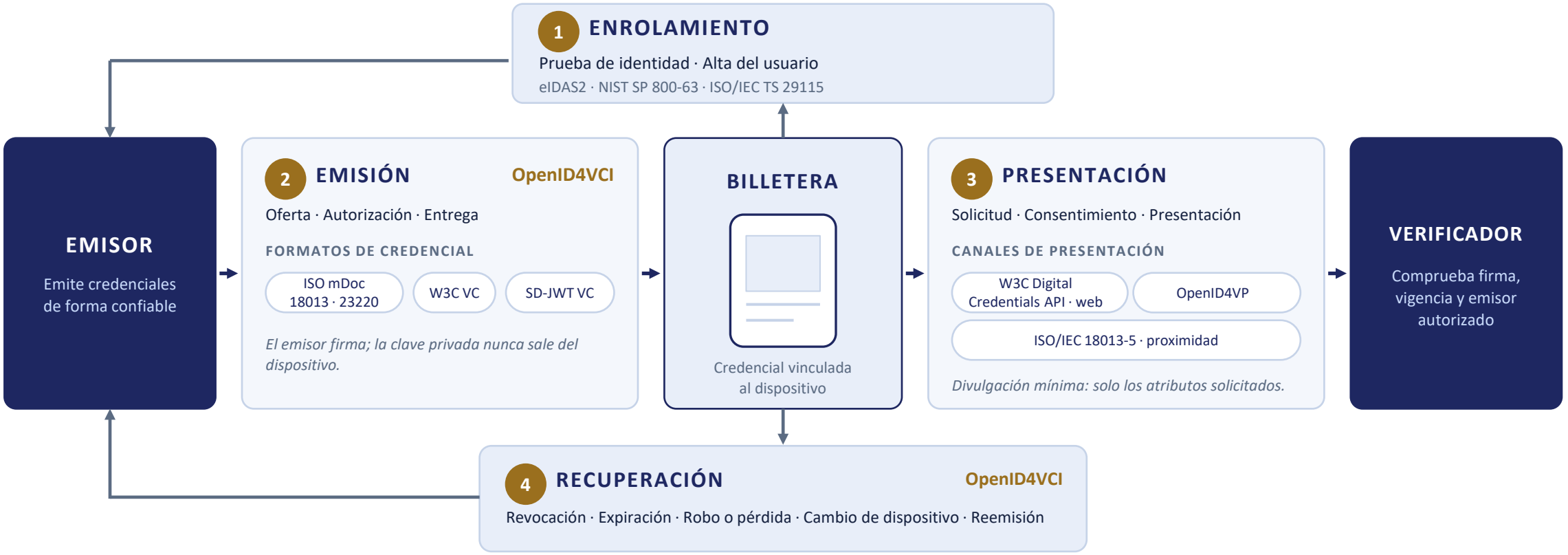
06

Estándares, comparativa con crypto wallet y desafíos

Tecnología con una década de estándares detrás, con nuevos desafíos a la vista.

EL FLUJO · ENROLAMIENTO, EMISIÓN, PRESENTACIÓN, RECUPERACIÓN

El ciclo de vida de un ID digital criptográfico



CONFIANZA TRANSVERSAL

Tres planos independientes, cada uno con su propia vía de revocación

1 · Autenticación

¿Quién es este participante?

- ISO/IEC 18013-5 · IACA y VICAL
- ETSI TS 119 612 y TS 119 602 · listas de confianza
- OpenID Federation 1.0 · W3C DID

2 · Autorización

¿Está autorizado a actuar?

- ETSI TS 119 475 · atributos del verificador
- ETSI TS 119 411-8 · certificados de acceso
- ARF EUDIW · registro nacional de verificadores

3 · Estado

¿La credencial sigue vigente?

- IETF Token Status List · en cola de publicación
- W3C Bitstring Status List
- RFC 5280 CRL y RFC 6960 OCSP · capa PKI

FORMATOS DE CREDENCIAL

¿Qué documentos se pueden emitir en formato de credencial?

Cada uno tiene un propósito diferente.

TRES FORMATOS

ISO mdoc

18013-5 y -7 · 23220

Documentos soberanos. Único con proximidad.

SD-JWT VC

IETF

Divulgación selectiva sobre JWT. Billetera europea.

W3C VC

JSON-LD

Modelo de datos general. Semántica extensible.



PERMISO DE CONDUCIR

Licencia móvil

ISO/IEC 18013-5 y -7

Primer perfil mdoc. Proximidad sin red y, desde la 18013-7, también remoto.

mdoc



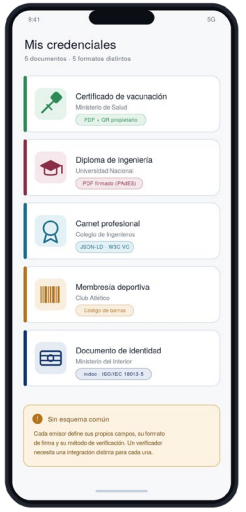
IDENTIDAD Y VIAJE

Photo ID y DTC

ISO/IEC 23220-4 · ICAO DTC

Cédula digital y pasaporte derivado. El namespace dtc lo conecta con la frontera.

mdoc



ATESTACIONES SECTORIALES

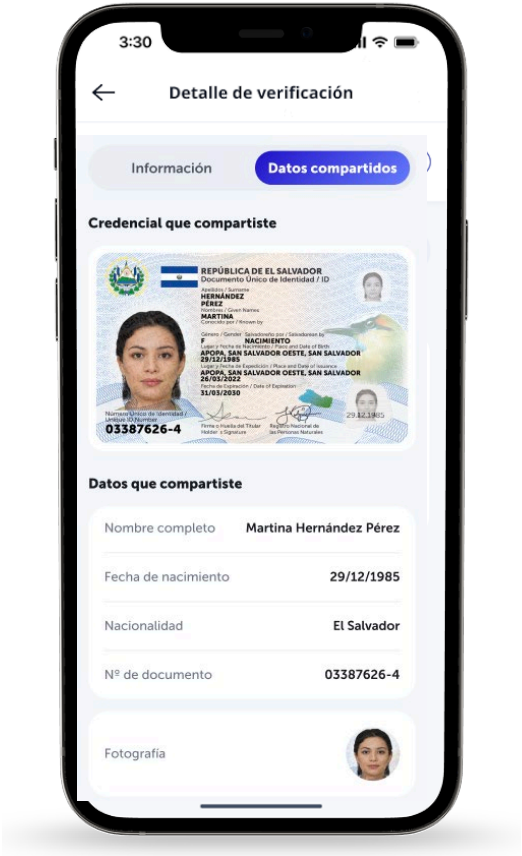
Otras credenciales

W3C VC · SD-JWT VC

Diplomas, colegiaturas y certificados de salud. Semántica extensible, sin proximidad.

JSON-LD · JWT

En la credencial verificable se incorpora certeza criptográfica



1

FIRMA DEL EMISOR

El registro civil firma el documento.

✓ **Documento válido · emisor confiable · no revocado**

2

FIRMA DEL TITULAR

El ciudadano firma desde su teléfono, con una clave que nunca sale del dispositivo.

✓ **Quien lo presenta es su titular**

3

CONSENTIMIENTO

El ciudadano aprueba qué atributos comparte y con quién.

✓ **Divulgación mínima y registro de cada uso**

¿Cómo verificamos una credencial verificable?

El canal no lo elige el emisor ni el verificador: lo impone el escenario. Solo uno funciona sin red.

	1 **Proximidad** ISO/IEC 18013-5	2 **OpenID4VP directo** ISO/IEC 18013-7 · OpenID4VP 1.0	3 **OpenID4VP sobre DC API** W3C Digital Credentials API
Tipo	**Presencial**	**Remoto · app a app o web**	**Remoto · navegador**
Casos de uso	Identificación ante tránsito, apertura cuenta sucursal, embarque, retirada de paquetería, acceso a locales, control de edad en mostrador	Alta bancaria y KYC remoto, firma electrónica, trámites en la app del Estado	Verificación de edad en checkout, alta en plataformas y, de forma emergente, comercio agéntico

2 y 3 no compiten: la DC API es la capa del navegador sobre la que corre OpenID4VP. El corte real está entre el canal 1 y los otros dos: solo la proximidad funciona sin red en ambos extremos.

Misma tecnología que una billetera cripto, lógica radicalmente distinta

	BILLETERA CRIPTO	BILLETERA DE IDENTIDAD
Qué custodia	Activos financieros	Atributos certificados por un emisor
A qué se vincula la llave	Identidad anónima o pseudónima	Documento emitido por una autoridad
Si pierdes la llave	Pérdida total e irreversible	El emisor revoca y re-emite
Dónde reside la confianza	En la llave y la red	En la llave, el emisor y un registro de confianza

Perder el teléfono no es perder la identidad: es pedir que te re-emitan el documento.

DE DÓNDE VIENE ESTO

El concepto nació como Self-Sovereign Identity; sobrevivieron los estándares y los conceptos de confianza criptográfica

SELF-SOVEREIGN IDENTITY

Concepto

- Billetera
- Llaves criptográficas
- Credenciales verificables
- Atributos auto-atestados

DESAFÍO

¿Quién confía en esas credenciales?



“Self-Sovereign Identity: The Future of Identity” — publicación BID, M. Allende.

Revisión conceptual del paradigma,

https://publications.iadb.org/en/self-sovereign-identity-future-identity-self-sovereignity-digital-wallets-and-blockchain

Confidencial · © 2026 Blerify

DE DÓNDE VIENE ESTO

El concepto nació como Self-Sovereign Identity; sobrevivieron los estándares y los conceptos de confianza criptográfica

SELF-SOVEREIGN IDENTITY

Concepto

Billetera

Llaves criptográficas

Credenciales verificables

Atributos auto-atestados

DESAFÍO

¿Quién confía en esas credenciales?

BILLETERAS DE IDENTIDAD CON ID DE GOBIERNO

Concepto

Billetera

Llaves criptográficas

Credenciales verificables

Emisión ente regulado

DESAFÍO

¿Escala e interoperabilidad cross-país?



“Self-Sovereign Identity: The Future of Identity” — publicación BID, M. Allende.

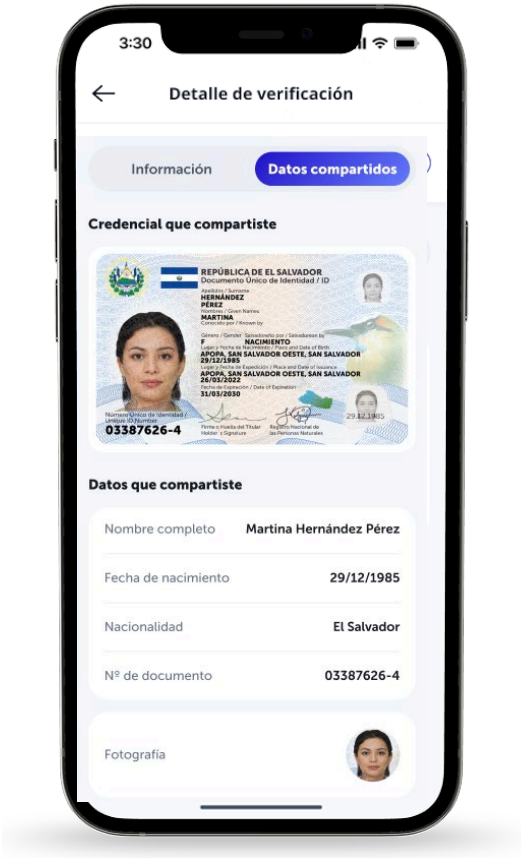
Revisión conceptual del paradigma,

https://publications.iadb.org/en/self-sovereign-identity-future-identity-self-sovereignity-digital-wallets-and-blockchain

Confidencial · © 2026 Blerify

EL DISPOSITIVO IMPORTA

No todos los teléfonos dan la misma garantía



Hardware seguro	Secure Enclave o StrongBox: la llave nace en el chip y no se puede extraer ni copiar.	*Sin chip seguro, la llave vive en software: menor garantía.*
Bloqueo de pantalla	Sin PIN o biometría configurados, cualquiera con el teléfono podría usar la credencial.	*La billetera exige bloqueo para operar.*
Sistema no alterado	Un teléfono con root o jailbreak rompe el aislamiento de la app.	*Se detecta y se refleja en la evidencia.*
Biometría local	La huella o el rostro desbloquean la llave en el propio teléfono; la plantilla nunca sale.	*Nadie custodia biometría central.*

ATESTACIONES

Cómo sabemos que la llave, la app y el teléfono son genuinos

1

Atestación de la llave

El fabricante del chip certifica que la llave se generó dentro del hardware seguro y no puede salir de él.

¿La llave es real y no copiable?

2

Atestación de la app

La plataforma (Google o Apple) certifica que la app es la original de la tienda oficial, no una versión modificada.

¿Es la app legítima?

3

Atestación del dispositivo

El sistema operativo certifica que el teléfono no está comprometido ni emulado.

¿El entorno es confiable?

Las tres atestaciones viajan firmadas dentro de la presentación: el banco las verifica, no las supone.

CICLO DE VIDA

Bloqueo, pérdida y recuperación: la identidad no se pierde con el teléfono

Teléfono bloqueado

La credencial es inútil sin la biometría o el PIN del titular. Robar el aparato no es robar la identidad.

Pérdida o robo

El titular lo reporta y el emisor revoca la credencial. Cualquier verificador lo ve al instante en la lista de estado.

Recuperación

Nuevo enrolamiento con el nivel de garantía exigido y reemisión al nuevo dispositivo. Las llaves nunca se copian.

Coerción

Señales de uso forzado y mecanismos para que el titular pueda bloquear o invalidar una presentación.

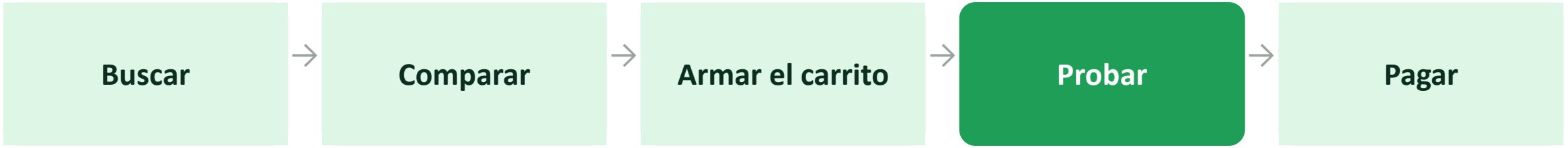
07

Agentes IA, el siguiente paso

Las billeteras y las credenciales son el instrument ideal para la delegación verificable.

EL PUNTO DE PARTIDA

El agente ya puede pagar. ¿Puede probar que tiene permiso?



El agente lo hace solo

Demostrar autorización

¿Es mayor de edad?

Para un producto restringido, sin revelar la fecha de nacimiento.

¿Es cliente de verdad?

Un beneficio o descuento ligado a una relación real.

¿Lo autorizó la persona?

Un pago que el titular aprobó, desde su propio dispositivo.

Las credenciales criptográficas permiten completar procesos de autenticación y autorización de agentes. La llave ya está en el bolsillo del titular: en su billetera de identidad.

LA BRECHA

Saber quién inició sesión ya está resuelto. Probar una autorización expresa para una acción, no

LO QUE YA EXISTE

Sesión autenticada: el agente entró con una cuenta válida.

Mandato de compra: alguien aprobó este carrito.

Un token al portador se puede robar y reutilizar.

LO QUE FALTA

Un atributo firmado por un emisor sobre la persona real.

Vinculado a una llave que no puede salir del dispositivo.

Una llave en el elemento seguro, no.

Por eso la billetera de identidad es clave para el comercio con agentes.

DEMO

Tres escenarios, de menor a mayor complejidad jurídica

Resuelto hoy

Titular presente

La persona está ahí, presenta su credencial y la acción se completa. Es el caso base.

Resuelto hoy

Titular presente al pagar

El agente trabaja por adelantado y la persona aparece solo en el momento decisivo: aprobar.

Donde están las preguntas difíciles

Titular ausente

Un mandato preautorizado: el agente actúa solo dentro de los límites que fijó la persona.

Para el derecho financiero: ¿quién responde si el agente se excede? ¿Qué vale como prueba del consentimiento? ¿Cómo se revoca un mandato a tiempo?

MANDATOS VERIFICABLES

El consentimiento como cadena de firmas

1 · Intención

FIRMA EL TITULAR

"Zapatillas hasta USD 200, antes del viernes, solo en estas tiendas"

Límite, plazo, comercios y qué credenciales puede usar

2 · Carrito

FIRMA EL COMERCIO

"Este producto, USD 178, precio final"

Líneas exactas y total sellado: no hay deriva ni ambigüedad

3 · Pago

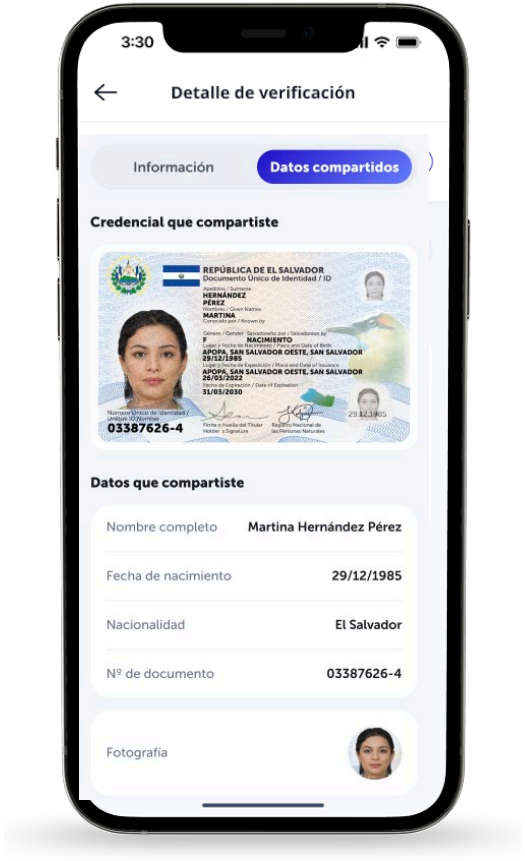
FIRMA EL AGENTE CON LA CREDENCIAL DE PAGO

"Cargar USD 178, una vez"

Un monto, una orden, una vez: dentro de la intención

Las tres firmas deben coincidir antes de liquidar. Si hay disputa, la cadena es la prueba.

La misma billetera, una credencial de pago (DIGITAL PAYMENT CREDENTIAL)



Qué	Categorías o comercios autorizados
Cuánto	Presupuesto total y máximo por compra
Hasta cuándo	Plazo de vigencia del mandato
Revocable	El titular lo cancela en cualquier momento desde su billetera

Los límites se aplican del lado del servidor; la pantalla solo los muestra.

Credencial de pago en la billetera (DPC)

Junto al documento de identidad, el banco emite una credencial de pago. La autorización del pago se firma con la misma llave del dispositivo: autenticación fuerte, sin contraseñas ni códigos por SMS.

Identidad y pago sobre la misma infraestructura de confianza.

EL MAPA DE ESTÁNDARES

Pagos agénticos: cada capa tiene ya su estándar en construcción

Comunicación entre agentes	Identidad y confianza del agente	Descubrimiento y checkout	Autorización y autenticación del pago
Model Context Protocol Anthropic	**Trusted Agent Protocol** Visa	**Agentic Commerce Protocol** OpenAI	**Visa Intelligent Commerce** Visa
Agent to Agent Google	**ERC-8004** Código abierto	**Universal Commerce Protocol** Google	**Agent Payments Protocol (AP2)** Google
		x402 Coinbase	**Agent Pay** Mastercard

CONSOLIDACIÓN EN FIDO ALLIANCE

Abr 2026
Google y Mastercard donan AP2 y Verifiable Intent

Sep 2026
Especificaciones en repositorio público para revisión

Fin 2026
Armonización de AP2 y Verifiable Intent

Mitad 2027
Primera versión consolidada

Anatomía de una credencial de pago digital (DPC)

Lo que el banco emisor entrega a la billetera del titular. Misma lógica que el documento de identidad: firmada por el emisor y atada a una llave del dispositivo.

Metadatos de la credencial

Identifican emisor, credencial y titular. No visibles para el usuario.

Tipo de credencial	Obligatorio
Emisor	Obligatorio
Llave de vínculo del titular	Obligatorio
Fecha de emisión	
Fecha de expiración	

Atributos divulgables

Lo que se puede revelar al verificador, según lo que pida.

ID de credencial	Obligatorio
Red de pago	Obligatorio
ID de tarjeta	

Metadatos de visualización

Construyen la tarjeta que el usuario ve en su billetera.

- Arte y nombre de la tarjeta
- Últimos cuatro dígitos
- Red y cobranding
- Banco emisor y contacto de soporte

Fuera del esquema: la firma del titular, el contexto del protocolo y las protecciones anti-repetición se añaden en cada presentación, según el protocolo usado.

LA PRESENTACIÓN

El usuario revisa y firma la autorización de pago

1 · QUÉ CREDENCIAL SE PIDE

- Por ID de credencial
- Por ID de tarjeta
- Descubrimiento de credenciales
- Por red de pago

2 · EL CONTEXTO DEL PAGO

- Referencia del pago
- Monto y moneda (o estimado)
- Resumen de la compra
- Beneficiario: nombre, web y logo
- Tipo de pago
- Recurrencia: intervalo, fechas, cuotas

3 · EL TITULAR VE Y FIRMA

La billetera, o el navegador vía DC API, muestra las credenciales que coinciden y el detalle exacto de la transacción.

La firma del titular queda atada a ese pago concreto: no se puede reutilizar para otro monto ni otro comercio.

Convergencia: EMVCo trabaja con FIDO Alliance para estandarizar el contexto del pago, y eIDAS (TS12) define los elementos de pago para la billetera europea.

08

La dimensión cuántica

Una prueba firmada hoy tiene que seguir valiendo en 2045.

Todo esto es criptografía. Y la criptografía está bajo amenaza

1

Todo el sistema es criptográfico

Llaves en la billetera, firma del emisor, firma del titular, mandatos de pago, registros de confianza.

2

Shor rompe la criptografía actual

Cuando un computador cuántico corra el algoritmo de Shor a escala, RSA y curvas elípticas dejan de ser seguros.

3

"Harvest now, decrypt later"

Lo que se captura hoy puede descifrarse o falsificarse mañana. Los registros de décadas no se migran fácil.

Allende et al., "Quantum-resistance in blockchain networks", Nature Scientific Reports, 2023 · DOI 10.1038/s41598-023-32701-6

VALIDEZ EN EL TIEMPO

Por qué es un problema jurídico: las pruebas tienen que durar más que la criptografía

Documento de identidad	~10 años de vigencia
Consentimiento y mandatos	Prueba en disputas durante años
Contrato de crédito o hipoteca	15 a 30 años
Registro de confianza	Historial auditable de décadas

HORIZONTE REGULATORIO

NIST propone retirar RSA y curvas elípticas hacia 2030 y prohibirlas hacia 2035.

Un DUI digital emitido en 2026 seguirá vigente cuando su firma ya no sea confiable si no se diseña para migrar.

Lo que se firma hoy debe poder verificarse, y defenderse en juicio durante años.

Qué pedir desde hoy a los proyectos de identidad digital

1

Agilidad criptográfica en el diseño

Cada desarrollo debería poder migrar algoritmos sin re-emitir todo.

2

Inventario criptográfico

Saber qué sistemas, documentos y registros dependen de RSA o curvas elípticas.

3

Firmas híbridas para no reemplazar si no reforzar

Documentos, contratos y evidencias de larga vida, firmados ya con doble firma.

PUBLICADO EN NATURE · SCIENTIFIC REPORTS

Resistencia cuántica sin reconstruir la red



scientific reports

Explore content · About the journal · Publish with us

nature › scientific reports › articles › article

Article | Open access | Published: 06 April 2023

Quantum-resistance in blockchain networks

Marcos Allende, Diego López León, Sergio Cerón, Adrián Pareja, Erick Pacheco, Antonio Leal, Marcelo

76k accesos

108 citas

2023 publicación

Acceso abierto · métricas de la revista a la fecha

TRES CAPAS DE PROTECCIÓN, ENFOQUE HÍBRIDO

1 Canales post-cuánticos

Túneles cifrados entre nodos con certificados post-cuánticos.

2 Doble firma

Se respeta la firma nativa y se añade una segunda firma post-cuántica encima.

3 Consenso post-cuántico

Los nodos firman los bloques con llaves post-cuánticas.

Implementado sobre la red blockchain LACChain: la solución se probó en una red real, no solo en teoría.

Allende, M., López León, D., Cerón, S., et al. **"Quantum-resistance in blockchain networks."** *Scientific Reports* 13, 5664 (2023). DOI: 10.1038/s41598-023-32701-6

PUBLICADO EN NATURE · SCIENTIFIC REPORTS

Resistencia cuántica sin reconstruir la red


scientific reports

Explore content · About the journal · Publish with us

nature › scientific reports › articles › article

Article | Open access | Published: 06 April 2023

Quantum-resistance in blockchain networks

Marcos Allende, Diego López León, Sergio Cerón, Adrián Pareja, Erick Pacheco, Antonio Leal, Marcelo

76k accesos

108 citas

2023 publicación

Acceso abierto · métricas de la revista a la fecha

Escanea para leer el paper

Implementado sobre la red blockchain LACChain: la solución se probó en una red real, no solo en teoría.

Allende, M., López León, D., Cerón, S., et al. **"Quantum-resistance in blockchain networks."** *Scientific Reports* 13, 5664 (2023). DOI: 10.1038/s41598-023-32701-6

CIERRE

Seis reflexiones para llevarse

1

La IA rompió el KYC, no la identidad

Lo que falla es verificar con fotos; la solución es verificar con criptografía.

2

Más certeza no exige más datos si no verificabilidad

La solución es que cada dato sea verificable criptográficamente.

3

El documento digital ya es una realidad

Hay estándares, países en producción y una billetera en El Salvador.

4

El primer paso no necesita una ley

Europa obliga y Estados Unidos habilita: basta con que el supervisor reconozca el documento digital para el KYC.

5

El consentimiento es infra y sirve para agentes

Si no es firmado, revocable y verificable, no es soberano. Con los agentes de IA se vuelve imprescindible.

6

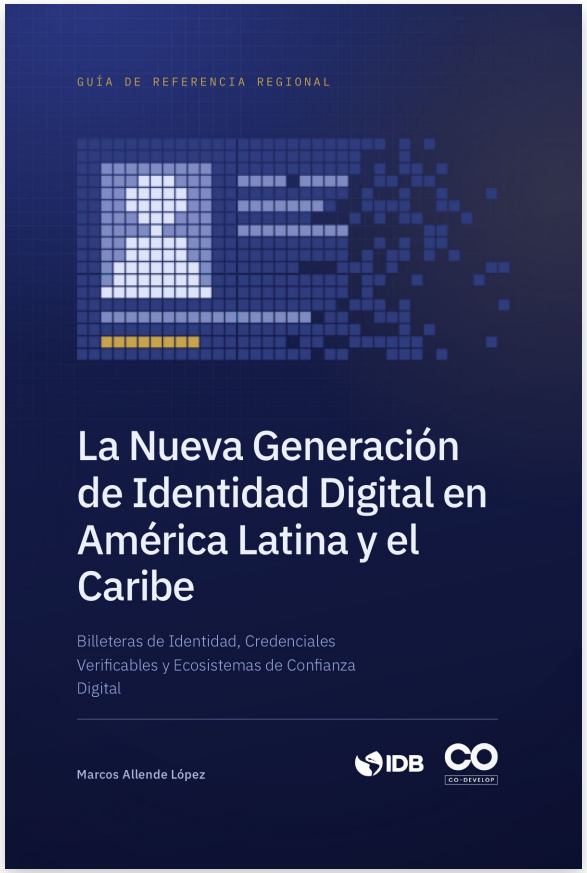
Lo que se firma hoy debe valer en 2045

La agilidad criptográfica se exige desde el diseño, no se añade después. Debemos buscar resistencia cuántica.

GUÍA DE REFERNCIA

El libro regional

Elaborado con revisión de pares de la región y del ecosistema internacional de identidad digital.



PUBLICACIÓN Y DISTRIBUCIÓN

Disponible próximamente en los canales públicos del BID y de Co-Develop

BID | CoDevelop

Panel de revisión de pares

Manuel Aguilera
CDPI

Ignacio Alamillo
Astrea · CEN/CLC/JTC19, ETSI ESI

Ysaias Álvarez
CDPI

Javier Barreiro
IdLAC, Red GEALC

Juan Echevarría
IUGO Tech Studio

Juan Pablo García
AGESIC

José Luis Hernández Carrión
BID

Lucas Jolías
Sovra

Luis Papagni
Consultor DPI y ciberseguridad

Drummond Reed
First Person Coop. · ToIP

Julia Vieira
BID

Andrew Piscione
COO Blerify

La revisión de pares no implica respaldo institucional de las organizaciones mencionadas.

Material elaborado por Blerify. Contenido derivado de obra del BID bajo licencia CC. No distribuir sin consentimiento



GRACIAS · CONECTEMOS

Marcos Allende López

Co-Founder & CEO · Blerify

LINKEDIN /marcosallendel

Sigue lo que viene

El ecosistema sigue creciendo. Entérate primero.

INSTAGRAM	LINKEDIN	X	WEB · BLOG
@blerifyid	/blerify	@blerify_id	blerify.com

COLADE 2026 · CONFERENCIA MAGISTRAL

La Identidad Soberana ante la Frontera de los Neurodatos y la IA

Redefiniendo la propiedad del "yo" en la banca

Marcos Allende López
CEO y Cofundador, Blerify

San Salvador · 15 de octubre de 2026