

De la fragmentación
a interoperabilidad soberana

El futuro digital de Europa: una identidad única y segura

Mayo 2026

 gradiant





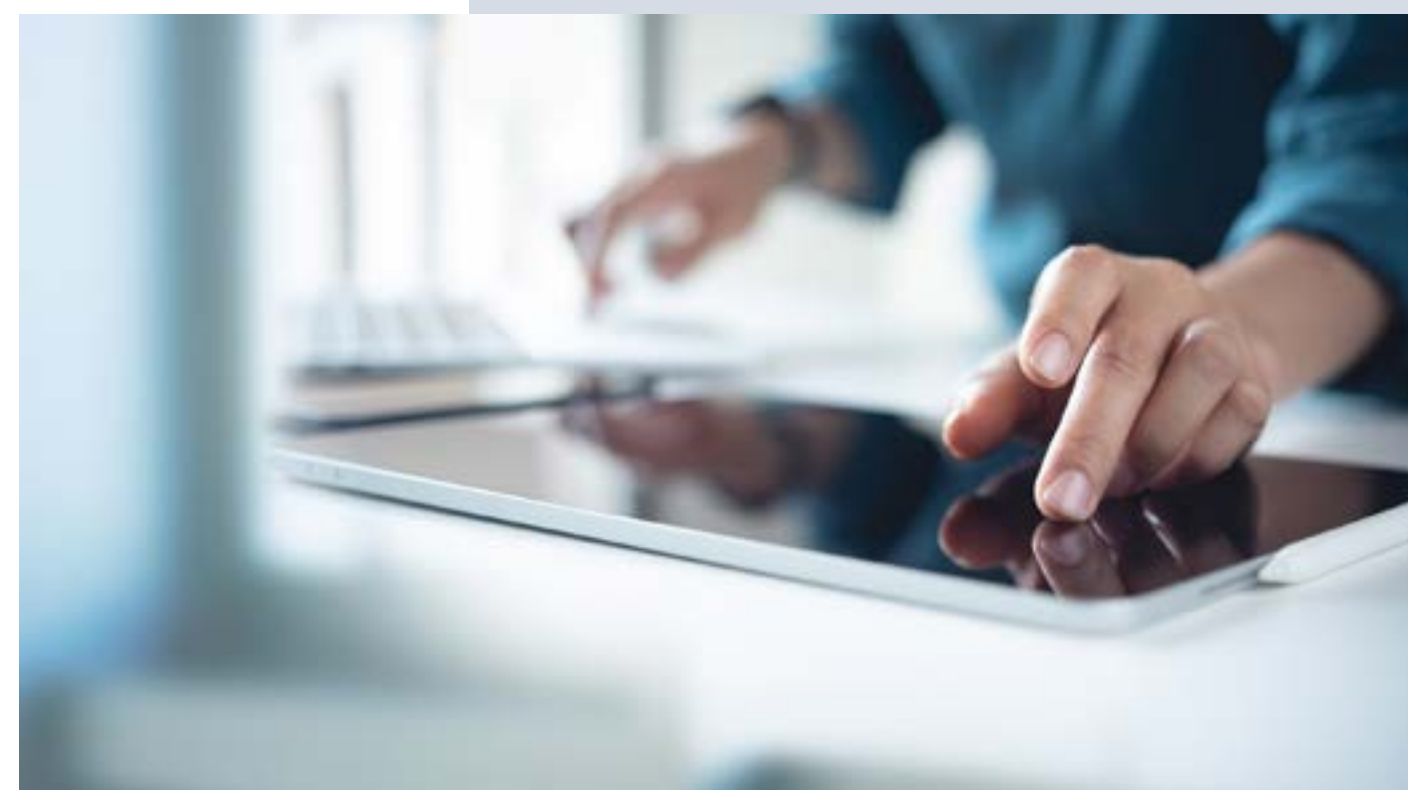
1.

De un mosaico de identidades digitales a una solución europea única y segura

El pasado año, siete de cada diez europeos de entre 16 y 74 años recurrieron a una web o aplicación de una autoridad pública. La mayoría lo hizo para consultar información sobre:

- Servicios, prestaciones, leyes o horarios de atención **(44%)**
- Acceso a datos personales **(40%)**
- Descarga o impresión de formularios **(38,1%)**.

En el extremo opuesto, apenas un 5,3% presentó por esta vía solicitudes, reclamaciones o quejas.



86%

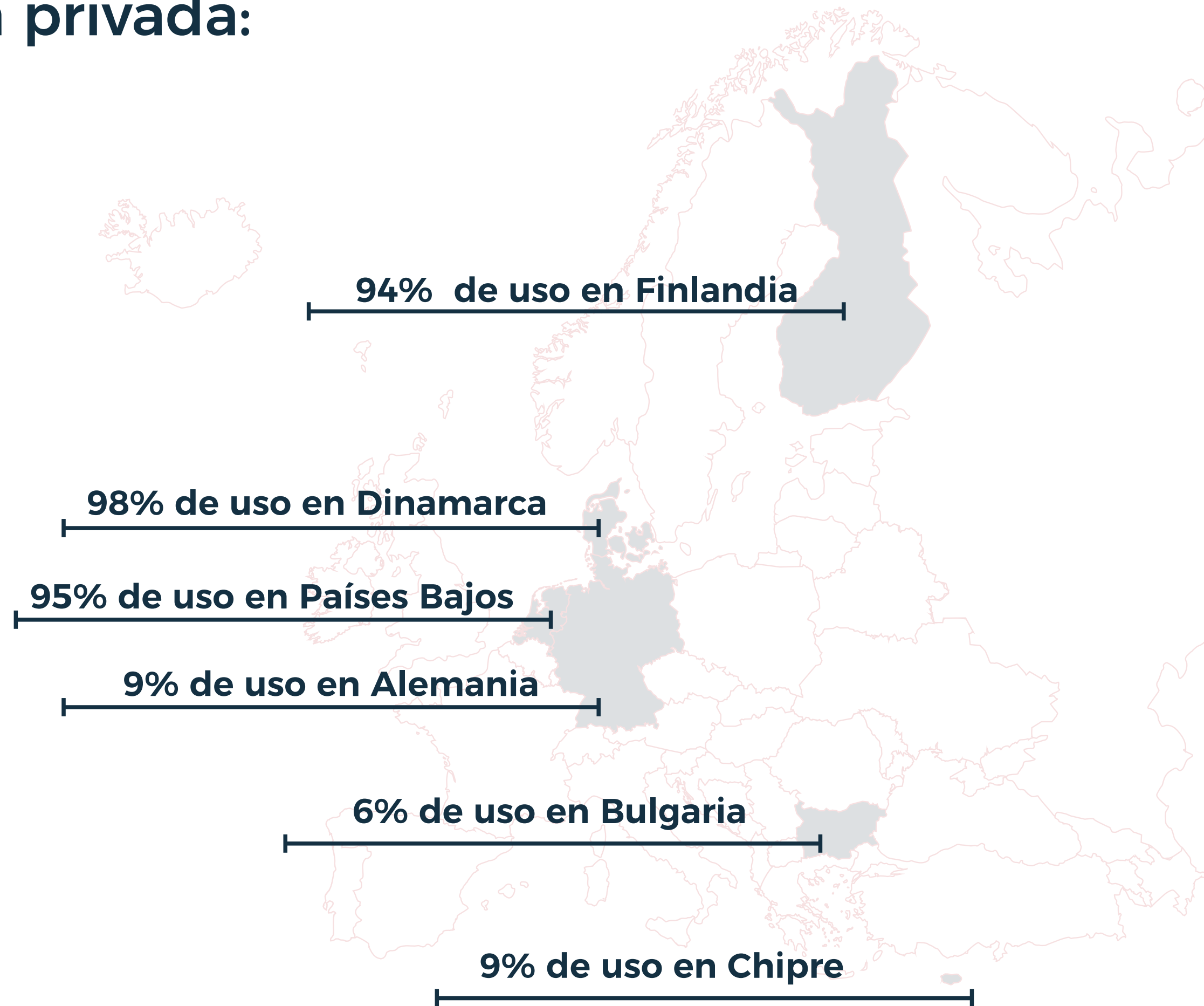
Servicios gubernamentales en la Unión Europea ya están disponibles en línea, según el informe eGovernment Benchmark 2024 elaborado por Capgemini.



41%

Personas de entre 16 y 74 años en la UE declaró haber utilizado su eID para acceder a servicios en línea con fines privados. Según datos de Eurostat en 2023.

Desigualdad entre países en su aplicación en la esfera privada:



El auge de los servicios digitales trae consigo nuevos desafíos:

Robo de identidad

Filtración de datos

Fraude

Por eso, asegurar la protección de los trámites electrónicos es clave:

No sólo para resguardar al ciudadano, sino también para mantener la confianza en la administración pública.



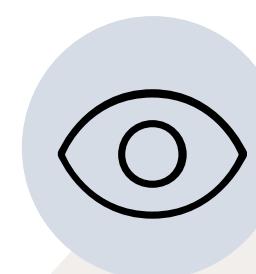


Con ese objetivo, la **Unión Europea** avanza hacia una **identidad digital personal y segura**, válida en todos los Estados miembros.



electronic IDentification Authentication and trust Services

Hasta el momento, la identificación electrónica en Europa estaba marcada por la fragmentación: cada país contaba con su propio sistema nacional, difícilmente interoperable y con un alcance transfronterizo muy limitado. Esta realidad, regulada por el reglamento eIDAS de 2014 dejaba a los ciudadanos europeos con experiencias dispares, poca confianza en la seguridad de sus datos y escasas garantías de uso más allá de sus fronteras.



El **eIDAS** sentó las bases del marco legal para la identificación digital en la UE y reguló servicios de confianza como la firma o el sello electrónico. Sin embargo, su aplicación práctica resultó insuficiente.



14 Estados miembros

notificaron formalmente un sistema de identidad digital y su aceptación fuera de las fronteras nacionales fue mínima.

Resultado

Transacciones electrónicas poco homogéneas, fricciones en la verificación de identidad -a menudo dependiente de procesos manuales o intermediarios privados- y dudas crecientes sobre privacidad.



Sector privado

Integrar eID y servicios de confianza permite sustituir trámites presenciales por operaciones digitales seguras (**apertura de cuentas, firma de contratos, onboarding de clientes**) y un importante ahorro de tiempo y recursos, ya que reduce la carga administrativa y el coste de verificación manual de identidad.



MAYO 2024

- Nuevo reglamento europeo (**UE 2024/1183**)
- Marcha de la Cartera Europea de Identidad Digital (**EUDI Wallet**)

MARCA UN PUNTO DE INFLEXIÓN, TRATANDO DE REVOLUCIONAR LA FORMA EN LA QUE CIUDADANOS Y EMPRESAS SE IDENTIFICAN EN LA RED.

Vocación de ser una herramienta:

- ✓ Segura
- ✓ Portátil
- ✓ Válida

Pretende :

- 1.- Reducir costes
- 2.- Fricciones
- 3.- Riesgos en el acceso tanto a servicios públicos como privados.



Objetivo

Mosaico de soluciones nacionales



Identidad digital europea única

Marcará un antes y un después en la relación entre ciudadanos, empresas y administraciones.

Deadline

28 de noviembre de 2024: Se adoptan los actos de ejecución.

Fecha límite resultante: Diciembre de 2026.

Inicio del plazo: Desde esa fecha comienza a contar el plazo máximo.

Obligación de los Estados miembros: Ofrecer gratuitamente al menos una cartera.

Duración del plazo: 24 meses.

El reto va más allá de una simple actualización normativa y la consecución del objetivo dependerá de la coordinación entre los gobiernos, el sector privado y el ecosistema tecnológico. (Retos y soluciones tecnológicas)

En este informe se analizan los aspectos clave de la estrategia de despliegue de la **EUDI Wallet**:



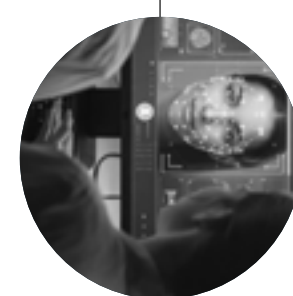
Actos de implementación



La certificación de la cartera

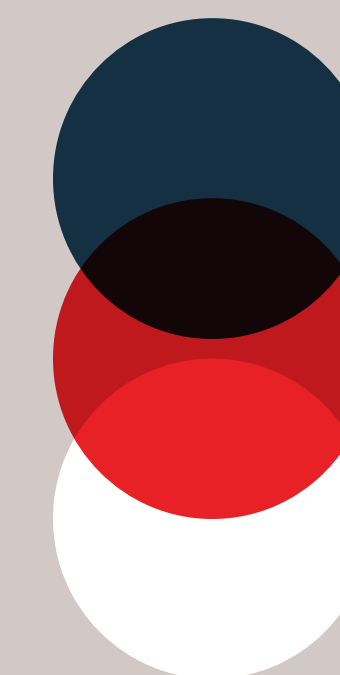


Proyectos piloto a gran escala (Large Scale Pilots, LSP)



Retos y soluciones tecnológicas

Triple perspectiva



Soluciones tecnológicas

Política

Necesidad del mercado

2.

eIDAS 2: los pilares del nuevo paradigma

El **eIDAS 2.0** es una actualización del reglamento europeo sobre identificación electrónica y servicios de confianza que entró en vigor en mayo de 2024, introduciendo la **Cartera Europea de Identidad Digital (EUDI Wallet)**, una identidad digital unificada y soberana que marcará un antes y un después en la relación entre ciudadanos, empresas y administraciones.

Este reglamento supone un cambio de paradigma cuyas claves son:

1

Cartera Europea de Identidad Digital (EUDI Wallet)

Cada Estado miembro tendrá la obligación de poner a disposición, de forma gratuita y antes de que acabe el próximo año, al menos una cartera digital que podrá ser utilizada por ciudadanos, residentes y también por empresas. Esta herramienta será válida y reconocida en toda la Unión Europea, gracias a un marco de interoperabilidad técnica y legal que garantiza su uso sin barreras fronterizas. Además, la Comisión Europea ha dejado abierta la posibilidad de que proveedores privados puedan ofrecer también su propia EUDI Wallet.

2

Interoperabilidad y seguridad

La cartera debe ser interoperable entre los sistemas nacionales y cumplir con altos estándares de seguridad, incluyendo una certificación de ciberseguridad por parte de la Agencia de la Unión Europea para la Ciberseguridad (ENISA).

3

Control total del usuario sobre sus datos

Los usuarios pueden decidir qué información compartir y con quién, aplicando el principio de minimización de datos.

4

Acceso a servicios públicos y privados

A partir de finales de 2027, todos aquellos prestadores de servicio que requieren una autenticación fuerte como la banca, las telecomunicaciones, la sanidad, la educación, el transporte, la energía o el comercio electrónico deberán aceptar obligatoriamente la EUDI Wallet como medio válido de identificación y autenticación.

5

Servicios de confianza integrados

La cartera incluirá servicios como firma electrónica, sellos electrónicos, y declaraciones electrónicas de atributos.

6

Protección de datos y privacidad

Se implementarán tecnologías, como la divulgación selectiva para minimizar la información intercambiada, garantizando la protección de datos conforme al Reglamento (UE) 2016/679 (GDPR).

EUDI Wallet

01

Portabilidad total
Una única identidad
válida en toda la UE.

02

Privacidad reforzada
Control granular sobre la
información compartida.

03

Seguridad certificada
Cumplimiento
del estándar de
ciberseguridad más alto.

04

Interoperabilidad real
Aceptación obligatoria
en toda la Unión.

Oportunidades inmediatas

La Cartera Europea de Identidad Digital permitirá a cada ciudadano europeo acceder, identificarse y actuar online con seguridad, comodidad y control, consolidando una Europa digital más inclusiva, interoperable y centrada en la persona.

Además, las entidades emisoras de atributos, como universidades, colegios profesionales o administraciones podrán emitir credenciales verificables compatibles desde el inicio.

Por su parte, los Prestadores de Servicios de Confianza deberán adaptar sus procesos de validación, preservación y firma a los nuevos requisitos legales y técnicos.

Arquitectura de referencia: Architecture and Reference Framework (ARF)

El ARF (Architecture and Reference Framework) es la guía común que la Unión Europea ha creado para desarrollar la Cartera Digital Europea. Establece las reglas y estándares que garantizan que las distintas carteras digitales sean seguras, compatibles y válidas en todos los países de la UE.

Gracias a este marco, los ciudadanos podrán identificarse y realizar trámites digitales en cualquier Estado miembro de forma sencilla y segura.

El ARF se actualiza periódicamente para incorporar nuevas tecnologías y mejoras en interoperabilidad.

3.

Hoja de ruta: claves para una adopción plena

Son cinco los elementos que marcarán en los próximos años la hoja de ruta para la adopción plena de la nueva normativa y cada uno de ellos tiene a su vez reflejo en el ámbito político, de mercado y en el plano tecnológico:



1.

Los actos de implementación que definirán en detalle cómo se desplegará la normativa.



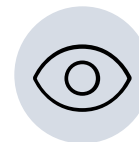
2.

La certificación de la cartera, esencial para garantizar seguridad y confianza.



3.

Los proyectos piloto a gran escala (LSP), que pondrán a prueba la EUDI Wallet en entornos reales antes de su implantación generalizada.



4.

La arquitectura basada en principios clave que aseguran su eficacia y confiabilidad, como la interoperabilidad, la seguridad y privacidad o el control del usuario.



5.

La implementación de referencia, una solución técnica desarrollada por la Comisión Europea, basada en el Architecture and Reference Framework (ARF), que sirve como modelo estándar para el desarrollo de carteras digitales interoperables, seguras y conformes con la normativa europea.



Actos de implementación: del texto legal a la realidad operativa

2024

20 de mayo: Entrada en vigor del Reglamento

Diciembre: Primer paquete de actos de implementación: requisitos técnicos de la cartera digital, ecosistema, interfaces y certificación.

2026

24 de diciembre: Cada Estado miembro debe ofrecer al menos una cartera digital gratuita a ciudadanos, residentes y empresas.

2025

Mayo: Segundo paquete de actos de implementación: gestión de brechas de seguridad, registro y obligaciones de e-lying parties, lista de carteras certificadas e ID matching.

Julio: Tercer paquete de actos de implementación: acreditaciones electrónicas de atributos, reglas de supervisión y reporting, revisión de esquemas de eID.

Finales de 2025: Acto de ejecución del marco de interoperabilidad para la identificación transfronteriza (fecha concreta TBD).

2027

Diciembre 2027: Entrada en vigor de la obligación para determinadas organizaciones públicas y privadas de aceptar la wallet como medio de identificación cuando se requiera autenticación fuerte.

Uno de los aspectos clave de este reglamento es la creación e implementación de normas y procedimientos detallados a través de una serie de actos de implementación gradual.

Estos actos buscan establecer normas claras y procedimientos que garanticen la seguridad e interoperabilidad de la Cartera de Identidad Digital Europea y los esquemas de certificación de ciberseguridad. Definen los procesos de certificación para asegurar que las carteras y otros servicios relacionados cumplan con los estándares europeos, promoviendo la confianza entre los Estados miembros.

Además, aseguran el cumplimiento operativo de servicios de confianza, como la atestación electrónica de atributos (acreditación de la identidad de una persona en el ámbito digital) y el libro mayor electrónico (registros de transacciones que aseguran una trazabilidad verificable y segura), mejorando la fiabilidad de las transacciones digitales en la UE.



Los actos de implementación desde una perspectiva triaxial

La aprobación de los actos de implementación exige avanzar de manera coordinada en tres planos:

Plano político y de gobernanza

La clave está en armonizar los criterios sin perder soberanía: los Estados miembros deben construir un marco común que evite dialectos nacionales y, al mismo tiempo, garantice una supervisión eficaz, con indicadores compartidos y un circuito claro de sanciones y medidas correctivas.

Plano del mercado

El mercado, por su parte, afronta el reto de incorporar la EUDI Wallet como estándar competitivo. Las entidades financieras, el comercio electrónico o la sanidad deben planificar un calendario de adaptación que les permita integrarse con antelación, capitalizando la ventaja de un onboarding sin fricción y de una reducción del fraude.

Plano de tecnología

Desde la vertiente tecnológica, el éxito pasa por consolidar especificaciones de API (Interfaz de Programación de Aplicaciones), formatos de acreditaciones y mecanismos de verificación criptográfica que aseguren resiliencia, latencias mínimas y una operativa transfronteriza robusta.



Adelantarse a los plazos de los actos de implementación puede ser una ventaja competitiva para las empresas.

Sólo la **sincronía** entre estos **tres ámbitos** permitirá que la regulación se traduzca en una **realidad interoperable y segura.**



Por otro lado, es fundamental tener en cuenta la visión del mercado y las empresas necesitan visualizar estos actos no como un trámite, sino como un manual técnico que define cómo podrán integrarse en la EUDI Wallet.

Cada paquete trae oportunidades (nuevas formas de onboarding digital, autenticación o firma) pero también obligaciones (registro, aceptación obligatoria, adaptación de sistemas).





La certificación de la cartera desde una perspectiva triaxial

- Criterios de homologación homogéneos
- Laboratorios acreditados
- Procesos de evaluación repetibles que garanticen la confianza en todos los Estados miembros.



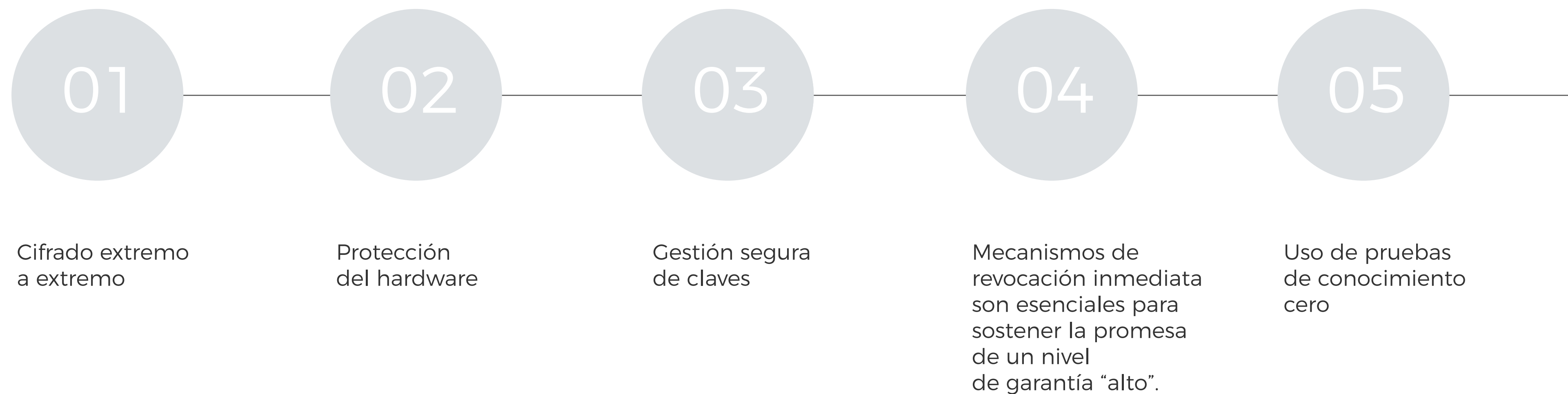
En el plano **económico** y de mercado, la obtención del sello de certificación se convierte en un activo de marca, capaz de transmitir fiabilidad tanto a usuarios finales como a clientes institucionales y de obligar a toda la cadena de valor -verificadores, emisores y entidades de confianza- a documentar su conformidad.





Sin esa convergencia, la certificación sería un mero trámite; con ella, se transforma en la licencia real para operar en el ecosistema europeo.

El plano tecnológico completa el triángulo:





Existen varios proyectos y consorcios clave para el desarrollo de la identidad digital en Europa:

Pilotos a gran escala (LSP): la validación en el mundo real

Los pilotos a gran escala o LSP (Large Scale Pilots) son iniciativas financiadas por la Comisión Europea que permiten probar y mejorar las especificaciones técnicas de la cartera digital antes de su implementación generalizada en los Estados miembros. Estos proyectos abarcan una amplia variedad de casos de uso cotidianos, involucrando a más de 350 entidades públicas y privadas de 26 Estados miembros, así como de Noruega, Islandia y Ucrania.

Busca fomentar la innovación en seis sectores estratégicos: servicios gubernamentales, banca, telecomunicaciones, licencias de conducir móviles, firmas electrónicas y salud.

POTENTIAL

Proyecto multinacional que aprueba la Cartera de Identidad Digital Europea.

Digital Credentials for Europe (DC4EU)

Trabaja en la implementación de credenciales digitales de viaje para facilitar la movilidad transfronteriza segura.

EU Digital Wallet Consortium (EWC)

Formado por países nórdicos, bálticos, Italia y Alemania, diseñado para probar el uso de la cartera digital a la hora de autorizar pagos y promover la interoperabilidad en transacciones electrónicas.

NOBID

Los pilotos a gran escala (LSP) desde una perspectiva triaxial

Los proyectos piloto a gran escala (LSP) actúan como filtro de realidad para todo el sistema. Desde la gobernanza, permiten que los Estados miembros extraigan lecciones conjuntas y las conviertan en directrices operativas que faciliten la adopción posterior, incluso en administraciones locales.

En el terreno del mercado, estos pilotos ofrecen a las organizaciones la ventaja del “first mover”: ensayar procesos de alta, firma electrónica o verificación de atributos con usuarios reales, medir tasas de conversión y abandono y ajustar modelos de negocio antes de la obligatoriedad general.

En el frente tecnológico, los LSP son un auténtico laboratorio de interoperabilidad, donde se validan credenciales, flujos de presentación y mecanismos de revocación entre plataformas, sistemas operativos y redes distintas, identificando cuellos de botella y garantizando la estabilidad del servicio.

La experiencia conjunta en estos tres niveles es la que permitirá llegar a 2026 con riesgos controlados y una infraestructura lista para escalar.

Los LSP son fundamentales para validar y verificar los sistemas y detectar posibles riesgos antes del despliegue masivo



4.

Retos y soluciones tecnológicas

Uno de los retos actuales es el manejo de la ingente cantidad de información que se genera en cualquier proceso productivo, en los sistemas de la administración y servicios públicos o en las diferentes fases de desarrollo de cualquier empresa.

Los centros tecnológicos como **Gradient**, líder europeo en el desarrollo de **Deep tech** en el ámbito de las TIC, trabajan para ofrecer soluciones que permitan almacenar, gestionar y hacer un uso eficiente de todos esos datos con técnicas de Inteligencia Artificial Aplicada. El centro cuenta con una amplia experiencia en el desarrollo y diseño de sistemas de procesamiento de información de diversa naturaleza y adaptados a diferentes entornos.

Son herramientas que se valen de la Inteligencia Artificial Aplicada para poder extraer la información relevante y que las empresas y administraciones públicas pueden aplicar con todas las garantías de seguridad y privacidad.

En paralelo al desarrollo de estas soluciones, destacan además los avances realizados por **Gradient** a la hora de garantizar:

- Seguridad
- Privacidad
- Anonimización de los datos, de los que se extrae información de gran utilidad para agilizar procesos en los que el tiempo es un factor clave.

Precisamente tecnologías como **blockchain** pueden servir de base para la construcción de plataformas de identidades seguras, donde de una manera descentralizada, empresas, administraciones públicas y ciudadanos puedan servirse de ellas para verificar los atributos de identidad.

Blockchain actuaría como registro inmutable y transparente sobre el que construir un anclaje de confianza que las entidades pueden utilizar para verificar información proveniente de las carteras.

En este sentido, conviene diferenciar entre credenciales

Cualificadas

Podrán emitir prestadores de servicios de confianza o entidades públicas adscritas como emisores cualificados. Por encima de estas, se encuentra la PID (Person Identification Data), que es la credencial que identifica a una persona natural como ciudadano de la Unión, y sólo podrán ser emitidas por las organizaciones designadas a nivel nacional, por ejemplo, la policía.

No cualificadas

Son aquellas que puede emitir cualquier entidad que desee realizar cualquier acción con una e-wallet.

5.

NovaWallet: el futuro de la identidad en la UE

Las carteras digitales se han convertido en uno de los productos estrella para los usuarios de dispositivos móviles. Empresas y administraciones públicas se están sumando al uso de esta tecnología para facilitar el acceso a los servicios en línea, especialmente ahora que las carteras digitales se convertirán en un componente esencial de las identidades digitales dentro del marco eIDAS2.

Dentro del ecosistema de identidad digital europeo, Gradiant cuenta con NovaWallet, una e-wallet sencilla, confiable y alineada con eIDAS2 y la infraestructura EBSI (European Blockchain Services Infrastructure). Se trata de una solución -disponible para iOS, Android y web- que permite a los ciudadanos europeos acceder de manera más rápida y sencilla a los servicios online que ofrecen las administraciones públicas, garantizando su seguridad y privacidad.

La cartera combina:



diseñada para facilitar la adopción empresarial de esquemas de identidad soberana.

NovaWallet es una herramienta de Gradiant ya disponible para facilitar una identidad digital europea interoperable y soberana como exige el eIDAS2

Esta innovación, pensada para sustituir a los certificados digitales actuales, constituye una de las primeras e-wallets en recibir el sello de conformidad a nivel europeo EBSI, que la acredita como una de las pruebas de identidad seguras y compatibles con su modelo regulatorio para la identificación digital de ciudadanos.

Con la incorporación de la tecnología blockchain a esta billetera digital, Gradiant ofrece un servicio completo que permite la autenticación de los usuarios, de forma totalmente segura y fiable, tanto para personas como para organizaciones.

NovaWallet ha sido una de las primeras carteras digitales en recibir el sello de conformidad europeo

NovaWallet admite tanto flujos dentro del mismo dispositivo como entre dispositivos y está preparada para ofrecer respaldo en la nube con altos niveles de privacidad y seguridad.

Además, cuenta con un framework que permite crear carteras digitales ad-hoc, pudiendo también crear futuras wallets estandarizadas como la EU Business Wallet (EUB Wallet) u otras soluciones a medida que una entidad quiera tener para sus procesos internos.

Características NovaWallet

Integración con EBSI y eIDAS2

Adopta estándares de interoperabilidad, credenciales verificables y protocolos de intercambio alineados con la normativa europea.

Roles múltiples

Las empresas pueden operar como Trusted Accrediting Entity (TAE), Trusted Issuer (TI) o Verifier, facilitando todo el ciclo de emisión, recepción y validación de credenciales.

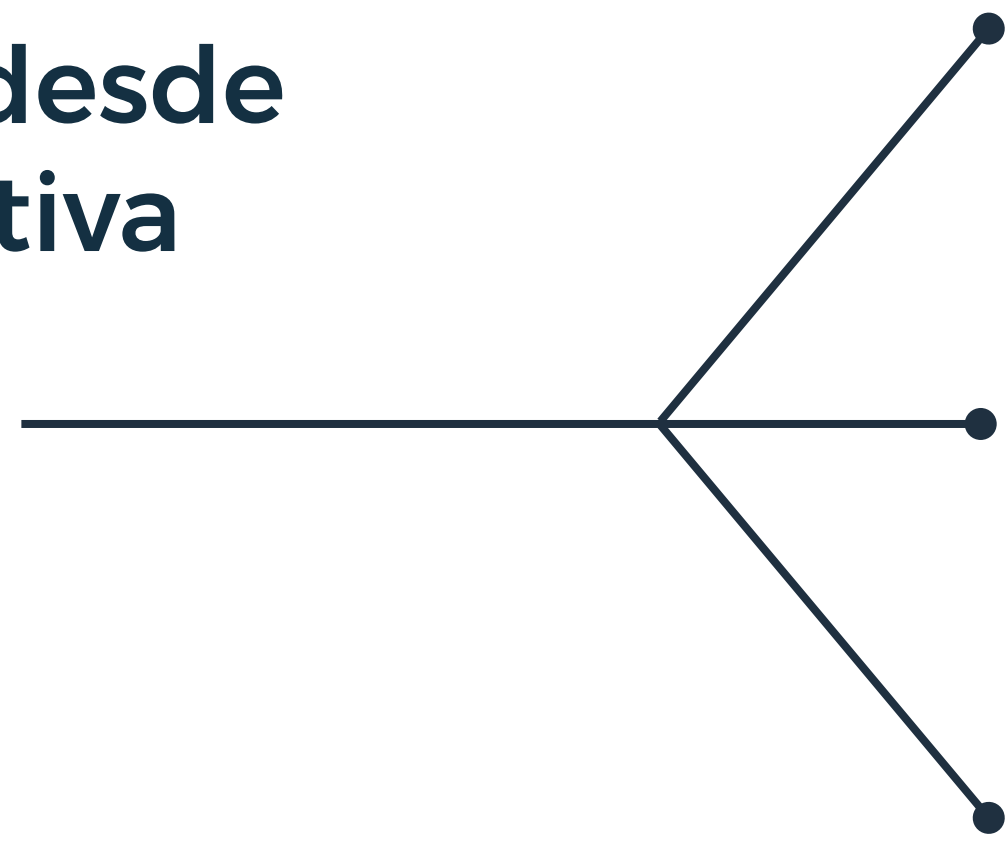
Privacidad y seguridad avanzadas

Implementa tecnologías de mejora de privacidad (PET), entornos de ejecución confiables (TEE), disclosure selectiva y pruebas de conocimiento cero (ZKP), reforzando el control del usuario sobre sus datos.

Experiencia fluida

Su interfaz intuitiva facilita el registro, onboarding, gestión de credenciales y presentación, sin comprometer la accesibilidad, incluyendo soporte TEE y movilidad en la nube.

Análisis de NovaWallet desde una perspectiva triaxial



En el plano político y de gobernanza, la solución se alinea con el reglamento eIDAS2 y con los estándares de la infraestructura europea de servicios blockchain, ofreciendo a las administraciones una herramienta que facilita la interoperabilidad y la definición de políticas de gestión y revocación de credenciales.

Desde la óptica de mercado, su propuesta de valor es clara: reduce los costes de desarrollo interno, acelera procesos de alta y verificación, y abre oportunidades en sectores tan diversos como las finanzas, la educación, la sanidad o la administración pública, respaldada por casos de uso ya validados.

En el plano tecnológico, NovaWallet destaca por su arquitectura segura -con enclaves de ejecución confiable, técnicas de privacidad avanzada y compatibilidad plena con iOS, Android y web-, su observabilidad mediante métricas detalladas y su adhesión estricta a los estándares EBSI, lo que garantiza una integración rápida y fiable.

La combinación de estos tres vectores convierte la plataforma en un acelerador real para quienes deban cumplir los plazos de la identidad digital europea.

Casos de uso reales

NovaWallet ya ha sido validada en escenarios reales como:

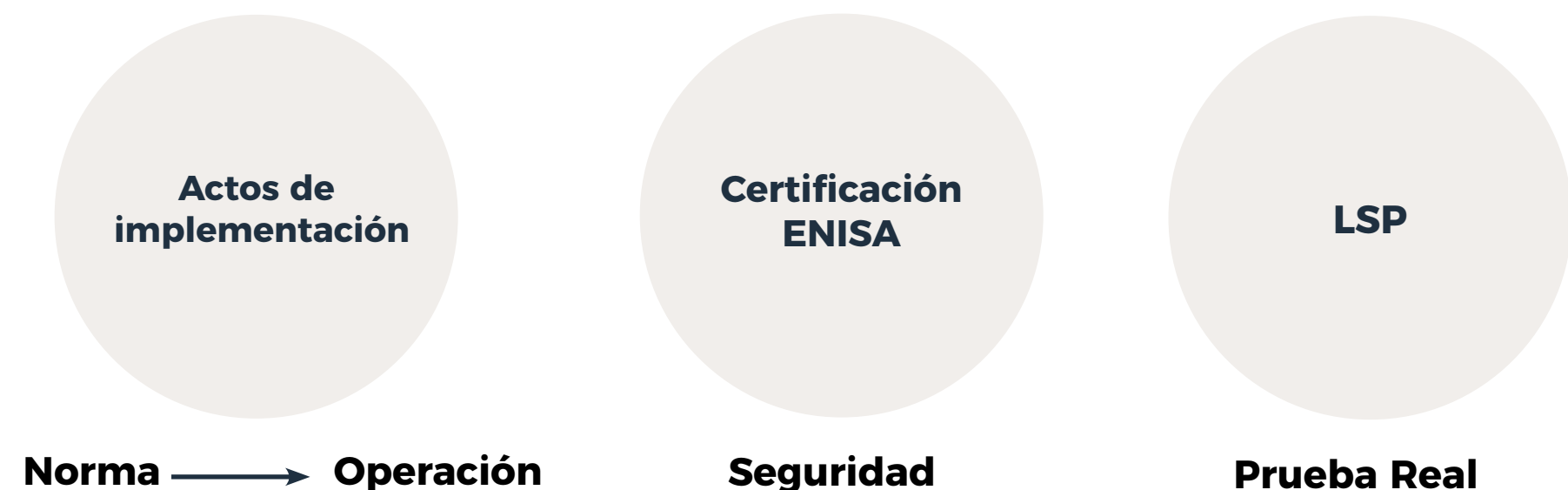
- Onboarding digital (administración pública, seguridad financiera, telecomunicaciones, movilidad).
- Trámites con la administración pública basados en identidad soberana.
- Emisión y verificación de certificados educativos y profesionales.
- Pilotajes en proyectos respaldados por la UE, especialmente dentro del programa ACID (identidad descentralizada para ciudadanía).

6.

Conclusiones

La identidad digital europea entra en una fase decisiva:
Pasar de fragmentación a interoperabilidad soberana.

eIDAS2 + la EUDI Wallet



Transformación en realidad operativa

Administraciones

- Armonizar y seguridad
- Métricas Comunes
- Supervisión efectiva
- Confianza pública

Mercado/Empresas

- Obligación de Aceptación
- Onboarding sin fricción
- Firma electrónica
- Verificación de atributos

↓ Fraude ↑ UX

Ecosistema tecnológico

- APIs Estables
- Formatos robustos
- Gestión de claves
- Ingeniería de interoperabilidad

Interoperabilidad - Seguridad - Confianza

NovaWallet Gradient

- Conformidad EBSI
- APIs maduros
- Seguridad avanzada
- Certificaciones técnicas
- Casos validados



Cumplir plazo regularotios



Escalar confianza



Acelerar adopción



Identidad digital europea

Interoperable,
soberana y operativa
desde hoy