



• GUÍA PRÁCTICA · EDICIÓN 2026

eIDAS 2.0: la **Cartera Europea de Identidad Digital**, lo que se sabe y lo que no

Todo lo que necesita saber sobre la Cartera Europea de Identidad Digital (EUDI Wallet) para preparar sus flujos desde hoy, sin apostar a ciegas por un dispositivo todavía incierto.

🕒 10 min de lectura

📅 Wallets a finales de 2026

👤 Banca · Telecom · Retail

El reglamento **eIDAS 2.0**, en vigor desde mayo de 2024, fija un calendario preciso para el despliegue de la **Cartera Europea de Identidad Digital (EUDI Wallet)**. Lanzamiento a finales de 2026, integración obligatoria para bancos y telecoms a finales de diciembre de 2027. El marco está definido, pero muchos aspectos concretos siguen sin aclararse y afectan directamente a sus decisiones de negocio e IT. Una cosa es segura: bien enfocada, esta regulación es una **oportunidad de negocio**: menos fricción, menos fraude, más conversión. Esta guía detalla también **la urgencia propia de cada sector**, banca, telecom o retail, con casos concretos por actividad.

1 Cómo funciona

DEFINICIÓN

La **EUDI Wallet** es una cartera de identidad digital puesta a disposición por cada Estado miembro. Permite a un ciudadano europeo demostrar su identidad, y transmitir determinados documentos, a un tercero (banco, operador, administración) con un nivel de confianza «alto», equivalente a un documento de identidad físico.

3 fechas clave que recordar

Finales de 2026

Lanzamiento de las wallets

Puesta a disposición

Finales de dic. 2027

Integración obligatoria

Bancos y telecoms

2030

Objetivo de adopción

80% de los ciudadanos de la UE

El recorrido del usuario en 4 pasos



Escaneo del QR

El servicio muestra un código QR que el usuario escanea con su wallet



Autenticación

Biometría o código PIN para abrir la cartera



Consentimiento

El usuario valida los datos que se comparten con el tercero



Transmisión

El servicio recibe datos certificados por el Estado: nada que fotografiar, nada que volver a teclear

Contenido mínimo garantizado: el PID



Datos de identidad

Nombre, apellidos, fecha de nacimiento, nacionalidad: la identidad básica certificada por el Estado emisor



Nivel de confianza «alto»

Equivalente a un documento de identidad físico: la cartera cuenta con el nivel de garantía más elevado



Documentos complementarios

Justificante de domicilio, nóminas, títulos académicos... y, más adelante, la autenticación reforzada de los pagos, prevista por el reglamento



Clave: a partir de finales de diciembre de 2027, los bancos y los operadores de telecomunicaciones deberán aceptar la cartera europea como medio de identificación en sus procesos de alta de clientes.

El marco está definido, pero **muchos aspectos concretos siguen sin aclararse** y afectan directamente a sus decisiones de negocio e IT. Cuatro grandes zonas de incertidumbre estructuran hoy el debate.



#1 · Calendario de las atestaciones

El PID (datos de identidad) estará disponible a finales de 2026. Pero para los **demás documentos** (domicilio, nóminas, títulos), no se ha comunicado ningún calendario.

Visibilidad limitada



#2 · Ritmo de despliegue nacional

Italia ya está en producción y Dinamarca ha lanzado la suya. Francia está en fase de pruebas (France Identité aún no está certificada) y Alemania apunta a principios de 2027. **Se esperan entre 30 y 50 wallets**, todavía no interoperables.

Despliegue desigual



#3 · Variantes nacionales

Los actos de ejecución están publicados desde diciembre de 2024. Pero cada implementación nacional conserva **sus propias variantes**, y la interoperabilidad real está por demostrar.

Interoperabilidad por demostrar



#4 · Tasa de adopción real

El uso ya es una realidad: **más de 100 M de europeos** tienen una identidad digital nacional (80-95 % en los países nórdicos, 83 % en Italia). Queda por delante un **periodo híbrido de 5 a 10 años** durante el cual la cartera y los flujos clásicos coexistirán.

Híbrido 5-10 años



Consecuencia estratégica: ante estas incertidumbres, solo una estrategia se sostiene: construir desde ahora flujos **flexibles**, capaces de absorber la cartera cuando llegue, sin depender de ella. Y el nivel de garantía de la cartera ya está disponible: la **lectura NFC** del chip del documento de identidad, firmado por el Estado. De hecho, es en ese mismo chip en el que se apoyarán las wallets para enrolar a sus usuarios.

Las 5 limitaciones estructurales de la cartera

Incluso una vez desplegada, la cartera europea solo resolverá **una parte de la necesidad**. Cinco limitaciones estructurales se imponen, no por defectos de implementación, sino por el propio diseño del dispositivo.



#1 · Ningún dato financiero

La cartera certifica **quién** es el cliente, no **si puede pagar**. Sin ingresos, sin cargas, sin historial bancario.



#2 · Sin detección dinámica del fraude

La cartera certifica la identidad en un **momento puntual**. No detecta deepfakes, ni identidades sintéticas, ni testaferros.



#3 · Solución exclusivamente B2C

La cartera no cubre **el KYB**: titulares reales, cuentas anuales y procedimientos concursales deben verificarse por otras vías.



#4 · Limitada a Europa

La cartera cubre **únicamente** a ciudadanos y residentes de la UE. Para clientes de fuera de la UE, una verificación complementaria sigue siendo imprescindible.



#5 · Solo flujos digitales

La cartera está diseñada para los flujos digitales. **En el punto de venta físico**, es imposible utilizarla sin una solución complementaria.

La cartera cubre el **20 %** de la necesidad, no más

20 %

Cartera europea
(identidad básica certificada)

80 %

Soluciones complementarias
(solvencia, fraude, tienda, KYB)



La cartera por sí sola no basta. Solvencia, fraude post-onboarding, flujos en tienda, cumplimiento AMLR: otras tantas áreas que seguirán siendo responsabilidad suya.

Más allá del principio, estas tres situaciones concretas ilustran lo que la cartera europea **no podrá resolver**, ni siquiera plenamente desplegada.

1

Financiación en el concesionario

Un cliente quiere financiar su vehículo directamente en el punto de venta.

Problema:

la cartera no funciona en el punto de venta físico. Vuelta al papel: fotocopia, verificación manual, 20 minutos perdidos y cero garantías sobre la autenticidad.

2

Cuenta comprometida 3 meses después de la validación

Un cliente fue validado en el momento del alta. Tres meses más tarde aparecen transacciones sospechosas: sus credenciales han sido comprometidas y su cuenta la está utilizando un defraudador.

Problema:

la cartera certifica la identidad una sola vez, en el momento del alta. ¿Y después? Ninguna monitorización, ninguna detección de anomalías.

3

Crédito de 20.000 € con deudas ocultas

Un particular solicita un crédito de 20.000 €. Su identidad se verifica con la cartera. Seis meses después: impago y descubrimiento de 50.000 € de deudas no declaradas.

Problema:

la cartera dice

quién

es el cliente, no

si puede pagar

. La identidad está certificada; la solvencia, no.

Un punto en común: en cada uno de estos casos, la cartera aporta una pieza, la identidad, pero el riesgo está en otra parte. Es toda la **orquestración** del recorrido lo que hay que replantear.

Detrás de la etiqueta «cartera europea» se esconden **realidades nacionales muy distintas**. La gestión de un dato tan simple como la dirección postal es el ejemplo más ilustrativo.

🕒 Francia · 2 fuentes, hasta 1 año de desfase

- **Fuente 1: la administración tributaria.**
Dirección fiscal, actualizada una vez al año (mayo-junio).
- **Fuente 2: La Poste.** Dirección postal, actualizada en el momento de la mudanza.
- **Desfase de hasta un año** entre ambos registros.

✓ Alemania · fuente centralizada, siempre actualizada

- ✓ **Fuente única centralizada.** Dirección fiscal = dirección postal.
- ✓ **Declaración obligatoria** de cualquier cambio en un plazo de 3 semanas.
- ✓ **Sincronización automática** entre administraciones.

⚠ **Consecuencia:** el «estándar europeo» esconde implementaciones nacionales muy distintas. Su solución debe saber gestionar **las particularidades de cada país** y agregar varias fuentes para cubrir las lagunas.

El fraude, en cambio, no espera a 2027: **+2 137 % de deepfakes en tres años, +300 % de documentos falsos generados por IA**. Prepararse para el DAS 2.0 significa, por tanto, elevar el nivel de garantía ahora, **sin apostar todo** a un dispositivo cuyo contenido exacto y cuya tasa de adopción siguen siendo inciertos. Se trata de integrar una solución que **orqueste de forma inteligente** la cartera Y los flujos clásicos.



1 · No apostar todo a la cartera

La cartera será un canal de identidad entre otros, nunca el canal único. Invierta en una solución capaz de orquestar todas las fuentes según su disponibilidad.



2 · Anticipar las particularidades nacionales

Cada país tiene sus especificidades (p. ej.: la dirección en Francia vs Alemania). Su solución debe poder agregar varias fuentes para cubrir las lagunas y gestionar las diferencias.



3 · Pensar en orquestación, no en integración

Una lógica automática: ¿cartera disponible? Se utiliza. ¿Documento con chip? Lectura NFC, abierta al sector privado desde junio de 2025 (reglamento 2025/1208): el nivel de garantía de la cartera, desde hoy. ¿Si no? Flujo documental. ¿Cliente extranjero? Soluciones internacionales. ¿Cliente empresa? KYB.



4 · Mantener el cumplimiento AMLR

La cartera facilita el control de identidad básico, pero no exime de las obligaciones: CDD, EDD, screening de sanciones / PEP, monitorización continua. Y para aceptarla habrá que estar inscrito en el registro de partes usuarias (reglamento 2025/848).



Recordatorio AMLR: la identidad certificada por la cartera no exime de las obligaciones de diligencia debida en materia de PBC/FT. CDD, EDD, screening de sanciones / PEP y monitorización continua siguen siendo imprescindibles.

El calendario regulatorio de eIDAS 2.0 no se aplica de la misma forma a todas las actividades. Algunos sectores tienen una **obligación legal con fecha**, otros un **dolor operativo inmediato** que la cartera no resolverá, y otros, por último, quedan fuera del ámbito de la obligación pero se enfrentan a la misma limitación estructural: **la cartera solo funciona online**.



Bancos & Fintechs

Obligación legal con fecha: integración de la cartera europea impuesta a **finales de diciembre de 2027** (artículo 5f del reglamento eIDAS 2.0, articulado con el AMLR, aplicable el 10 de julio de 2027 para el alta de clientes a distancia).

La cuestión ya no es «si», sino «cómo orquestar»: aceptar la cartera cuando el cliente la tenga, mantener un flujo clásico cuando no la tenga, sin rupturas de cumplimiento PBC/FT. **Las primeras licitaciones sobre la wallet ya circulan** en el sector.

Obligación a finales de dic. 2027



Telecom & Grandes Facturadores

El mismo plazo obligatorio de 2027, y un dolor mucho más inmediato: la **activación de tarjetas SIM en tienda** ya exige una verificación de identidad presencial que la cartera, pensada para los flujos online, no cubre.

Mientras la cartera no cubra el punto de venta físico, la verificación de identidad en tienda seguirá siendo un ángulo muerto regulatorio y operativo que hay que resolver desde hoy. Ahí es donde se juega el fraude en la contratación.

Dolor inmediato: SIM en tienda



Retail, Auto & Punto de venta

Sin una obligación legal simétrica a la de bancos y telecos, pero con la misma limitación estructural: la cartera solo funciona **online**. En el concesionario o en la tienda, sin conexión con la cartera, la vuelta al papel es pura y simple.

El punto de venta físico seguirá siendo, durante mucho tiempo, un recorrido que asegurar con independencia del calendario de eIDAS: financiación en concesionario, entrega de llaves, recogida en tienda. La verificación en el punto de venta ya es una necesidad diaria del sector.

Sin obligación legal, uso diario



En resumen: con o sin obligación legal, cada sector tiene una razón propia para no esperar al plazo de 2027 para prepararse: un calendario regulatorio, un dolor operativo ya presente o una limitación estructural de la cartera que no va a desaparecer.



El enfoque Meelo: adaptarse a sus flujos

La cartera resuelve el 20 % del problema (la identidad básica certificada). Meelo resuelve el **80 % restante**: solvencia, fraude, KYB, cumplimiento AMLR, flujos en tienda. Una sola integración, y **Meelo se adapta a sus flujos, no al revés**: online, en tienda o en oficina, en España como a escala internacional.

Cartera sola vs Meelo

CARTERA SOLA

Identidad certificada, y nada más

La cartera europea aporta una pieza esencial: demostrar quién es el cliente, con un nivel de confianza «alto».

No cubre: los datos financieros

No cubre: el fraude post-onboarding

No cubre: el KYB (sociedades pantalla)

No cubre: fuera de la Unión Europea

No cubre: los flujos en tienda

MEELO

Una orquestación inteligente, end-to-end

Meelo orquesta la cartera europea y los flujos clásicos, añadiendo todo lo que la cartera no cubre.

Identidad: cartera, lectura NFC o verificación documental

Solvencia: Open Banking + análisis de justificantes

Fraude: IA y monitorización continua

KYB: análisis de la empresa & su dirigente

Cumplimiento: AMLR + flujos en tienda

La cobertura, de un vistazo

20 %

Cartera europea
Identidad básica

80 %

Meelo
Solvencia · Fraude · KYB · Tienda

100 %

De la necesidad
cubierta

Lo que Meelo añade a la cartera



Solvencia

Open Banking + análisis automático de justificantes para evaluar la capacidad de reembolso



Fraude

Detección con IA y monitorización continua, más allá del simple control puntual



KYB

Análisis de la empresa + sus dirigentes: titulares reales, cuentas anuales, procedimientos concursales



Cobertura nacional

Agregación de fuentes nacionales para cubrir las particularidades de cada país



Flujos en tienda

Verificación de identidad en el punto de venta físico, allí donde la cartera no funciona



Cumplimiento AMLR

CDD, EDD, screening de sanciones / PEP y monitorización continua integrados



Una sola integración: Meelo orquesta automáticamente la cartera europea y los flujos clásicos, añadiendo lo que la cartera no cubre: solvencia, fraude de comportamiento, KYB avanzado, cumplimiento AMLR y verificación de identidad en tienda.