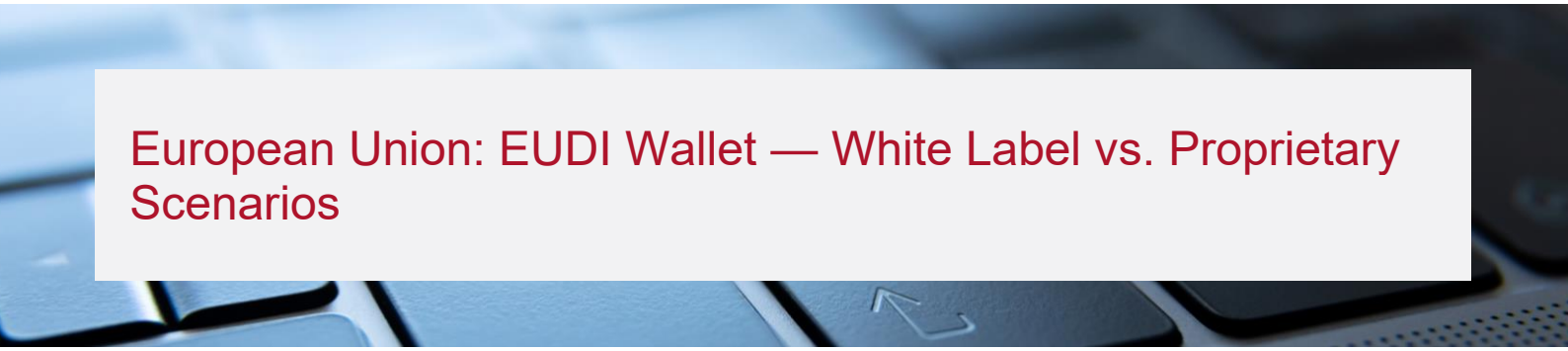
Baker McKenzie.

Client Alert

April 2026



European Union: EUDI Wallet — White Label vs. Proprietary Scenarios

Contents

In brief

The European Digital Identity (EUDI) Wallet will have significant impact on Very Large Online Platforms (VLOPs), app stores, social media services, video-sharing platforms, regulated services such as gambling or adult media, healthcare providers, financial and banking services, public sector bodies and everyone who is obliged either by contract or law to implement two-factor authentication to identify their users.

In depth

The EUDI Wallet is not a single app that will be handed to businesses ready to use. It is a European legal and technical framework established by the Electronic Identification, Authentication and Trust Services **(eIDAS) 2.0 Regulation** (Regulation (EU) 2024/1183) that will produce a market of wallet solutions — some operated by Member States, some by large platforms and companies, and some by specialized providers offering white label products to companies that do not want to or cannot develop their own wallet.

This article looks at the different ways in which businesses can engage with the EUDI Wallet framework. It explains what white label wallets are, how they differ from proprietary wallet builds, which approach is best suited for which type of business, and which businesses may not need their own wallet at all to benefit from the EUDI Wallet. Lastly, the article examines the question of whether a business that deploys a white label wallet under its own brand needs to obtain its own certification — and, if it does, what facilitations the eIDAS 2.0 framework may offer.

White label wallets

What is a white label wallet?

A white label wallet is a wallet solution developed by a specialized provider and offered to other companies so that they can deploy it under their own brand. The customer does not build the wallet entirely on its own. Instead, it uses a pre-developed wallet product and adapts it to its own visual identity, service environment and customer journey.

Even though the official recognition process for EUDI Wallets will only begin in late 2026 or early 2027, there are already numerous providers in the market developing or offering such solutions. Their products differ in scope and delivery model, but the commercial idea is the same: someone can launch a wallet without having to engineer every component himself.

Two main delivery models exist:

- **On-premises solutions**: The wallet is deployed within the customer's own technical environment. The customer operates the infrastructure.
- **Wallet-as-a-Service (WaaS)**: The wallet runs in the white label wallet provider's cloud environment. The white label provider operates the entire technical infrastructure — servers, security modules, backups, and ongoing updates required by evolving EU standards. The customer effectively **rents** the wallet functionality through an Application Programming Interface (API). An API is a standardized technical interface that allows two software systems to communicate with each other. In this context, it means the customer can integrate wallet functions into its own app or service by connecting to the provider's system through a defined set of commands — without needing to understand or manage the wallet technology behind it. This significantly

simplifies implementation, because the customer's developers do not need to build wallet logic themselves but can call on it as a ready-made service.

The WaaS model can create significant cost savings, because the customer does not need to build or maintain the underlying infrastructure.

Proprietary wallet or white label? A strategic decision

When it comes to EUDI Wallets, businesses face a fundamental strategic question: build a proprietary wallet, use a white label solution — or simply accept existing EUDI wallets, operated by third-parties?

The answer depends largely on the company's size, technical capabilities, strategic goals and willingness to invest in a complex regulatory infrastructure. However, many businesses may find that they do not need their own wallet at all.

Not every business needs its own wallet

It is important to understand that the EUDI Wallet framework does not require every business to provide its own wallet. Businesses can benefit from the EUDI Wallet already by simply accepting it.

Under the eIDAS 2.0 framework, VLOPs, public sector bodies and private parties with two-factor authentication obligations will be required to accept recognized EUDI Wallets as a means of identification. Other businesses are free to accept them voluntarily. In either case, the commercial benefit is the same: a business that accepts EUDI Wallets can verify customer identities or ages in seconds, without needing to build or operate any wallet infrastructure of its own.

Consider a bank that currently relies on video identification for customer onboarding — a process that is not only costly but also reduces conversion rates, because many customers abandon the process before completion. Once its customers carry a recognized EUDI Wallet, the bank can verify their identity in seconds by simply accepting the wallet presentation. There is no need for the bank to issue its own wallet to achieve this result.

The same applies to telecoms providers verifying customer identities for mobile contracts, to platforms implementing Digital Services Act (DSA) age-gating obligations, and to many other businesses. For these companies, the most efficient path is often to simply accept wallets issued by Member States, large platforms or other recognized providers — rather than becoming a wallet provider themselves.

For this to work, however, the user must first load the relevant document — such as a national ID card or a driving licence — into their EUDI Wallet. In many Member States, this is expected to be a straightforward process. In Germany, for example, users can transfer their identity data from the national ID card's eID chip to the wallet by simply holding the card against their smartphone and entering a PIN. The process takes only a few seconds.

That said, not every citizen will have set up their wallet immediately. In Germany, only around 22% of the population had activated the eID function of their national ID card as of 2024 — although this still represents roughly 15 million users as of now. However,this number is likely to grow significantly once EUDI Wallets become more widely available from 2027 onwards, not least because major platforms are already investing heavily in supporting them

For businesses considering whether to accept EUDI Wallets, it is worth noting that the wallet is an additional option, not a replacement. Businesses can continue to offer their existing identification methods (video identification, document upload, in-person verification) alongside the wallet. There is no obligation to discontinue other channels. Over time, as wallet adoption grows — driven in part by mandatory acceptance by VLOPs and the likely integration by major technology platforms — the wallet is expected to become the dominant identification method.

Who is likely to build a proprietary wallet?

For the largest technology platforms or businesses, building a proprietary wallet may be commercially justified and strategically attractive. These are typically companies that:

- Operate a broad **platform economy** or **world of services** where identity, payments and user accounts are already deeply integrated;
- Have existing **payment wallets** or account infrastructures that could be expanded to include EUDI Wallet functions;
- See the wallet as a **competitive advantage** — a way to deepen user engagement, control the customer experience and create new revenue streams;
- Have the **technical resources** to build and maintain cryptographic infrastructure, comply with the EUDI Wallet's **Architecture and Reference Framework (ARF)**, and manage ongoing certification processes; and

- Are willing to invest in a **long-term infrastructure project** rather than a quick deployment.

For these players, the wallet is not just a compliance tool. It becomes part of a larger ecosystem strategy. A major platform could,for example, integrate age verification, identity checks, electronic signatures and credential presentation into its existing services — all under its own brand and within its own user experience. It can then profit either from an elevated user experience, platform economy and/or by monetizing the use of the wallet vis-à-vis third parties (e.g., an app store that charges app providers a few cents for each identification).

Who is likely to use a white label solution?

White label wallets are most relevant for organizations that want to provide a wallet under their own brand but do not want to build the underlying technology themselves.

One notable group in this category are Member States themselves. Each Member State must provide at least one EUDI Wallet by late 2026. Not every Member State will have the technical capacity or political will to develop the entire wallet stack internally. White label providers can offer them a ready-to-deploy solution under the state's own brand.

Beyond Member States, white label solutions may also be attractive for businesses that do not merely want to accept existing wallets, but see a strategic value in offering their own branded wallet as part of their service environment. These are typically companies that:

- Want to **control the entire customer journey**, including the wallet experience, rather than relying on third-party wallet apps;
- See the wallet as a **differentiator** in their market — for example, a major financial services group or telecoms provider that wants to position the wallet as a core part of its digital offering;
- Want to offer wallet-based services to **their own business partners or ecosystem participants** (e.g., a platform that enables merchants to verify customer identity through the platform's own wallet);
- **Regularly need to verify specific documents** that must be present in the wallet. A car-sharing company, for example, regularly wants to verify the driving licences of its customers. So far, this requires taking a picture and a machine check, which can take up time and is inconvenient for the customer. By offering its own wallet — with the driving licence already loaded — it can ensure that the required document is always available, rather than depending on whether the customer happens to carry it in a third-party wallet. This reduces the time taken for rechecks to just a few seconds, and it is legally even more secure than requesting a photo; and
- Want the benefits of wallet provision without investing significant resources in building and maintaining an EU digital identity architecture from the ground up.

The burden of building a wallet under the eIDAS 2.0 Regulation

A company that wants to develop its own EUDI Wallet is not simply building a mobile app with login and storage functions. It is building against a regulated European identity framework with demanding legal, technical and organizational requirements.

Compliance with the architecture requirements

Every EUDI Wallet must comply with the **ARF**, the common technical architecture blueprint published by the EU. The ARF specifies how wallets must handle credential issuance, storage, presentation, trust establishment, privacy controls, communication with relying parties, and interoperability with other wallets and services. The framework uses specific protocols such as OpenID for Verifiable Presentations (OpenID4VP)E and defines detailed requirements for secure cryptographic operations. Beyond the ARF itself, wallets must also meet a wide range of additional standards — from ISO norms for document formats to European Telecommunications Standards Institute (ETSI) rules for electronic signatures and EU cybersecurity certification requirements — nearly 200 specifications in total.

The ARF currently spans several hundred pages of technical specifications and is continuously evolving. A company building its own wallet would need a specialized team capable of tracking every update to the EU standard and translating it into working code, security architecture and compliance documentation.

Certification requirements

Under the eIDAS 2.0 Regulation and the **Implementing Regulation on Wallet Certification** (Implementing Regulation (EU) 2024/2981), EUDI Wallets must undergo a formal **certification process** before they can be recognized. This certification is conducted at national level by accredited conformity assessment bodies — in Germany, for example, typically the **BSI (*Bundesamt für Sicherheit in der Informationstechnik*)**.

Certification matters for **two sides** of the ecosystem:

- For **wallet providers**, certification is what gives a wallet its legal standing. Only certified and recognized wallets produce the legal effects established by eIDAS 2.0 — most importantly, the obligation to be accepted by businesses. A wallet that is technically functional and fully compliant with all applicable standards, but not formally certified, does not benefit from this effect. Without certification, there is no mandatory acceptance — and without mandatory acceptance, the wallet has limited practical value.
- For **businesses that accept wallets**, certification is what makes the wallet a reliable compliance tool. Accepting a certified EUDI Wallet is the digital equivalent of being presented a physical identity document, a driving licence or another official credential. When a bank verifies a customer's identity through a certified wallet, a social network checks a user's age, or a car-sharing service confirms a valid driving licence, etc., each of these businesses can be confident that it has met its legal obligation — whether under financial services regulations, the DSA, road traffic laws or any other applicable framework. No one can subsequently argue that the verification was insufficient. The additional advantage is that this level of assurance can be achieved in just a few clicks. That advantage, however, depends entirely on the wallet being certified. An uncertified wallet, no matter how technically sophisticated, cannot offer the same legal certainty.

However, the certification process itself is rigorous. It covers:

- **Functional requirements** (does the wallet do what it is supposed to do?),
- **Cybersecurity requirements** (is the wallet secure against attacks?), and
- **Data protection requirements** (does the wallet protect personal data in accordance with the GDPR? — the eIDAS 2.0 Regulation expressly allows certification of GDPR compliance as part of the wallet certification process).

In practice, this means extensive documentation, security testing, penetration testing, code audits, governance processes, and engagement with regulators. The process is expensive, time-consuming and requires highly specialized expertise.

How white label solutions address these challenges

The technical complexity and certification burden described above are precisely the areas where white label solutions become attractive. Rather than building the wallet architecture and navigating the certification process internally, a business can outsource both to a specialized provider.

Outsourcing technical and regulatory complexity

The white label provider takes on the initial burden of designing, developing and certifying a wallet solution that meets all applicable requirements under the eIDAS 2.0 framework. Once the wallet is operational, the provider also tracks the ARF, implements updates, maintains security standards and handles ongoing compliance work. The customer does not need to build this expertise internally.

Faster and less burdensome certification path

As discussed above, a wallet that is not certified cannot produce the legal effects of the EUDI Wallet framework. For businesses considering a white label solution, this raises a critical question: if the white label vendor has already certified its wallet solution, does the customer need to obtain its own certification — or can it rely on the vendor's existing certification, provided the vendor retains full operational responsibility and all systems remain under its control? If the customer does need its own certification, the follow-up question is whether the legal framework provides any facilitations — or whether the customer must undergo the same full certification process as if it had built the wallet itself.

(a) Who needs to be certified — and who is the "wallet provider"?

The eIDAS 2.0 legal framework does not contain any specific rules on white label wallet scenarios. In particular, it does not clearly define whether a company that deploys a white label wallet under its own brand automatically becomes a "wallet provider" in the regulatory sense — or whether the white label vendor can remain the recognized provider while the customer simply uses the wallet under its own branding, with the operation and regulatory responsibility remaining fully with the white label vendor.

The answer to this question depends on the interpretation of the term "wallet provider." The implementing legislation defines this very broadly as "a natural or legal person who provides wallet solutions" (Article 2(8) of Implementing Regulation (EU) 2024/2981). This definition offers little guidance, as it does not specify whether "provides" refers to the technical operation, the commercial offering to end users, or both. The broader legal framework provides few additional clues.

In practice, the question of whether a white label customer becomes a "wallet provider" requiring its own certification is likely to depend on the specific circumstances of each arrangement. Relevant factors may include who appears as the contractual partner

of the end user, who is listed in the app store as the provider of the wallet application, who bears liability for the wallet's technical and legal operation, and similar considerations.

(b) Certification facilitations for white label customers?

In the event a white label customer is considered a wallet provider and must obtain its own certification, the eIDAS 2.0 implementing legislation provides a mechanism that can substantially reduce the certification burden compared to a full independent certification.

Under Implementing Regulation (EU) 2024/2981, national certification schemes must allow evaluators to take into account existing "assurance information" — such as certificates of conformity, evaluation reports, test results and security assessments — when certifying a wallet solution. This is done through a process known as dependency analysis, as set out in Annex VI of the Implementing Regulation (EU) 2024/2981.

In practical terms, this likely means:

- If the white label vendor has already obtained certifications for key components of the wallet solution — for example, European Union Cybersecurity Certification Scheme (EUCC) certifications for secure cryptographic modules, ISO 27001 certifications for backend infrastructure, or detailed security evaluation reports — these documents can be **presented as evidence** in the customer's own certification process.
- The conformity assessment body then conducts a **dependency analysis**: it assesses whether the existing documentation is available, relevant and adequate for the specific wallet solution being certified.
- Where the existing assurance information is found to be adequate, the evaluator does not need to **re-evaluate those components independently**. The customer's certification effort can instead focus on the aspects that cannot be supported with existing assurance information.
- Where the existing documentation does not fully cover a requirement, the evaluator may accept **compensating controls** implemented by the customer, or may require additional evidence for the specific gaps.

This is not a formal transfer of the provider's certification. However, it is a structured mechanism for reusing existing compliance evidence, which can significantly reduce the time, cost and complexity of the customer's own certification process.

The exact scope of certification relief in white label scenarios will likely become clearer once national certification schemes are operational and conformity assessment bodies begin processing applications. What can already be said is that the regulatory framework provides the tools for a materially lighter certification path when building on an already-certified wallet solution — even if it does not eliminate the certification requirement entirely.

Your contact

Sebastian Schwiddessen LL.M.
Counsel
sebastian.schwiddessen@bakermckenzie.com

© 2026 Baker & McKenzie. **Ownership:** This site (Site) is a proprietary resource owned exclusively by Baker McKenzie (meaning Baker & McKenzie International and its member firms, including Baker & McKenzie LLP). Use of this site does not of itself create a contractual relationship, nor any attorney/client relationship, between Baker McKenzie and any person. **Non-reliance and exclusion:** All information on this Site is of general comment and for informational purposes only and may not reflect the most current legal and regulatory developments. All summaries of the laws, regulation and practice are subject to change. The information on this Site is not offered as legal or any other advice on any particular matter, whether it be legal, procedural or otherwise. It is not intended to be a substitute for reference to (and compliance with) the detailed provisions of applicable laws, rules, regulations or forms. Legal advice should always be sought before taking any action or refraining from taking any action based on any information provided in this Site. Baker McKenzie, the editors and the contributing authors do not guarantee the accuracy of the contents and expressly disclaim any and all liability to any person in respect of the consequences of anything done or permitted to be done or omitted to be done wholly or partly in reliance upon the whole or any part of the contents of this Site. **Attorney Advertising:** This Site may qualify as “Attorney Advertising” requiring notice in some jurisdictions. To the extent that this Site may qualify as Attorney Advertising, PRIOR RESULTS DO NOT GUARANTEE A SIMILAR OUTCOME. All rights reserved. The content of the Site is protected under international copyright conventions. Reproduction of the content of this Site without express written authorization is strictly prohibited.