GFOSS
OPEN TECHNOLOGIES ALLIANCE

9, Iroon Polytechneiou str. 15780, Athens, Tel: 2102209380

Athens, 8 July 2025
Protocol Number 378

Subject: Leveraging the EUDI Wallet for EU Login: Technical Evaluation and Proposed Model

Introduction

The European Digital Identity (EUDI) Wallet is a new initiative under the eIDAS 2.0 regulation, intended to provide all EU citizens and businesses with a secure, user-controlled digital identity wallet. It can store personal identification data and electronic attestations (credentials) and allow users to **authenticate to services and share specific attributes** in a privacy-preserving way. The European Commission's Directorate-General DIGIT has been piloting the use of the EUDI Wallet in various domains – for example, testing a wallet-compatible app for Commission employees in the healthcare sector – to enable convenient access to EU services using digital credentials instead of traditional login methods. These pilots align with broader EU trials in sectors like finance, education, transport, and health to validate the wallet's functionality.

A key challenge has emerged in integrating the EUDI Wallet with **EU Login** (the European Commission's central authentication service): **regulatory requirements mandate that any service interacting with the EUDI Wallet must be a recognized, trusted party.** According to the EUDI Wallet Architecture and Reference Framework (ARF v2.0) and the draft implementing acts of the regulation, *wallet-relying parties* (i.e. services that request or verify credentials from the wallet) must be officially **registered on an EU trust list**. In practice, this means any entity that wants to issue credentials to the wallet or consume credentials from it must be certified and listed by a Member State's designated authority. This requirement raises the question: **How can EU Login – an EU institution service (not tied to a single Member State or a conventional legal entity under national law) – qualify as a trusted relying party in the EUDI ecosystem?**

Challenge: Trust Framework Requirements for Relying Parties

Under the proposed European Digital Identity framework, **all participants** in the wallet ecosystem (wallet providers, identity/attribute issuers, and relying parties) must adhere to a strict trust model. This includes undergoing conformance assessments and being listed in **national "trusted lists"** maintained by Member States. Each Member State will have a **register of wallet-relying parties** (services intending to use wallets) and an authority (registrar) overseeing it. A relying party must typically:

- **Be a legal entity established in a Member State** (so it can register under that country's jurisdiction).

- **Apply for registration** as a wallet-relying party, providing details about the service and the user data it will request.

- **Obtain credentials (digital certificates)** from a trusted authority to authenticate itself to wallets. In particular, an approved relying party receives a *wallet-relying party access certificate* used to identify itself when connecting to a user's wallet, and a *registration certificate* listing which attributes it is authorized to request.

These measures ensure that when a wallet is asked for data, it can verify the requesting service's legitimacy (via the certificate) and inform the user that the service is officially trusted. The wallet will **refuse or warn** on requests from unlisted or untrusted parties.

For the Commission's **EU Login** service, this presents a dilemma. EU Login enables access to many EU institutions' digital services and is operated by the EU itself (DIGIT), rather than by a legal entity in a single Member State. The **European Union as an entity is not a "legal person" in a national jurisdiction**, and EU institutions don't neatly fall under a Member State's supervisory authority for trust lists. In other words, EU Login **cannot directly register** as a wallet-relying party in a national trust list in the same straightforward way a company or national agency could. This could technically bar EU Login from consuming credentials from the EUDI Wallet, despite the policy goal of enabling EU-wide public services to accept wallet-based authentication.

Proposed Solution: Wallet Integration Service as an Intermediary

To overcome this hurdle, a **dedicated wallet Integration service operated by a separate legal entity** has been proposed. In this model, an organization that *is* a legal person (for example, a private company or a public-law entity in a Member State) would serve as an **intermediary between the EUDI Wallet and EU Login**. This intermediary acts on behalf of EU Login to fulfill all the trust framework obligations. Essentially, it would be the **certified relying party** interacting with wallets, and EU Login would rely on it for wallet-based authentication. The intermediary service could either be a contractor to DIGIT or a special-purpose entity set up for this role. The key elements of this model are:

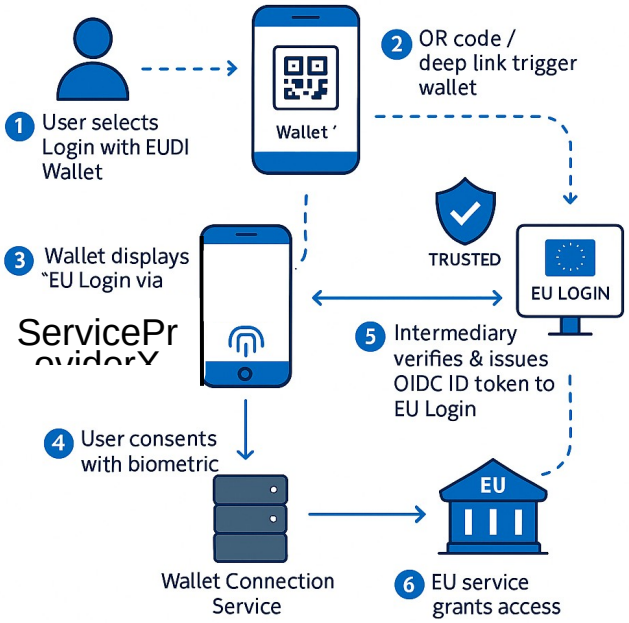
- **Trust List Registration:** The wallet Integration service would formally **register as a wallet-relying party** in one of the Member States. As a legally recognized entity, it can go through the national registration process, submit the required information (service details, data requested, etc.), and obtain approval to be included in the national trust list of wallet-relying parties. Once registered, it gains a trust anchor (public key certificate) that is published in the trust list, allowing wallets across the EU to recognize it as trusted. This satisfies the requirement that any party interacting with the wallet is **in the EU trust ecosystem**. EU Login itself would **not need to register**; instead, it leverages the intermediary's trusted status.
- **Attestation Issuance:** In addition to being a verifier, the intermediary can also function as an **issuer of credentials** (attestations) needed for EU Login. For example, EU Login may require a certain credential in the user's wallet to authenticate them – such as an "EU Login Authentication Attestation" or an organizational identity credential for EU staff. The wallet Integration service can be equipped to **issue such attestations into users' wallets** on behalf of the EU institution. To do so, it would also register (if necessary) as an *Attestation Provider* under the trust framework (the requirements for issuers are similar: they must be audited/trusted and listed). The **technical protocol for issuance** would follow the EUDI Wallet standards: specifically, the service would use **OpenID Connect 4 Verifiable Credential Issuance (OIDC4VCI)** to issue credentials to the wallet. The EUDI ARF mandates OIDC4VCI as the interface for wallet issuance flows,

meaning the intermediary can seamlessly send a signed attestation to the user's wallet app over a standard API. This attestation might contain, for instance, the user's identity as recorded in EU Login, or a verified attribute (such as their employee status or security clearance) needed for login.

- **Verification and Authentication Service:** The core role of the intermediary is to act as a **verifier** when a user wants to log in with their EUDI Wallet. In practice, this means the service will handle the **Verifiable Presentation** of credentials from the wallet. Technically, it would initiate an **OIDC4VP (OpenID Connect 4 Verifiable Presentations) flow** to request the necessary data from the user's wallet. For example, when a user chooses to log in via EUDI Wallet, EU Login (through this service) might request a "proof of identity" or a specific attribute from the wallet (like *date of birth*, or an *employment credential* if logging in as an EU staff member). The intermediary, as a registered relying party, **creates a presentation request** in the format defined by OIDC4VP – which includes details of the requested credential(s) and a challenge – and transmits it to the user's wallet (often via a QR code scan or a secure app-to-app redirect or even via DC API). The wallet, seeing the request is signed by a trusted party (the intermediary's certificate), prompts the user to consent and then returns a **Verifiable Presentation** (a cryptographically signed package of the requested attributes) back to the intermediary. The intermediary service then **validates the presentation**: it checks the digital signatures on the credential (to ensure it was issued by a trusted authority and hasn't been tampered with), verifies the credential's issuer is on the trust list (e.g. a national ID provider or the intermediary itself if it issued it), and confirms that the credential is not expired or revoked. It also verifies **proof of wallet possession** (device binding) and user binding if required – ensuring the person presenting the credential is the rightful holder. This verification step uses the wallet trust architecture (trust anchors and possibly the European Blockchain Services Infrastructure for revocation checks, depending on implementation). Only if all checks pass does it proceed to authenticate the user.
- **Augmenting EU Login's Authentication:** Once the intermediary has a valid credential from the user's wallet, it can assert the user's identity to EU Login. Essentially, the wallet connection service functions as an **Identity Provider (IdP)** that EU Login trusts. The integration between the intermediary and EU Login would be set up via standard federated authentication protocols – most likely **OpenID Connect (OIDC)** or possibly SAML2 if needed for compatibility. In a login flow, EU Login would redirect the user to the intermediary (or to a page that invokes it) when wallet login is chosen. The intermediary completes the OIDC4VP interaction with the wallet as described, and then **issues an authentication token** (for example, an ID token or SAML assertion) back to EU Login, containing the user's identity data that was verified. From EU Login's perspective, it receives a confirmed identity (e.g., the user's name, eID number, or employee ID) via a trusted IdP and can create a session for the user. The user gains access to the EU service without ever typing a password – the security is provided by the possession of their EUDI Wallet and the cryptographic validation of their credentials. This model effectively **adds the EUDI Wallet as a new login method** to EU Login's existing methods, via the intermediary bridge.

  Illustrative Flow: A user navigates to an EU service and chooses "Login with EUDI Wallet." They are either shown a QR code or a link that triggers their wallet. The wallet connection service (intermediary) has encoded a request for, say, the user's **Person Identification Data (PID)** (the core digital identity) at LoA High, or an **EU-issued attestation** if relevant. The wallet app launches, the user sees that *"EU Login via [ServiceProviderX]"* is requesting certain info, and that this requester is certified (the wallet will display the service name and that it's a trusted party). The user consents, perhaps by entering their wallet PIN/biometric to approve. The wallet sends back the signed data. The intermediary verifies everything, then silently logs the user into EU

Login by generating an OIDC ID token. The web page refreshes and the user is now logged in. From the user's perspective, it's a smooth experience – they used their wallet to prove who they are, and got access.



- **Data Minimization and Privacy:** In this model, the intermediary acts as a **conduit of verified information** and not a data silo. Per regulatory requirements, it **does not store the contents** of any attributes or credentials longer than necessary for the transaction. After completing the verification and passing the needed data to EU Login, it must immediately delete the user's credential data. It also does not get to see unnecessary information – for example, if only an age verification or specific attribute is needed, the wallet can utilize selective disclosure to share only that piece of information. This aligns with the privacy-by-design ethos of the EUDI Wallet. The intermediary service would also facilitate compliance with features like **digital consent and audit logs**: the wallet keeps a local log and could inform the user of which attributes were shared and allow them to later exercise rights like requesting deletion by the relying party, as mandated by the framework. From a GDPR perspective, the intermediary would likely be a data processor acting on instructions from the EU institution (which remains the data controller for the authentication process).

- **Legal Arrangement:** The EU institution (DIGIT) could contract this service from an external provider or possibly establish a special entity in a Member State to host it. The important aspect is that **the service operator is a legal person in the EU** that can assume liability and undergo certification. It would abide by the **eIDAS 2.0 rules** applicable to trust service providers or wallet relying parties. For instance, it may need to meet security requirements, be audited by a Conformity Assessment Body, and be notified to the European Commission by the Member State once in compliance. All these ensure it is a trustworthy component of the ecosystem.

Alignment with EUDI Regulations and Architecture

This proposed **intermediary model is fully aligned with the EUDI Wallet regulatory framework** and guidance:

- **Intermediary as a Recognized Pattern:** The idea of a single service connecting on behalf of multiple relying parties is explicitly anticipated in the draft European Digital Identity Regulation. Article 5b(10) of the regulation states that *"Intermediaries acting on behalf of relying parties shall be deemed to be relying parties and shall not store data about the content of the transaction."*. In other words, the law allows an intermediary to step in as the certified party for others. The ARF elaborates that an intermediary can **register once** as a relying party, obtain the necessary credentials, and then **facilitate wallet interactions for multiple "end services"** while ensuring no sensitive data is retained. In this case, the wallet connection service is exactly such an intermediary – it acts on behalf of EU Login (and potentially other EU services in the future) and follows the rule of not storing user data. This approach not only solves the legal entity issue but also *simplifies onboarding many services:* rather than each EU institution or agency separately going through certification, one intermediary can serve them all, each "end relying party" being listed under its umbrella if needed. The ARF notes that an intermediary will obtain a registration certificate for each end-party it represents (listing the attributes that end-party is allowed to request) but the end-party itself **does not need a separate access certificate**. This fits the scenario – EU Login (and by extension various Commission services behind it) could be treated as end relying parties served by the intermediary.

- **Compliance with Trust Lists:** By using a properly registered intermediary, the solution adheres to the principle that *"any service provider that wants to interact with digital wallets must register on a specific trust list at the national level and obtain an access certificate."* The intermediary will appear in the EU Trust Lists (which are expanded to include Wallet ecosystem roles). Wallets will have the trust anchors (public keys) of all authorized parties – including this service – so they can verify the signature on requests and know the source is genuine. This ensures that an EU citizen's wallet will treat the login request from EU Login (via the service) as it would any trusted eGovernment service request, maintaining the **chain of trust**. Meanwhile, EU Login itself remains out of scope of direct regulation as a relying party, avoiding a grey area in the legal framework.

- **Use of Standard Protocols (OIDC4VCI/OIDC4VP):** The proposed model strictly uses the **protocols outlined in the EUDI Wallet Common Toolbox**. The Commission's implementing act on wallet interfaces (CIR 2024/2982) and the ARF specify OpenID Connect-based protocols for issuance and presentation. In our design, the intermediary uses **OIDC4VCI for credential issuance** to wallets and **OIDC4VP for requesting/verifying credentials** from wallets. According to the ARF, OpenID4VCI and OpenID4VP are the default mechanisms for remote wallet interactions, ensuring interoperability across Member States and wallet providers. These protocols provide robust security: for instance, OIDC4VP defines signed, JWT-based presentation requests and responses, and it has inbuilt measures to guarantee **confidentiality, integrity, and mutual authentication** between the relying party and the wallet. By conforming to these standards, the intermediary service will be compatible with any wallet that follows the EU standards. It also means features like **selective disclosure** (using SD-JWT or BBS+ signatures, etc.) are supported as per the EUDI spec, allowing the intermediary to

request only what's necessary (minimizing data). Furthermore, the **wallet-relying party certificate** that the intermediary uses is part of the OIDC4VP exchange: the wallet will authenticate the service's request using that certificate, and the user will see the service's identity as derived from the cert. This technical alignment gives confidence that the solution will work within the evolving European digital identity infrastructure.

- **Policy and Security Oversight:** The intermediary model maintains the high level of assurance required by eIDAS. The intermediary, being a trust-listed party, would be subject to **supervision and audits** just like other trust service providers. Member State authorities will ensure it meets standards. The Commission's request for ENISA to support wallet certification and the stringent requirements for providers (e.g. using QSCDs for signing, incident reporting, etc.) all contribute to a secure environment. From a policy perspective, the Commission can be comfortable that even though an external entity is handling the wallet interaction, that entity is operating under strict EU-wide rules and liability frameworks. This setup thus balances the **distribution of legal responsibility** (the intermediary is responsible for its role under eIDAS 2.0) with the Commission's goal of integrating new technology.

- **Addressing the "EU not a legal person" issue:** By contracting or establishing a legal entity in a Member State to run the wallet connection service, the European Commission effectively sidesteps the problem of the EU's legal status. The reliance on a Member State's jurisdiction for trust list registration is a practical necessity given the regulation's structure (which is built on national notification and oversight). This solution has precedent in other areas – for example, EU institutions often rely on external trust service providers for qualified certificates, etc., since the trust services are nationally supervised. Here, similarly, the Commission would leverage a nationally supervised service for its own authentication needs. It's a **workaround that remains within the letter and spirit of the law**.

Technical and Operational Evaluation

Feasibility: The proposed model is technically feasible and in fact mirrors patterns already being tested. Many large-scale pilots of the EUDI Wallet involve intermediary gateways. For instance, some pilots envision private sector identity providers aggregating services for others, acting as an intermediary to connect wallets to services that cannot themselves invest in the full infrastructure. The Commission's own reference implementation and ARF documentation recognize that not every relying party will integrate directly – intermediary services (sometimes called "brokers") will play a role. The use of OIDC protocols means the intermediary can be built with modern, readily available components (OAuth2/OIDC servers with extensions for VC exchange). There are already libraries and vendors familiar with OIDC4VP/VCI since these are emerging standards (largely based on OAuth2 and JWT). Moreover, EU Login's compatibility with federated login (it already supports connecting to external IdPs via protocols like SAML or OIDC) means the integration on the EU Login side is straightforward – essentially configuration and trust establishment for tokens issued by the intermediary.

Security: This approach will **enhance the security** of EU Login authentication. Currently, EU Login supports methods like password, SMS OTP, and in some cases national eID federations. Using the EUDI Wallet introduces a **cryptographic authentication factor** of very high assurance (LoA High credentials, possibly even qualified certificates in the wallet if signing). For the user to authenticate, they must possess a wallet that is itself secured (likely by a PIN/biometric and a secure element for keys) and have a government-issued identity loaded. This greatly reduces the risk of phishing or credential theft compared to passwords. The intermediary also enforces that

the credential presented is up-to-date (not revoked) and was issued to that user's device (wallet attestation binding ensures the credential can't be copied to another device easily). Additionally, the transaction involves **dynamic challenge-response** (preventing replay attacks). All communication is over HTTPS and JSON Web Tokens, with mutual TLS likely used for the OIDC flows – aligning with best practices. The main security consideration is that the intermediary itself must be **highly trustworthy** and secure since it becomes a critical link. It will need robust protection (hardware security modules for its keys, continuous monitoring, etc.). Given that it will operate under eIDAS-like supervision, these aspects will be audited and must meet state-of-the-art security requirements.

User Experience and Acceptance: From an end-user perspective (whether Commission staff or external users of EU services), logging in with a EUDI Wallet will be a new option that could simplify access. Instead of maintaining separate credentials for EU Login, a user could leverage an identity they already have in their national wallet. For example, a citizen with a national digital ID in their wallet could use it to access an EU Commission online consultation portal via EU Login – fulfilling the vision that *"European citizens can access online services across the EU with their own national digital ID"*. Commission employees could similarly use a professional ID credential issued to their wallet (perhaps replacing or complementing the physical badge or separate login accounts). The pilot in the healthcare context for employees suggests scenarios like proving one's EU staff insurance status or eligibility via the wallet when accessing healthcare services. All these become easier with a wallet. The intermediary model does not impede user experience; it mostly operates behind the scenes. Users might see the name of the intermediary service during the wallet consent step – for transparency, the wallet might display something like "Service: EU Login via [Trusted Partner]" (as per the registration certificate info). This is acceptable, and the Commission can ensure the display name is user-friendly. Because the intermediary must reveal to the wallet the end relying party's identity, the user will also see "EU Login (European Commission)" in the consent prompt alongside the intermediary's name. The ARF actually mandates this, so users aren't confused. This dual naming could be communicated in user guidance, but ultimately if the process is smooth and quick, users will adapt. Notably, once the wallet ecosystem is common, users will expect such flows for many services (government or private), so EU Login would be keeping pace with the broader trend.

Policy Implications: Adopting this model demonstrates the Commission's commitment to its own regulations. It shows that EU institutions will also adhere to the high-level trust and security requirements, even if via an indirect method. There may need to be some **policy coordination** – for example, deciding which Member State's trust list to use for the intermediary. This could depend on where the intermediary company is established (perhaps Belgium or Luxembourg due to the Commission's presence, or any Member State willing to support the registration). The Commission will likely coordinate with that Member State's digital authority to ensure smooth notification to the EU trust framework. Since the implementing act on notification (CIR 2024/2980) sets out how Member States inform the Commission of registered entities, the intermediary would be included in that process. The Commission (as the operator of EU Login) might want a clear **Memorandum of Understanding** with the intermediary outlining compliance with all regulations, data protection, incident handling, etc. But again, because the intermediary is regulated, much of this is enforced by law already.

Pros and Cons Summary:

- *Pros:*
    - Enables EU Login to use EUDI Wallet **without changing the law** – uses existing provisions (intermediaries, trust lists).

- Leverages **high-security authentication** methods (digital signatures, verified IDs).
- **Scalable** – one intermediary can serve multiple EU services, and it can handle high volumes of auth requests (with proper infrastructure).
- The Commission retains control over the authentication **policy** (what attributes are needed for login, when to require wallet login, etc.) while outsourcing the heavy compliance lifting to a specialist service.
- Ensures **user trust**: users know any request coming to their wallet is from a verified source. EU Login gets provable data, reducing fraud (e.g., it's nearly impossible to fake someone's national ID that's in a wallet due to cryptographic protections).

- *Cons / Considerations:*
  - The intermediary sees (temporarily) some personal data (like user attributes). While it must delete them and not misuse them, the Commission should ensure strong contractual privacy clauses. There's a slight inherent privacy trade-off whenever an intermediary is in the loop versus a direct wallet-to-EU Login connection. However, given the legal obligation not to retain data, this risk is minimized.
  - The regulatory landscape is still evolving. The intermediary approach should remain valid, but the Commission should stay engaged in the eIDAS Cooperation Group discussions to ensure that EU institutions' needs are taken into account (perhaps in guidance or future standards). For instance, there might eventually be an explicit mechanism for "EU institution as relying party" – but until then, this intermediary path is the pragmatic solution.

Conclusion

In conclusion, the use of a wallet connection intermediary service is a sound and compliant strategy for integrating the EUDI Wallet with EU Login. It resolves the core issue (the EU not being a legal person that can register in a Member State) by delegating wallet interactions to a certified entity that meets all eIDAS 2.0 trust framework requirements. This model is backed by provisions in the regulation itself for intermediaries, and it aligns with the technical architecture laid out in the EUDI Wallet ARF and Toolbox (using OIDC4VCI/OIDC4VP protocols and trust list-based authentication). By implementing this approach, DIGIT can **augment EU Login's authentication capabilities** with minimal disruption: users will gain a new, secure login method using their digital wallets, while the existing EU Login infrastructure can remain largely unchanged besides integrating the new IdP.

This solution offers a high-assurance, future-proof way for EU institutions to consume the EUDI Wallet ecosystem. It demonstrates a proactive adaptation to the coming European Digital Identity framework, positioning EU services as early adopters of wallet-based login. It is both an **internal technical solution** (ensuring systems work together) and a **policy-compliant move**, supporting the broader goal of a unified European digital identity. With the intermediary model in place, the Commission can confidently pilot and roll out EUDI Wallet integrations – for example, enabling Commission staff to log in with a wallet credential, or allowing EU citizens to access Commission

portals via their national digital IDs – all while respecting the stringent security, privacy, and trust requirements that underpin the EUDI Wallet initiative.