gaia-x
Hub France

Digital Wallets at the Core of Trust in Data Spaces

Gaia-X Hub France

17/04/2026

gaia-x Hub France

Gaia-X Hub France

The Gaia-X Hub France serves as the national representative and contact point for Gaia-X in France. Its objectives are as follows:

- Bring together stakeholders involved in the Gaia-X initiative, whether members or non-members.
- Promote and organize Gaia-X-related activities across France.
- Facilitate structured exchanges and collaboration among professionals and stakeholders engaged in Gaia-X-compliant data spaces.
- Accelerate co-innovation of services and use cases, and support the incubation of data spaces that foster the development of Gaia-X-based service offerings.
- Maintain dialogue with Gaia-X, other national hubs, and the French public administration.
- Develop and disseminate training materials.

The Gaia-X Hub France is coordinated by Institut Mines-Télécom, with the support of Cigref. Its activities and outputs are funded by the Data Space Lab project (ANR-23-DSLA-0001).

Institut Mines-Télécom

RÉPUBLIQUE FRANÇAISE
Liberté
Égalité
Fraternité

Cigref
RÉUSSIR
LE NUMÉRIQUE

FRANCE 2030

Towards a Trusted Ecosystem for Data Spaces

On October 7, 2025, the Gaia-X Hub France brought together ecosystem stakeholders for a technical workshop dedicated to digital wallets (digital identity wallets). In the context of data spaces, identity and compliance to governance rules have become fundamental pillars for ensuring sovereignty and secure data exchanges.
The objective of this workshop was to explore the paradigm of decentralized identity (Self-Sovereign Identity – SSI), which gives users full control over their digital credentials, and to analyze the significant impact of the new European eIDAS v2 regulation. As a key technological pillar of SSI, digital wallets were presented through several solutions. This booklet compiles both theoretical insights and practical feedback shared during the event.

Summary of Contributions

1. Understanding Self-Sovereign Identity (SSI)
By Maryline Laurent and Montassar Naghmouchi (Télécom SudParis)
This contribution lays the theoretical foundations of the topic by explaining the transition from siloed or federated identity models to a user-centric SSI model. It details the key components: the Holder, the Issuer, the Verifier, and the decentralized registry (often a blockchain). The presentation illustrates these concepts through the TracIA project, which uses wallets to enable dynamic consent management for patients in the healthcare sector.

2. The EUDI Wallet for Data Spaces
By Van Hoan Hoang (Atos Eviden)
This contribution analyzes the evolution from eIDAS v1 to eIDAS v2 and the introduction of the European Digital Identity Wallet (EUDI Wallet). It demonstrates how this wallet strengthens trust within data spaces by providing legally recognized mechanisms to identify participants and manage access through attribute attestations. Eviden also presents its modular SSI platform and its involvement in the European APTITUDE consortium.

3. Gaining a better understanding of the Digital Identity Portfolio ecosystem
By Romain Santini and Valérie Bruna (Docaposte)
This contribution clarifies the link between Gaia-X technical building blocks (such as Verifiable Credentials) and the European legal framework. It outlines the regulatory timeline requiring Member States to provide digital wallets by the end of 2026. It also presents large-scale projects (POTENTIAL, APTITUDE, WEBUILD) and offers access to the DOCAPOSTE technical "playground" enabling developers to test the interoperability of credential issuance and verification.

4. Live Identity Wallet
By Bruno Salinier (Orange Business)
This contribution focuses on the application of digital wallets in industrial and B2B contexts, notably through the Orange Business Live Identity Wallet solution. Use cases include onboarding new business

customers, managing agricultural consent via AgDataHub, and developing an "object wallet" for vehicles, enabling the management of a tamper-proof digital logbook from the moment they leave the factory.

5. IN Groupe Wallet Solutions and Their Experimentation in Transport
By Vincent Desbiendras (IN Groupe)

IN Groupe shares its experience in deploying digital identity solutions at both national (Colombia, Chile) and sectoral levels. Particular emphasis is placed on experimentation in the transport and logistics sector in France (My Hub Pro solution), aiming to simplify access to physical sites and secure the onboarding of transport companies through digital wallets.

Understanding Self-Sovereign Identity (SSI)

Authors: Maryline Laurent, Montassar Naghmouchi, SAMOVAR,
Télécom SudParis, Institut Polytechnique de Paris, Palaiseau, 91120, France

In our increasingly digital world, identity management is a complex and fragmented process. A recent presentation by Prof. Maryline Laurent and PhD candidate Montassar Naghmouchi of Télécom SudParis - Institut Polytechnique de Paris delves into the evolution of digital identity management, culminating in a detailed exploration of Self-Sovereign Identity (SSI) as a privacy-preserving and user-centric solution.

Keywords: Self-Sovereign Identity, Identity management, Privacy, Blockchain, Wallet applications.

To understand the significance of SSI, it's essential to look at the identity models that preceded it:

1. **Siloed Model:** This is the traditional approach, where each service provider (SP) requires a user to create a separate account. This leads to a proliferation of credentials, with users managing countless usernames and passwords, and their data scattered across siloed databases. This model is now considered obsolete due to its inefficiency and security risks.
2. **Federated Model:** This model establishes a trust relationship between an Identity Provider (IdP) and multiple Service Providers (SPs). Users can use a single set of credentials to access multiple services, which is more convenient than the siloed model. However, it concentrates power and data in the hands of a few large IdPs, creating potential privacy concerns and a single point of failure.
3. **User-Centric Model:** This approach allows users to manage their identity information which they obtain from an identity provider (IdP) and present to a service provider (SP). However, the user still relies on this information from IdPs to access services, but with no single point of failure. The closest analogy is the way we store our identity cards and credentials in our physical wallets, and present them to SPs to access services (example: in the airport).

SSI represents a paradigm shift, that puts individuals in complete control of their digital identity. Instead of relying on a centralized authority, SSI operates on a decentralized trust model. Although considered a user-centric model, SSI provides more user autonomy, control and ownership of identity than any previous models.

The core components of this model are:

- **Holder:** The individual who owns and controls their identity and credentials.
- **Issuer:** An entity (e.g., a university, government, or employer) that creates and cryptographically signs verifiable credentials for a holder.
- **Verifier:** An entity that requests and verifies credentials from the holder to grant access to a service.
- **Identity Wallet:** The application that enables the previous actors to exchange and verify credentials.
- **Decentralized Registry:** Often a blockchain or other Distributed Ledger Technology (DLT), this serves as a secure and tamper-proof public ledger for anchoring identity information, such as public keys, without storing personal data.

In an SSI ecosystem, a university (Issuer) can issue a digital diploma (a Verifiable Credential) to a student (Holder). The student stores this credential in their personal digital wallet. When applying for a job, the student can present this credential to a potential employer (Verifier), who can instantly and cryptographically verify its authenticity without having to contact the university directly.

SSI systems can be through of as a technology stack, with each layer providing specific functionalities and privacy features:

1. **Infrastructure Layer:** This is the foundation that provides a mechanism for decentralized public key infrastructure (DPKI). While blockchains (public or private) are common, web-based infrastructures are also viable. This layer ensures data integrity and availability.
2. **Identifiers & Cryptographic Material Layer:** This layer deals with Decentralized Identifiers (DIDs), a new type of globally unique identifier standardized by the W3C. DIDs allow individuals to be identified without relying on a central registry. This layer supports pseudonymity and ensures that identifiers used in different contexts cannot be correlated.
3. **Credentials & Presentations Layer:** This layer manages Verifiable Credentials (VCs) and Verifiable Presentations (VPs). VCs are claims containing attributes about a holder, created and signed by an issuer. Technologies like Zero-Knowledge Proofs (ZKP) and Selective Disclosure are crucial here, allowing a holder to prove something (e.g., that they are over 18) without revealing the underlying data (their exact date of birth).

4. **Wallet Layer (Application Layer):** The SSI wallet is the primary user interface. It allows the holder to store and manage their DIDs and VCs, and interact securely with issuers and verifiers. Wallets typically consist of an **Edge Agent** (on the user's device) and a **Cloud Agent** (for mediation and recovery). Communication between wallets is often handled by protocols like DIDComm, which provides secure messaging, and DID-Auth which ensures DID authentication to establish authenticated communication channels.

A Practical Use Case: Managing Patient Consent in Healthcare

As part of the France 2030 PEPR Santé Numérique - TracIA project, we propose an identity and consent management layer based on SSI, Blockchain and Dynamic Consent.
TracIA (Traceability for trusted multi-scale data and fight against information leak in artificial intelligence systems in healthcare) aims to solve traceability challenges in e-health like **data provenance, trustworthy and secure deployment of AI** and **patient-centric consent management** at the scale of a national learning medical information system (LMIS). The fixed objectives are timely data governance and patient consent management, fine grained data provenance and combating information leakage. These goals will provide the building blocks needed to develop reliable AI-based systems in healthcare, while preserving patient privacy and the security of their health data. Our work in this project focuses on patient-centric identity and consent management.
In healthcare, patient data is often fragmented across different Hospital Information Systems, making it difficult to consistently manage identity and consent for research. ClinConNet **(Clinical Consent Network)** proposes a solution where:

- **Patients (Participants)** use SSI wallets to control their identity and manage consent for clinical trials in a granular and dynamic way.
- **Research Organizations** can efficiently and securely request and verify patient consent.
- A **Consortium Blockchain** is used to record immutable proofs of consent (hashes of consent forms, not the data itself), ensuring transparency and auditability, while maintaining patient privacy.
- A **Dynamic Consent Model** built with smart contracts to automate the consent management. It enables patients to manage their consent directly.

This SSI-based approach ensures that a patient's participation in different research projects cannot be linked, protecting their privacy. The consent is managed through smart contracts, giving patients true ownership and control over their consent data. Performance tests on the prototype show that the PoC is efficient, making it a viable solution for real-world deployment.

In summary, Self-Sovereign Identity is more than a new technology; it is a new philosophy for digital interaction built on the principles of privacy, security, and user control. By decentralizing trust and empowering individuals to manage their own credentials, SSI has the potential to revolutionize the way we interact online, from accessing government services and conducting business to managing our personal health data. While interoperability and adoption challenges remain, the path to a more secure and equitable digital identity framework is becoming clearer.

This work benefited from State aid managed by the Agence Nationale de la Recherche under the France 2030 programme, reference ANR-22-PESN-0006, project TRACIA.

For further information, refer to: https://pepr-santenum.fr/2023/11/08/tracia/

The EUDI Wallet for Data Spaces

Author: Van Hoan HOANG, Atos Eviden

This contribution presents an overview of the evolution of digital identity in Europe, the impact of eIDAS v2, and how the EUDI Wallet can reinforce trust inside dataspaces. It also provides details on Eviden's SSI solution and our active work in the APTITUDE consortium.

1. From eIDAS v1 to eIDAS v2

The first version of eIDAS, introduced in 2016, established a legal framework for electronic identification and trust services in Europe. It allowed citizens to use their national eID to access public services across borders and created several trust services such as electronic signatures, seals, timestamps and eDelivery. However, eIDAS v1 faced several practical limitations. Member States implemented their systems differently, which made interoperability difficult. The adoption rate stayed low, especially in the private sector. Many services were not designed for mobile use, which became a barrier to user adoption.
With eIDAS v2 (in force since May 2024), the EU took a major step forward by introducing the E**uropean Digital Identity Wallet (EUDI Wallet)**. Every Member State must provide an official wallet before the end of 2026. eIDAS v2 also brings new qualified trust services, such as electronic archiving, remote-qualified signature devices, electronic registries and qualified attestations of attributes. This new version aims to create a unified, mobile-first identity layer that works across the whole European digital market.

2. The Role of eIDAS in Dataspaces

Dataspaces aim to enable secure, sovereign and interoperable data sharing between organizations. To make this work at scale, they need reliable mechanisms to identify participants, control access to datasets, sign or seal data transactions, and maintain auditable records of what happened.
eIDAS v2 provides exactly the kind of legally recognized trust services that dataspaces have been missing.

- **EUDI Wallet** brings a harmonized way to authenticate users and organizations, using verified attributes rather than simple usernames or self-declared information.
- **Electronic Attestation of Attributes (EAA / QEAA)** can be used to express roles, permissions or domain-specific rights, which fits naturally with attribute-based access control in dataspaces.

- **Qualified signatures** and seals give legal validity to transactions and agreements exchanged inside the dataspace.
- **Qualified Registered Delivery** allows secure, integrity-protected and legally-provable communication between participants.
- **Qualified Web Authentication Certificates** strengthen the identity of connectors, APIs or endpoints that exchange data.
- **Qualified timestamps and ledgers** support traceability, compliance and safe audit.

Because these services come with legal recognition at the EU level, they allow dataspaces to scale beyond pilots and local ecosystems. They give all participants a common baseline of trust, regardless of sector or country, making eIDAS v2 a natural foundation for Gaia-X and other European data-sharing initiatives.

3. The EUDI Wallet Ecosystem

The Wallet ecosystem is based on a clear distribution of responsibilities:

- **Authentic Sources** such as civil registries, diploma authorities and tax agencies.
- **Issuers** that create PID, qualified attestations of attributes or domain-specific credentials.
- **Wallet Providers** responsible for delivering the official national wallet application.
- **Relying Parties** that consume credentials in real use cases (banks, public services, travel companies, etc.).
- **Qualified Trust Service Providers** and **Certification Authorities** who secure keys, certificates and trust anchors.

The ecosystem is supported by a large set of technical standards, mainly from ETSI and CEN/CENELEC, defining how keys, credentials, certificates and interactions must be handled. This ensures interoperability of wallet solutions across all Member States.

4. Eviden Solution

Eviden has developed a complete Self-Sovereign Identity (SSI) platform that meets the requirements of eIDAS v2 and integrates smoothly with the EUDI Wallet. The platform is designed for real organizations that need flexibility, strong security and compliance.

Issuer Side

The issuer platform supports multi-tenancy, allowing several organizations to operate on the same infrastructure while keeping data and configurations separated. Keys can be generated and managed

either with standard HSMs or with qualified HSMs such as Trustway, depending on the required assurance level.

The platform manages DIDs, certificates, schemas and credential formats, and exposes standard issuance APIs such as OpenID4VCI. It also includes a lifecycle component for revocation, status lists and credential updates.

Verifier Side

On the verifier side, the platform also supports multi-tenancy. It includes a trust anchor management system, enabling organizations to define which issuers they trust and under what conditions. The policy registry allows each verifier to define the exact requirements for accepting credentials: mandatory attributes, acceptable formats, validation rules, etc.

The verification engine supports DCQL, DIF Presentation Exchange, OpenID4VP and other modern protocols. Relying parties can integrate either through simple webhooks or no-code connectors, depending on their needs.

Why this matters for dataspaces

With this modular architecture, organizations can issue and verify credentials in a fully controlled way, using their own policies, HSMs and identity systems. This aligns perfectly with dataspace requirements, where each participant must remain sovereign over their identity infrastructure while still interoperating with others through shared standards.

5. Contribution to the APTITUDE Consortium

APTITUDE is one of the major European pilot programs for testing EUDI Wallet interactions in real life. With over 115 partners, the project covers several domains: Digital Travel Credentials, ticketing and check-in, mobile driving licence and strong customer authentication.

Atos/Eviden is the **technology provider for the Tickets & Check-in use case,** where we test the practical integration of the wallet for travel and mobility scenarios.

The project helps identify usability issues, interoperability gaps, performance constraints and potential regulatory problems. The lessons learned feed back into the European standardization work and help ensure that the global ecosystem will be ready for large-scale adoption.

Gaining a better understanding of the Digital Identity Portfolio ecosystem

Author: Romain Santini & Valérie Bruna – Docaposte

The aim of the presentation was to show the link between the concepts used in GAIA-X (such as Verifiable Credentials) and European regulations on the Digital Identity Wallet, which are based on the same principles of decentralized digital certificates and decentralized identification/authentication. The aim was also to discuss the work being done at European level on this Digital Identity Wallet, with a focus on how Docaposte is participating in this work.

Reminder of European regulations, in particular Regulation N°. 2024/1183 on the European Digital Identity Framework (known as "eIDAS 2"). The main features and requirements of the European digital identity wallet, created by this regulation:

- **Securely proving personal or professional identity** for citizens, residents, administrations, and businesses.
- **Sharing "electronic attribute statements"** with probative value (proof of income, qualifications, driving license, connection to an organization, etc.).
- **Produce electronic signatures or stamps** with a high level of legal certainty.

This wallet will be:

- **Usable online and in the physical world.**
- **Designed to respect privacy.**
- **Deployed at the national level, but recognized throughout the European Union.**

The key regulatory deadlines and those for large-scale European projects co-financed by the European Commission were presented, in particular regarding the provision of wallets by states, which is mandatory by December 24, 2026, and the fact that regulated entities[1] must accept wallets by December 24, 2027. With regard to European projects, the POTENTIAL project was completed at the end of December 2025, while the WEBUILD (focused on professional use cases) and APTITUDE (focused on individual use cases) projects began between September and October 2025 and are scheduled for completion on September 1, 2027.

1 All public services that require user identification, all companies (except micro-enterprises and small businesses) that require strong authentication, and very large online platforms as defined by the Digital Services Act (DSA).

The link between the European eIDAS 2.0 regulation, the associated implementing acts, the standards cited therein, and the reference architecture framework:

The European regulation and implementing acts establish the legal framework and the fundamental functional and security requirements. The technical standards, when referenced in one of the implementing acts, specify the methods for complying with these requirements. The reference architecture framework does not have any clear legal value, but it is the most up-to-date document reflecting the vision of the European Commission and the Member States.

Reminder of existing implementing acts, in particular Regulation 2024/2977, which introduces the PID and portfolio certificates, Regulation 2024/2979, which specifies the core functionalities of the portfolio, and Regulation 2024/2982 on portfolio protocols and interfaces.

The reference architecture framework defines the functional architecture of the portfolio, fundamental principles, components, interfaces, protocols, and obligations of stakeholders.

The Wallet ecosystem corresponds in particular to the authentic sources used to verify the data contained in qualified electronic certificates, as well as to certificate issuance services (communicating with any wallet via standard protocols), which may be subject to qualification by the State..

The Wallet also includes a signing capability that can rely on remote qualified electronic signature services.

In addition, user parties rely on verification components that communicate with any wallet using standard protocols to retrieve and verify the validity of certificates in real time.

These services rely on trust lists and registries to validate data, and archiving services to store evidence related to wallet usage over time.

European projects on wallet-related topics:

POTENTIAL: "PilOTs for EuropeaN digiTal Identity wALlet"

Running from May 2023 to September 2025.

Led by the Agence Nationale des Titres Sécurisés (FR)

- 20 countries, 69 beneficiaries and their affiliates, 37 associated partners.
- Focus on six use cases: government services, opening a bank account, registering a SIM card, driver's license, electronic signature, prescriptions.

APTITUDE: Advanced Project for Trusted Identity Technologies and Unified Digital Ecosystem.

Led by the Agence Nationale des Titres Sécurisés (FR).

15 countries, 76 beneficiaries, 42 associated partners.

Focus on uses by individuals and government portfolios (travel, vehicle registration, payment).

WEBUILD: Wallet Ecosystem for Business & Payment Use Cases, Identification, Legal Person Representation, and Data Sharing.

Led by chambers of commerce/business registers (NL/SE). 26 countries, 94 beneficiaries, 87 associated partners.

Focus on uses by legal entities and organizational wallets (supplier knowledge, tax returns, electronic invoicing, payments, etc.).

Numerous interoperability events are being organized, as they are necessary for the joint development of the community of wallet providers and user parties.

Finally, the authors presented the Docaposte issuer/verifier demonstrator available on the ANTS "playground" website and accessible to the public (on-the-fly account creation without sending an email).

This solution was designed specifically for interoperability testing and therefore includes the technical settings necessary for developers to perform these tests.

https://api.playground.france-identite.gouv.fr/docaposte/keycloak/

This solution allows you to:

Issue and verify certificates already built according to Potential specifications (Person Identification Data: ID, IBAN, driver's license, etc.)

Build your own certificate issuance/verification templates and test them: please note that some wallets restrict certificate verification to certificates they recognize with a specific structure

A guide detailing its use can be downloaded from the help tab on the website.

gaia-x
Hub France

Live Identity Wallet

Author: Bruno Salinier, Orange Business

This presentation aims to demonstrate how wallets can be used in various use cases currently being deployed in projects in which Orange Business is involved.

Orange Business Solutions for Data Spaces

For several years, Orange Business has been involved in various European services and initiatives focused on data sharing, particularly data spaces. As a founding member of Gaia-X and a member of the Association for Data Intermediation (AID), we are actively involved in this ecosystem and offer a range of trusted products and services that comply with European regulations to manage various aspects such as cloud services, networks, identity and participant enrollment, consent management, and data space connectors. One example is agdatahub in the field of agriculture, the first data intermediation service based on the principles of decentralized identity, providing in particular a smartphone-based farm wallet that allows users to:

- easily create the identity of the farmer (natural person) and their farm (legal entity) based on trusted sources (France Connect and the National Business Register);
- grant consent for the sharing of data owned by the farmer.

Orange Business is also contributing its tools and expertise to other European data exchange projects such as DOME (distributed marketplace for trusted services), TEMS (data space for media), and CEADS (data space for agriculture), with additional management of rules and constraints and a Gaia-X Digital Clearing House instance.

Decentralized identity with Live Identity Wallet

Live Identity Wallet is a SaaS wallet service for legal entities or objects (Holders), providing the following features:

- secure storage of verifiable credentials (VC) from trusted sources;
- obtaining (through the Issuance mechanism) and providing (Presentation) credentials;
- issuing verifiable credentials (Issuer) on behalf of its owner (Holder)
- exchanging "business" messages between wallets;
- all while relying on a Trust Framework to ensure the authenticity of the ecosystem's actors and credentials.

Live Identity Wallet aims to support the main interoperability standards for decentralized identity, particularly for the Gaia-X ecosystems and the European identity wallet (ARF, eIDASv2).

Use cases

B2B networking

Orange Business is participating in the new European consortium WE BUILD, which aims to develop pilot use cases in the field of corporate wallets, with a business role in two use cases.

Onboarding new business customers

The main objective is to integrate new business customers within a legal and contractual framework. To do this, several essential pieces of information are collected during customer onboarding: the local wallet identifier (LPID), the company name, its address, its commercial register identification number, its VAT number (VATID), its legal representative, etc. This data is used to verify the company's identity and ensure its legal compliance.

Onboarding of authorized persons

In addition to information about the company itself, it is necessary to integrate the persons authorized to use the services. These persons have access to management and support tools related to the subscribed offer, such as cloud infrastructures, networks, or SaaS digital services. Their access must be reliably delegated, with a delegation of trust issued by the representative of the client company. Other customer contacts, such as stakeholders or billing contacts, are also registered to ensure comprehensive relationship management.

Vehicle health certificate

Orange Business is also working on the "object" wallet associated with each vehicle as it leaves the factory, accompanied by a tamper-proof register that enables the provision of several services such as:

- health record: administrative documents, maintenance history, information from real or virtual sensors
- access to the health record for third parties with the owner's consent
- wallet integrated into the mobile application provided by the manufacturer for differentiated services between owners and simple users, allowing transfer to the new owner
- automatic recognition of the driver when they get in the car, etc.

Conclusion

The Live Identity Wallet service aims to provide a comprehensive solution for managing corporate identity via digital wallets. It integrates onboarding, verification, secure data sharing, and access management processes, based on open standards and a decentralized architecture. This combination ensures trust, security, and interoperability in a European and industrial environment, facilitating identity verification and data sharing in a secure and compliant framework.

IN Groupe Wallet Solutions and Their Experimentation in Transport

Author: Vincent Desbiendras, IN Groupe

Overview

IN Groupe provides digital identity solutions for countries, ecosystems, and companies. We leverage digital wallets to improve citizens' and users' trust in their national identity, reduce costs, and simplify usage. We are also driving transformation in transport and logistics through digital identity wallets and secure authentication solutions, enabling faster and safer access to services and compliance processes.

Key Points

Objective: Modernize access to public and private services and strengthen identity verification in digital and physical contexts.

Solution:

- A digital wallet for secure authentication and consent-based data sharing.
- Features include online authentication via selfie, face-to-face verification, and selective attribute sharing.

Impact:

- Over **1 million Wallet IDs created in 2024.**
- Significant reduction in processing times for authorizations.
- Improved ability to fight document fraud.

International Use Cases

Colombia:

- Government partnership since 2020 to accelerate digital transformation using mobile identity wallets.
- Achievements: **1M mobile IDs issued in 2024; 3.2M since service launch.**

Chile:

- Deployment of a mobile identity wallet to enable secure access to public and private services.
- Achievements: **50K active wallets during the first pilot year.**

European Initiatives

IN Groupe actively participates in **Large Scale Pilots** (LSP) to shape the future of European digital identity:

- **Potential & Aptitude**: Focused on Digital Travel Credentials and interoperability testing.
- **WeBuild**: Experimenting with high-value use cases for transport, Know Your Business (KYB), and micro-credentials (professional experience and qualifications) before the 2026 launch.

Transport & Logistics Experimentation

- Since February 2025: **10,000+ wallets created.**
- Funded by **France 2030** program with ADEME and the Ministry of Transport.
- Goals:
  - Test initial use cases.
  - Gather user feedback.
  - Co-build future solutions.
- **Open to new companies until November 2026.**

Main Use Cases of Transport & Logistics Experimentation

- **Onboarding new partners:** Verify authenticity of transport company documents.
- **Single secure login:** QR code-based authentication for all business tools.
- **Physical site access:** Faster, safer entry using mobile wallet instead of paper documents.

Solution: My Hub Pro

- Modular platform for secure data exchange.
- Components:
  - **Hub Pro portal** as issuer of credentials.
  - **My Hub Pro** as mobile and web wallet.
  - **Hub Pro Connect** for secure authentication and offering an **OIDC bridge** to ease wallet usage by applications.
- Supports **EUDI Wallet**, attestations issuance, and verification**.**

gaia-x
Hub France

Gaia-X Hub France

The representative and contact point for Gaia-X in France.

www.gaia-x-hub.fr/