Dissemination level : Public

# EWC D3.4

ODI COUNTRY SCHEMES' DEFINITION, AND ORGANISATIONAL CREDENTIALS DEFINITION, SPECIFICATION, AND REGISTRATION ON INFRASTRUCTURE

WP3

Author: Archipels

Contributors: SCRO (Bolagsverket), Vero

Day of submission: 31/05/2025

# Contents








Co-funded by the European Union

Co-funded by the European Union

# Revisions

| Version | Date | Author | Changes |
|---|---|---|---|
| v0.1 | 2025-03-13 | Archipels | First version of the document with proposed structure and list of inputs |
| v.0.2 | 2025-03-27 | SCRO (Bolagsverket) | Wrote chapter 1.1 about business context and started on 1.2 legal context.<br><br>Inserted headers for chapter 4 (Risks and agps in LPID issuing process) and 5 (Annex) |
| v0.3 | 2025-04-01 | SCRO (Bolagsverket) | Wrote chapter 2.1 Group work with business registries and 2.2 Reuse of EU standards |
| v0.5 | 2025-04-04 | Vero | Wrote draft texts to chapters 1.4, 3.1 and 3.2 |
| v0.7 | 2025-04-08 | Archipels | 1.3, 1.4, 2.1, 3.3, 3.4, 5 |
| v0.8 | 2025-05-26 | SCRO (Bolagsverket) | Version presented in the Management Board |
| v0.9 | 2025-05-29 | SCRO (Bolagsverket) | Final version reviewed and agreed by contributors. Under review of Project Coordinators. |
| | | | |





Co-funded by the European Union

# Executive Summary

This deliverable outlines the results of Task 3.2 “PID/ODI and organisational credentials” and more specifically the subtasks T3.2.2 “Issuing of ODI attributes to the Legal Person (organisational) wallet”, T3.2.3 “Issuing of other organisational credentials not part of the attributes contained in ODI”, and T3.2.4 “Verification of other organisational credentials not part of the attributes contained in ODI”, focusing on the work done on Organisational Digital Identity (ODI), which was later changed to LPID (Legal Person Identification Data) and on organisational credentials – which in the context of this report are credentials concerning organisations issued by authentic sources. The report provides a comprehensive overview of the methodology, challenges, and lessons learned in establishing interoperable and legally reliable digital credentials for legal entities across EU Member States within the framework of eIDAS 2.0 and the European Digital Identity (EUDI) Wallet.

The report addresses the fragmented state of digital identity for organisations, noting the inefficiencies and risks stemming from siloed systems, manual processes, and a lack of interoperability. To counter these issues, the EWC pilot tested key use cases—including Public Procurement, KYC/KYS processes, and cross-border company branch creation—where official credentials such as the EU Company Certificate (EUCC), Ultimate Beneficial Ownership (UBO), Signatory Rights (SR), Power of Attorney (PoA), and IBAN were modelled and piloted.

A collaborative process involving national business registries (from Sweden, Norway, Finland, France, Germany, Netherlands, and Italy) established shared data schemas and rulebooks. These were based on existing EU semantic standards (ISA², SEMIC, BRIS, BORIS) and informed by legal frameworks including eIDAS, GDPR, AMLD, and PSD2. Despite progress, gaps in standardised definitions – particularly for SR and PoA – highlight the complexity of aligning national practices and legal interpretations.

The report emphasises the importance of semantic interoperability, recommending Linked Data principles and the adoption of a shared business vocabulary to ensure machine-readability and automation readiness in future implementations. It also explores the role of the Legal Person Wallet, which introduces specific needs around user management, access control, and credential lifecycle governance.

Finally, the report identifies several operational and legal risks related to LPID issuance, including authority verification, secure wallet binding, and lack of standardised trust mechanisms.

It also provides recommendations regarding the practical work with credentials including enhancing versioning practices, adopting modular schema design, and considering alternative tech stacks, such as W3C VCDM 2.0 and DID-based infrastructures.

This deliverable serves as both a blueprint and a status report, guiding future efforts within the WE BUILD Large Scale Pilot project starting on August 1st, 2025, and beyond to ensure robust, trustworthy, and interoperable organisational credentials across the European digital identity ecosystem.





Co-funded by the European Union

# List of abbreviations

| Acronym | Explanation |
|---|---|
| (Q)EAA | (Qualified) Electronic Attestation of Attributes |
| ACM | Access Control Mechanism |
| AML/CFT | Anti-Money Laundering / Combating Financing of Terrorism |
| AMLD | EU Anti-Money Laundering Directives |
| API | Application Programming Interface |
| ARF | Architecture and Reference Framework |
| B2B | Business-To-Business |
| B2G | Business-To-Government |
| BIDS | Business Information Data Space |
| BORIS | Beneficial Ownership Registers Interconnection System |
| BRIS | Business Register Interconnection System |
| CEO | Chief Executive Officer |
| CIR | Commission Implementing Regulation |
| DG DIGIT | Directorate-General for Digital Services |
| DID | Decentralized identifier |
| DIF | Decentralized Identity Foundation: DIF |
| DNS | Domain Name System |
| EAA | Non-Qualified Electronic Attestation of Attributes |
| EBRA | European Business Registry Association |
| EBSI | European Blockchain Service Infrastructure |
| EDIR | European Digital Identity Regulation |
| eID | electronic Identification |
| eIDAS | Electronic Identification, Authentication and trust Services |
| ENISA | European Union Agency for Cybersecurity |
| EU | European Union |
| EUCC | European Company Certificate |
| EUDI | European Digital Identity |
| EUDIW | European Digital Identity Wallet |





Co-funded by the European Union

| Acronym | Explanation |
|---|---|
| EUID | European Unique Identifier |
| F2F | Face-to-Face |
| FAQ | Frequently Asked Questions |
| GDPR | General Data Protection Regulation |
| IBAN | International Bank Account Number |
| ISA² | Interoperability solutions for public administrations, businesses and citizens |
| ISO | International Organisation for Standardisation |
| JOSE | JSON Object Signing and Encryption |
| JSON | JavaScript Object Notation |
| JSON-LD | JavaScript Object Notation – Linked Data |
| KYC | Know Your Customer |
| KYS | Know Your Supplier |
| LoA | Level of Assurance |
| LP | Legal Person |
| LPID | Legal Person Identification Data |
| LSP | Large Scale Pilot |
| M2M | Machine to Machine |
| NACE | Nomenclature of Economic Activities in the European Community |
| NFC | Near Field Communication |
| NIS2 | Network and Information Security Directive 2 |
| NP | Natural Person |
| NPID | Natural Person Identification Data |
| ODI | Organisational Digital Identity |
| OID | OpenID |
| OpenID4VP | OpenID for Verifiable Presentations |
| PID | Person Identification Data |
| PoA | Power of Attorney |
| PSD2 | Payment Services Directive 2 |
| Pub-EAA | Public Body Electronic Attestation of Attributes |





Co-funded by the European Union

| Acronym | Explanation |
|---|---|
| QC | Qualified Certificate |
| QES | Qualified Electronic Signatures |
| QSCD | Qualified Signature/Seal Creation Device |
| QTSP | Qualified Trust Service Provider |
| RFC | Request For Comments |
| SDGR | Single Digital Gateway Regulation |
| SD-JWT | Selective Disclosure for JWTs (JSON Web Tokens) |
| SEMIC | Semantic Interoperability Community |
| SME | Small and Medium Enterprise |
| SR | Signatory Rights |
| TSP | Trust Service Provider |
| UBL | Unified Business Language |
| UBO | Ultimate Beneficial Ownership |
| UN/CEFACT | United Nations Centre for Trade Facilitation and Electronic Business |
| VAT | Value Added Tax |
| VCDM | Verifiable Credentials Data Model |
| VDR | Verifiable Data Registry |
| W3C | World Wide Web Consortium |
| WACI | Wallet and Credential Interaction |
| WSCD | Wallet Secure Credential Device |
| WTO | World Trade Organisation |
| XML | eXtensible Markup Language |





Co-funded by the European Union

# 1. Context

## 1.1 Business context

### 1.1.1 Main challenges that the organisations face nowadays

Organisations today face multiple challenges when proving their identity or authority in digital processes. One significant issue is fragmented digital identities, where organisations must manage multiple separate digital identities across different systems and jurisdictions, causing complexity, redundancy, and administrative overhead. This fragmentation is further complicated by a lack of interoperability, as credentials issued in one context or jurisdiction are often not accepted elsewhere, creating barriers in cross-border business and regulatory interactions.

Manual verification and continued reliance on physical paperwork remain prevalent, contributing to delays, higher administrative burdens, and a heightened risk of errors and fraud. Additionally, organisations often struggle to digitally verify representation rights and mandates, particularly in cross-border or delegated-authority contexts, causing uncertainty in transactions and operational decisions.

Organisations also face considerable compliance and regulatory complexity, particularly when navigating varying trust frameworks across sectors and countries. This complexity makes adherence to regulatory requirements challenging and resource intensive. Traditional methods of proving identity, often relying on paper or unstructured digital communication, further expose organisations to fraud and identity theft risks, undermining security and trust.

Onboarding processes for partners, customers, and suppliers can become slow and expensive due to a lack of trusted digital credentials, negatively affecting efficiency and operational agility. Sharing sensitive organisational information through insecure or non-standardised digital channels additionally raises serious privacy and cybersecurity concerns. Finally, inconsistent international recognition of organisational credentials reduces trust in digital cross-border transactions, limiting opportunities for seamless global business interactions.

Addressing these challenges requires reliable, interoperable, and secure digital organisational credentials, enabling trusted digital interactions, streamlining regulatory compliance, and facilitating smoother cross-border operations.

However, the assumption that organisational credentials will help this complexity relies on widespread interoperability and acceptance of these credentials.

### 1.1.2 Purpose, need and use-cases for organisational credentials

Organisational credentials are expected to be needed in many different business contexts. The definition of organisational credentials is broad, but in the EWC Large Scale Pilot project, only those issued by an official authentic source are being considered for piloting.

The business scenarios piloted where organisational credentials are tested include Public Procurement with organisational credentials tested in B2G interactions between companies and tendering systems or other government services, interactions with banks as part of the Know Your Customer (KYC) use cases, for the Know Your Supplier (KYS) use case the organisational credentials are tested in B2B interactions between small and medium





Co-funded by the European Union

companies. These credentials are used during Strong Customer Authentication (SCA) and to enable subsequent processes, such as opening a bank account.

Another use case piloted is "Create a branch (in another country)," where organisational credentials are issued to a parent company by a business register in country A. These credentials are then presented to a business register in country B to establish a branch of the parent company.

Details of the business scenario pilots, and the specific use of organisational credentials are provided in deliverables D3.5 “Business scenarios pilot plans” submitted in M12 of the project and D3.6 “Business scenarios pilot results and evaluation” to be submitted at the end of the project.

The purpose and need for organisational credentials can be summarised in four main areas:

1. establishing trust,
2. enabling due diligence, and
3. facilitating business transactions
4. reducing regulatory burden

**Examples in B2B for establishing trust**

In supplier-buyer relationships, companies use organisational credentials – such as the Legal Person Identifier Data (LPID) – to authenticate each other and confirm the legal existence of the company. This is used to establish trust prior to engaging in business activities.

When signing business contracts, businesses can verify who within the company is authorised to sign contracts or make decisions.

For easy cross-border recognition, verifiable credentials issued by a national business register are used to authenticate a company in another jurisdiction.

**Examples in B2B for due diligence**

Organisational credentials also support due diligence processes by providing verifiable information.

Proof of company registration: Credentials showing registration status, registration date, and jurisdiction.

- Tax information: Verified VAT number for tax compliance checks.
- Banking information: Verified IBAN credential to confirm account ownership.
- Ultimate Beneficial Owners (UBO) declaration: Information about the Ultimate Beneficial Owners for anti-money laundering (AML) compliance.
- Compliance certifications: Credentials showing that a company meets certain regulatory or industry-specific standards (e.g. ISO certifications).

**Examples in B2B for conducting business**

- Public Procurement: Use of organisational credentials to log in to procurement platforms and submit bids or tenders.
- Supply chain onboarding: Faster onboarding of suppliers through verifiable proof of identity and qualifications.
- Delegation of authority: A company issues credentials to an employee to act on its behalf in digital transactions (e.g., submitting tenders, signing documents).





Co-funded by the European Union

- Contractual processes: Digital signing of contracts where both parties present verifiable organisational credentials to confirm roles and authorisations.

**Examples in B2G for reducing regulatory burden**

Businesses provide verifiable credentials (e.g., proof of registration, legal form, authorised representative) when registering a new company or applying for licenses.

Companies use organisational credentials as a part of the process of authentication and reporting tax data (e.g. VAT number, legal entity identity) to tax authorities.

Companies apply for public funding by presenting credentials that prove eligibility, such as SME status, registration date, or sector classification (e.g., NACE code).

Organisational credentials are used in procurement and public tenders to authenticate suppliers and verify documents like proof of legal existence, authorised signatories, and financial standing.

In cross-border notification, a business from one Member State uses credentials issued by its national authorities to notify another Member State of intended cross-border service provision.

In regulatory reporting (e.g., for environmental compliance, transport, energy, financial supervision), credentials are used to identify the reporting entity and the authorised individual submitting data.

In summary there are many potential use cases for organisational credentials. To show their value, it is encouraged to measure the potential savings in time and resources by organisational credentials, as well as the security benefits they provide. This can be put against the overhead needed to implement and accept organisational credentials to show their value to the ecosystem.

## 1.2 Legal context

### 1.2.1 Relevant laws and regulations

Identifying relevant laws for organisational credentials is challenging due to significant variations across sectors, countries, and specific use cases. Although overarching European regulations such as eIDAS, GDPR, and AML/CFT provide a common foundation, additional sector-specific laws often apply depending on the industry context. For example, credentials used in financial services must comply with PSD2 requirements, while those in the healthcare sector are governed by health-related privacy and patient data protection laws. Similarly, credentials related to energy or telecommunications must align with sector-specific regulatory frameworks. To fully understand the relevant laws, it is essential to carefully consider the specific business context, jurisdiction, and use case for each credential.

Non-exhaustive lists of laws and regulations relevant to organisational credentials:

- eIDAS Regulation (No 910/2014) (including eIDAS 2.0 EU 2024/1183) defines legal requirements for creating, issuing, and recognising organisational credentials across EU Member States.
- GDPR (General Data Protection Regulation EU 2016/679) governs how personal data within organisational credentials can be processed, ensuring data privacy compliance.
- AML/CFT package (Regulation 2024/1624 and Directive 2024/1640 on Anti-Money Laundering / Combating Financing of Terrorism) set the standards for credentials used





Co-funded by the European Union

in verifying organisational identities during mandatory due diligence processes such as KYC/KYS.

- PSD2 (EU 2015/2366 Payment Services Directive 2) establishes requirements for organisational credentials used in strong customer authentication (SCA) for financial services.
- NIS2 Directive (EU 2022/2555 Network and Information Security Directive 2) sets security obligations to protect organisational credentials from cyber threats.
- SDGR (EU 2018/1724 Single Digital Gateway Regulation) relies on organisational credentials to enable trusted digital interactions in cross-border administrative procedures.
- Company Law Directives (Directive 2017/1132, BRIS Directive 2012/17/EU) provide a legal basis for credentials related to company registration, representation rights, and cross-border operations as well as its amendment 2025/25 amending Directives 2009/102/EC and (EU) 2017/1132 as regards further expanding and upgrading the use of digital tools and processes in company law.
- Directive on Services in the Internal Market (2006/123/EC) supports cross-border recognition of organisational credentials for service providers operating across EU Member States.

### 1.2.2 Enabling conditions for legal recognition of organisational credentials

There are general conditions which should be met for organisational credentials to be legally recognised and trusted. Those conditions might need to be more defined regarding Electronic Attestation of Attributes (EAAs) issued by organisations themselves. This is not to be read as a list of requirements, rather as conditions which need to be looked into to facilitate an uptake and trust in organisational credentials. Even this list is non-exhaustive.

Security and compliance

- Certain assurance levels should be required for organisational credentials that could have significant consequences if misused (such as mandates). Analysis of existing security and risk assessment frameworks should be made in order to formulate requirements. The other way around, for organisational credentials that lack any consequences if misused, the assurance levels could be adapted as well to make administration easier.
- Processing and storage of credential data must align with GDPR or other applicable data protection regulations.
- Credentials must be securely protected against modification, tampering, or fraud.

Governance policies

- Credentials issued by an authentic source have trust anchors which follow from the eIDAS implementing regulations, but credentials issued by businesses should also have a trust anchor. Trust could be established in several ways, e.g. through cryptographic verification anchored in recognised infrastructures or indirectly (e.g. by linking/chaining) the credential to other trusted organisational credentials, typically those issued by authentic sources.
- The same revocation requirements as described in implementation acts should apply for credentials issued by organisations and which require a certain assurance level, as those issued by authentic sources. Rulebooks could define when revocation is needed.





Co-funded by the European Union

- Liability needs to be defined in case of wrongly issued or wrongly constructed organisational credentials. Scopes for roles and responsibilities in credential issuance and usage need to be defined.

Standards

- Credentials must comply with relevant regulatory standards, such as those defined in eIDAS, ensuring technical interoperability and trust.

Verifiability and Validity

- Credentials should be verifiable through cryptographic or other trusted mechanisms to ensure authenticity and integrity.
- Credentials must clearly state their validity timeframe and expiration conditions.
- Credentials regarding mandates.
- Credentials which convey representation, delegation or any authorisation mandate shall explicitly specify the scope of authority granted, such as roles, mandates, or representation rights.
- Clearly established trust mechanisms shall be applicable for such types of credentials for verification and validation.

Semantic Interoperability

- Attributes within organisational credentials must have clearly defined and harmonised meanings, enabling consistent understanding and processing across jurisdictions and sectors.
- Existing vocabularies should be reused whenever possible, e.g. EU Core Vocabularies (interoperable-europe.ec.europa.eu/collection/semic-support-centre/core-vocabularies).

Liability

- There is also an absence of discussion on risks, e.g. what happens if an organisational credential is misused, revoked, or contested across jurisdictions. These are gaps that need to be analysed further to facilitate acceptance of organisational credentials

In summary, all these conditions mentioned above could enable the legally compliant use of organisational credentials. It is also acknowledged that a lot of legal coordination still needs to be done to reach this goal.

## 1.3 Interoperability context

In the digital identity ecosystem, the significance of technical interoperability is well-recognized. It encompasses the ability of digital wallets to exchange data securely and reliably across platforms. However, once such communication channels are established, an equally critical requirement emerges: the need for semantic and procedural alignment between wallet holders, issuers and relying systems. Only through such alignment can digital identities be effectively employed within operational business processes.

To address this necessity, the credential issuance and verification tasks within the EWC has undertaken efforts to develop a standardized framework. This includes the definition of shared rules and harmonized data schemas for a predefined set of attestation types, facilitating mutual understanding and validation across diverse systems. These specifications are essential to ensure that issued credentials are not only technically transferable but also contextually interpretable and verifiable by all participating entities.





Co-funded by the European Union

## 1.4 EWC context

In the context of EWC, the first goal of sub-tasks T3.2.3 “Issuing of other organisational credentials not part of the attributes contained in ODI”, and T3.2.4 “Verification of other organisational credentials not part of the attributes contained in ODI”, was to provide to the Business scenarios pilots (task T3.3 “Business scenarios piloting”) the necessary attestations to run their pilots. From the outset, this work was constrained by tight timelines, which posed a significant challenge given the inherent complexity of defining organisational credentials. The development of such credentials requires careful deliberation, ideally in close coordination with relevant European institutions that have previously engaged in the standardization and specification of related data structures. As such, the time-bound nature of this effort limited the extent to which broader consultation and alignment could be fully achieved in the initial phase.

Since the actual content of the organisational credentials piloted in the EWC (EU Company Certificate (EUCC), Ultimate Beneficial Ownership (UBO), Signatory Rights (SR) and Power of Attorney (PoA)) was not defined in any published common data model or schema, the participants in the relevant EWC work stream decided to use some sort of common data model as a basis for these attribute attestations.

The present and future implementation of the data models of these attestations is a Member State responsibility and each registration authority has had to implement both a BRIS (contains EUCC and SR data) and BORIS (contains UBO data) API. Therefore, the development of common data models for the credential schemas should be an undertaking where the national competent authorities agree on a common model that can be fitted to the data models of the national registers.

As a basis for this common model, the EWC participants chose the EU Core Vocabularies published by the SEMIC Team of DG DIGIT. Particularly in the Nordic countries, lots of effort was put on the creation of a common Nordic data model (vocabulary) that would be used when creating the attribute attestation specific common data models.

Unfortunately, due to the fact that the key attestation developed for natural person (PID – Person Identification Data) and the one for legal person (LPID – Legal Person Identification Data) which followed – have been developed without any consideration to actual data modelling and the attributes in the credential schemas are simply presented as attribute labels with a short attribute specific description, the approach to introduce a common semantic foundation for organisational credentials could not be achieved during the EWC LSP.

Also, it was clear from the start of the EWC LSP that a Large-Scale Pilot project is not in the position to impose any permanent structures or methodology for the actual description of the content of each attribute attestation, since this part has generally been neglected in the eIDAS 2.0 regulation, the Implementing Act drafts and the Architecture and Reference Framework (ARF). The Implementing Acts reflect the attitude that, especially for natural persons, each attribute attestation is actually simply a list of individual attributes that are somehow defined separately, not having any links to any underlying data models or vocabularies.





Co-funded by the European Union

# 2. Methodology

## 2.1 Identification of the organisational credentials needed by EWC

As a preliminary step before the commencement of tasks related to credential definition, it was essential to identify the specific priorities and requirements of the pilot implementations. To this end, all business scenario and use case leads were systematically surveyed in order to determine which organisational credentials would need to be exchanged by Legal Person Wallets within the context of their respective pilots. The resulting list of organisational credentials, as detailed in this deliverable, was derived from this needs-assessment phase.

A key insight emerged during this process: the majority of required attestations are expected to be issued by national or regional Business Registries. Consequently, a critical dependency was identified – namely, the necessity for close collaboration with the Business Registries engaged in the EWC project. Their involvement was indispensable to ensure the credibility, accuracy, and interoperability of the organisational credentials envisaged for cross-border and cross-sector use within the European digital identity ecosystem.

## 2.2 Working with the Business Registries

At the start of the project, a two-day workshop was held with all business registries which participated in EWC. Present were representatives from Norway, Sweden, Germany, France, the Netherlands, Italy, Finland and Denmark (Denmark later left the pilot).

The objective was to clarify the expected deliverables and to establish a common understanding of relevant terminology, such as the initial term "ODI" (Organisational Digital Identity), which was later changed to "LPID" (Legal Person Identification Data). During the workshop, business registries discussed their interpretations of the LPID issuance process and the related attributes. The group documented a shared understanding of the necessary controls in the LPID issuance process, the agreed-upon attributes of the LPID, and the rationale behind selecting specific attributes – for example, the arguments for the use of EUID (European Unique Identifier) as an organisational credential against other possible organisational identifiers.

Following the initial workshop, the participating business registries convened approximately every two months online throughout the pilot. These meetings served as checkpoints to discuss progress, review the status of deliverables, and, in the later stages of the pilot, to demonstrate completed work and achieved outcomes.

A two-day joint workshop on organisational credentials was held in Paris with representatives from the business registries of Norway, Sweden, Germany, France, Finland, and the Netherlands. The purpose of the workshop was to reach a common understanding and agreement on the attributes to be included in the EU Company Certificate (EUCC), a Signatory Rights attestation, and the Ultimate Beneficial Owner (UBO) attestation. In preparation for the workshop, each participating registry had mapped a proposed list of attributes to the corresponding attribute names used in their national registers, providing a basis for comparison and alignment. Following the workshop, each participating country developed and refined data schemas for the agreed attestations, based on the joint work carried out during the session. These schemas served as common reference examples for use in the pilot implementation.

For the IBAN attestation, which is the only organisational credential issued by banks or open banking aggregators, a first online discussion was held by Archipels with Tink to define the





Co-funded by the European Union

scope, the rules and main attributes of the schema. After documentation work about the PSD2 and ISO standards, a data schema and a rulebook were proposed. Then a validation meeting was held with the experts of the payment use case (Tink, Visa, Wordline), and the material was slightly updated after that meeting.

## 2.3 Reuse of existing European models

The semantic working group in the EWC pilot took inspiration from the European ISA² Core Business Vocabulary. Developed under the European Commission's ISA² programme, this vocabulary aims to promote semantic interoperability across public administrations in the European Union (EU). It offers a simplified, reusable, and extensible data model that captures key characteristics of a legal entity, such as its identifier and business activities. For foundational business attributes – such as those included in the LPID and EUCC – the working group referred to ISA² examples like "`legalName`" and "`legal_identifier`." The vocabulary was then adjusted to align with the terminology used in eIDAS 2.0, which refers to the concept of a "legal person." As a result, the attribute names in EWC were adapted to reflect this, becoming "`legal_person_name`" and "`legal_person_id`," respectively.

The working group took a short time to compare to the SEMIC vocabulary as well, which was quite similar ("legalName" and "legalIdentifier"), but decided to retain the decided-upon attributes.

The Company Law Directive (Directive (EU) 2017/1132), as amended, aims to harmonise certain aspects of company law across EU Member States, including the standardisation of key cross-border attestations such as the EU Company Certificate (EUCC) and the EU Power of Attorney (EU PoA). The objective is to ensure that company-related information and authorisations can be recognised and trusted across borders without the need for additional national procedures. In addition, these attestations are expected to be compatible with the European Digital Identity Wallet (EUDIW), which the EWC pilot has tested. For the EUCC and the EU PoA, the group aligned its work with the ongoing standardisation discussions within EBRA (European Business Registry Association). While the EUCC was already well-defined by early 2024, work on the EU PoA had not yet begun. As a result, progress on the EUCC schema was quicker. The European Commission had already provided a list of attributes along with brief explanations, which gave the working group a clear starting point. Their task was limited to mapping these attributes to those in their national registers, defining the relevant value sets for the pilot, and agreeing on attribute names and the overall schema structure.

For the EU PoA, the group initially awaited further guidance from the European Commission regarding the scope and definition of the relevant attributes. It was only towards the end of 2024 that the semantic group received more detailed input, which enabled them to begin developing their own preliminary information model suitable for pilot purposes. At the time of writing, the PoA model is not yet finalised and will likely need to be further developed in the next phase of the WE BUILD LSP project. The working group also reviewed the EU Powers and Mandate Ontology in an effort to align with existing semantic frameworks. However, they concluded that the ontology was too comprehensive and detailed for the scope and practical needs of the pilot and therefore opted not to adopt it. A version of the PoA was used for the pilots as it will be presented in deliverable D3.6.

For the UBO attestation, the working group drew inspiration from the Beneficial Ownership Registers Interconnection System (BORIS) data schema, aiming to reuse its structure where possible. However, the schema was adapted to fit the scope of the pilot, with only a selected subset of attributes included in the final data model.





Co-funded by the European Union

Some elements were also drawn from the Business Register Interconnection System (BRIS) data schema for information exchange. For example, the organisation status values defined in BRIS were proposed for reuse and mapped in a similar way within the EUCC attestation.

Overall, the reuse of previous EU-level semantic projects – including the ISA² Core Vocabularies, SEMIC, the BRIS and BORIS data schemas, and the standardisation efforts under the Company Law Directive – provided a solid foundation for the semantic working group in EWC. This reduced the need to start from scratch and helped save time in developing consistent and interoperable data schemas for the pilot.

# 3. Remarks / Findings / Issues

## 3.1 Difficulties regarding Signatory Rights and Power of Attorney

Several challenges and interpretation discrepancies emerged while defining attributes related to Signatory Rights (SR) and Powers of Attorney (PoA). Specifically, inconsistencies were identified between the information required to document SR and PoA, and the data actually recorded in official registries or Chambers of Commerce.

Additionally, significant differences exist across member states regarding the content and format of records for SR and PoA. A further major challenge is the frequent presence of special signatory conditions and restrictions associated with both SR and PoA, such as limitations on financial transactions, permitted activities, and geographical boundaries. Unfortunately, these rules and restrictions are often stored in registries as unstructured, free-text entries rather than structured database entries.

Another complexity arose around terminology and classification. There is often ambiguity in naming these authorisations – terms like signatory rights, delegations, powers of attorney, mandates, and other variants may be used interchangeably, prompting fundamental questions about what constitutes a legal representative. Consequently, extensive discussions were required to clarify the distinct legal meanings and implications of SR, PoA, mandates, and delegations.

Many of these issues were addressed either through direct resolution or simplification – for example, by avoiding overly complex joint signatory rules and opting instead for authorisation by a single individual.

Ultimately, the resolution involved a two-pronged approach:

1. Viewing the issue from the standpoint of a relying party, considering precisely what information is necessary to establish the legal authority of an individual acting on behalf of an organisation.
2. Developing a comprehensive model capable of accommodating various forms of authorisation. This model allowed specific elements to be selected, clearly defining the minimum required attributes for SR and PoA.

Considering these factors, we arrived at a simplified yet effective definition of credentials for SR and PoA. These streamlined credentials were successfully implemented in pilot phases, serving as a foundational step toward more comprehensive credentials planned for future implementation.





Co-funded by the European Union

## 3.2 Securing the semantic interoperability of attestations

As described previously, the issue of semantic interoperability has hardly been considered at all in the context of the eIDAS 2.0 regulation and digital wallets. EUDI Wallets are mainly seen as authentication tools for natural persons, whereupon the issues of privacy preserving and data security has been the main driver for the technical development. This can be seen in the promotion of Selective Disclosure techniques where an individual can be given the capabilities of choosing what data to disclose to a Relying Party when asked for presentation of the attributes in a certain attestation.

Regarding the use cases for individual persons, attribute attestations are mainly issued by national authorities and the content in the attestation stems from national registries. In the discussions about the use of EUDI wallets and attribute attestations in business related contexts, the situation becomes much more varied as a great number of attestations can be business related documents created by the the business actors themselves or their business partners – or even the customers of the businesses. In this usage scenario, privacy preserving issues and the selective disclosure of single attributes like “age over 18” is of a secondary interest, whereas the ability to present business related documents with a complex information structure plus the machine-readable connection to the underlying semantics of the information presented will most certainly be a feature that will attract the interest of economic operators of various kind. Attribute attestations that build on the same semantical foundation will also enable a more efficient and trustworthy use of AI based solutions and AI Agents once business processes are ready to me automatized through these novel technological means.

Closer to data spaces, where emphasis has lately been put on creating machine-readable descriptions of the data products content, deviating from earlier approaches where a simple descriptive labelling of data products was seen as sufficient. In an information sharing situation where both the data provider and the data consumer are highly skilled subject-matter experts in a certain domain and the handling of the shared data is still a very manual, human-centric task, there might not have arisen any difficulties when interpreting received raw data feeds.

Also, UN/CEFACT’s approach to modernize the business documents in international trade utilises W3C Semantic Web standards and introduced the W3C Verifiable Credential specification as a basis for the implementation of these “documents”.

In order to enable optimal semantic interoperability in business ecosystems that rely on the upcoming European Business Wallets, all information sharing in the form of electronic attestations of attributes need to adhere to a strict data modelling methodology that ensures that all attestations issued and presented are linked to an underlying common business vocabulary, which is created by the use of the W3C Semantic Web (Linked Data) tech stack.

One recommended path to be followed in the WE BUILD LSP would be to make use of DSSC (Data Structure and Semantics Catalogue) recommendation compliant tools and create both an business ontology with terms, concepts and their relationships, then develop an extensive Business Vocabulary that is founded both on the commonly defined concepts as well as acknowledged global data standards and reference data models like the EU Core Vocabularies, Schema.org, W3C ontologies, the UN/CEFACT Core Component Library (in its’ Web Vocabulary form), GS1 Web Vocabulary, WTO data models, UBL 2.4 etc.

Finally, the attribute attestation specific data models could be produced as specialisations of the underlying common business vocabulary and serialized as JSON-LD depending on the use-case, which according to the latest technical standards development is also easily included in SD-JWT.





Co-funded by the European Union

## 3.3 Creating a Business Ecosystem using organisational attestations

In order to ensure that the EU Business Wallet (or EUDI Wallet for Legal Entities) will be considered and effectively used as a main building block in the cross-border digitalization of business processes, there will arise a need for the creation of a public-private governance model for an EU Business Wallet ecosystem.

One foundational part of this ecosystem will be the Business Information Data Space (BIDS)[1], which should operate according to recommendations given by the DSSC, including the creation of a common semantic foundation for all organisational attestations issues, held and presented in the various business processes that are included in the ecosystem.

The data sharing capabilities in the BIDS are mainly targeted at the ability to share data to business partners, governmental agencies, end customers and regulatory bodies – all in order to enable the optimally automated execution of business processes that require a large amount of manual work or even the exchange of paper-based information.

In the EU Business Wallet ecosystem, basically any type of information can be created and shared in the form of electronic attestations of attributes that are defined based on the common vocabulary and ontology that the ecosystem itself administers. As a side effect, all data products in the form of EAAs, PubEAAs or (Q)EAAs can also be used in the more traditional way a data space is operating, enabling data consumers to access a range of data products that can prove useful in their own business contexts – and also allowing data providers to monetize the value of the data shared.

## 3.4 Need of Legal Person Wallet for organisational attestations to handle user management

The drafting of the rulebooks catalysed valuable discussions regarding the rights of users in relation to the management and presentation of attestations. A key distinction emerged between the Natural Person Wallet and the Legal Person Wallet. Specifically, the Legal Person Wallet is designed to be accessible by multiple individuals within an organisation, thereby facilitating its integration into routine business processes without the need for the continuous involvement of the entity's legal representative.

This operational model, however, raises important considerations regarding data governance and access control. In the absence of user management mechanisms, any authorised user of the Legal Person Wallet could potentially access or utilise all available attestations. The findings of these tasks clearly demonstrated that user management capabilities are essential to ensure compliance with the GDPR and to uphold the privacy and confidentiality of sensitive data.

One prominent example is the UBO attestation. In order to comply with existing legal and regulatory requirements, only the designated legal representative of the organisation should be permitted to request and present this specific attestation. Similar concerns apply to other sensitive credential types – such as financial, legal, or human resources-related data – which

[1] The Business Information Data Space (BIDS) is a European initiative under the Data Spaces Support Centre (DSSC) and the European Data Strategy. It is a federated data ecosystem designed to make business information more accessible and shareable across borders and sectors.





Co-funded by the European Union

should not be universally accessible to all wallet users within a company. These considerations affirm the necessity of implementing fine-grained access and role-based controls within the Legal Person Wallet infrastructure.

## 3.5 Selective disclosure not necessary in EWC for organisational credentials

None of the organisational credentials defined in the EWC context highlighted the need of selective disclosure of attributes. This need might be identified in future work and in different ecosystems, but at this stage it is not a recommendation. For other use cases than those in EWC, there is a need for selective disclosure for organisational credentials for data minimisation, privacy, and related aspects. EWC has not looked into this topic.

## 3.6 Practical work with data schemas and rulebooks in Github

### 3.6.1 Versioning of data schemas and rulebooks

One challenge encountered in the pilot was the lack of versioning for attestation schemas and rulebooks, which made it difficult to track changes, ensure consistency, and manage dependencies between related schemas. Without clear version control, updates to attribute names or structures in one schema risked breaking compatibility in others, especially when multiple teams were working in parallel.

A known approach is to use semantic versioning which consists of three numbers: major, minor, and patch. For example, version **1.0.0** means:

- **1** is the major version – this changes when you make a breaking change, like renaming or removing an attribute. An example would be to change `organisation_id` to `legal_person_id`.
- **0** is the minor version – this changes when you add something new that is backward compatible, for example if an optional attribute was added to a data schema, such as `legal_entity_status`.
- **0** is the patch version – this changes when you make small fixes or corrections that don't affect the structure or meaning of the schema. Examples would be to correct a spelling mistake.

Furthermore, it is recommended to tag versions using Git. Example: git tag v.1.0.0

Each schema should also contain the current schema version inside the schema itself, and a changelog should be maintained which reflects the changes in each version and why a change has been made. Changelogs address consumers of schemas who want to know what changed, why and how the change might affect them in a summarised and curated way.

### 3.6.2 Reuse of attributes between data schemas

Quite often certain data schemas reuse attributes from other data schemas. An example is the EUCC which reuses `legal_person_id` and `legal_person_name` from the LPID data schema which acts as the master for the information. In these cases, there is a dependency between the master and those schemas that use attributes from the master, i.e. if the master changes, the dependent schemas should also change.





Co-funded by the European Union

It is therefore important to establish a clear method for managing dependencies. One way to address this in GitHub is to modularise the shared components by placing them in separate schema files and referencing them using $ref. Modularise means to split a data schema into smaller, reusable parts (modules) instead of defining everything in a single file. For example, instead of writing all attribute definitions (like `legal_person_id`, `legal_person_name`, etc.) directly inside each attestation schema (e.g. EUCC, Signatory Rights), they are defined once in a separate schema file and then referenced from other schemas.

These shared files can then be versioned independently, with each attestation schema referencing a specific version. To support this, GitHub tags or release branches can be used to mark schema versions, and automated checks (e.g. GitHub Actions) can alert developers when a referenced master schema has been updated. Maintaining a changelog and clear documentation for each schema will also help dependent schemas stay aligned with the latest definitions, reducing the risk of divergence or inconsistency over time.

**Example structure**

```
/schemas
 /shared
  LegalPerson.json      ← contains shared attributes like legal_person_id
  /attestations
    EUCC.json           ← references attributes from LegalPerson.json
  SignatoryRights.json  ← also references LegalPerson.json
```

**Example reference inside `EUCC.json`**

```
"legal_person": {
  "$ref": "../shared/LegalPerson.json"
}
```

If attributes are being reused this way, duplication can be avoided, and the project gains better consistency, easier maintenance and easier versioning support (where shared modules can have their own versions).

## 3.7 Alternative Tech-Stack W3C/DIF

The EWC decided to specify and pilot the business wallets based on the recommended technology described in the ARF and the corresponding tool box. Despite the Regulation establishing a framework for a European Digital Identity requesting an EU digital identity for both natural and legal persons, the ARF and the tool box are almost exclusively concerned with the specification of an EUDI-wallet for EU citizens (natural persons). The specific requirements of an EU Business Wallet are not addressed. Therefore, besides the stack recommended by the ARF an alternative tech-stack was analysed (see the table below).

| | EU Citizen wallet (Mobile) | Business Wallet (alternative) |
|---|---|---|
| Credential format | SD-JWT-VC | VCDM 2.0 |





Co-funded by the European Union

| | | |
|---|---|---|
| Data Model | JSON-Schema (Structure) | JSON-LD (Semantic) |
| Proof format | SD-JWT | VC Data Integrity |
| Binding | Key Binding JWT | DID |
| Exchange Protocol | OID4VCI/OID4VP | WACI<br>(DIF Manifest and Presentation Exchange) |

### 3.7.1 Data modelling

Exchanging data for enterprise applications requires a rich semantic model that enables the interoperability of different systems. While the JSON-Schema utilised in SD-JWT-VC is viable for concise attestations, it is not suitable for expressing complex relations. The VCDM mandates the use of vocabularies (ontologies) to define the semantics of the properties of a verifiable credential (VCDM 2.0 vocabulary) and the credential subjects. The reuse of existing vocabularies and the separation of concerns with respect to credential metadata and identity claims ensures a concise and interoperable definition of complex enterprise identities and finally facilitates interoperability with international and present ecosystems. The utilisation of semantic modelling and reusability of existing vocabularies to define both the verifiable credentials and the enterprise identities are strongly recommended for the forthcoming LSPs.

### 3.7.2 Crypto-agility and selective disclosure

The security vocabulary in conjunction with the verifiable credential data integrity specification allows proofs to be applied to verifiable credentials using a broad range of crypto-suites to match specific requirements with respect to level of assurance and selective disclosure (ecdsa, eddsa, ecdsa-sd, bbs, jose, cose, sd-jwt, …).

It is strongly recommended that crypto-agility, including support of advanced crypto-schemes and in-build selective disclosure, be utilised for the next LSPs.

### 3.7.3 Holder binding

The combination of JSON-LD with DIDs allows any node in a credential's knowledge graph to be linked to an identity, enabling multi-holder scenarios that reflect not only the legal entity, but also representatives. As a result, authentication and authorisation can be implemented for all holders referenced in a verifiable credential. This approach also ensures a seamless user experience. Simultaneous handling of personal and enterprise wallets (so-called wallet dance) is avoided. The same capability also allows to authorise and delegate rights to other natural and legal persons and to cryptographically verify the authority granted (power of attorney).

It is strongly recommended that enterprise wallets support flexible and multi-user credential binding.





Co-funded by the European Union

### 3.7.4 Machine to Machine (M2M) credential exchange and 24x7 availability

The OID protocols have been defined to support credential issuing and presentation scenarios involving a user agent. Business wallets are typically used in B2B business cases where user agents are not involved and 24x7 availability is assumed. Therefore, business wallets are typically (except for sole proprietorships) server-based and used by a group of persons. WACI is optimised for credential exchange without the overhead of user agent involvement and is very well aligned with W3C credentials.

The use of a protocol optimised for B2B communication is strongly recommended for business wallets.

### 3.7.5 User management

Business wallets are used by a group of persons who are entitled to represent the company by signing authority (legal representative) or by delegated authority (power of attorney). In both cases, the person acting on behalf of the company must be identified and authenticated. To avoid the so-called 'wallet dance', the enterprise wallet should be able to hold the credentials of all natural and legal persons associated with the enterprise and should provide user management to ensure that the secret key material associated with a particular identity can only be accessed by the person holding that identity.

### 3.7.6 Registration on infrastructure

DIDs are used to bind cryptographic material to identities. They facilitate the fulfilment of standard security requirements, such as key rotation. Universal resolving provides an abstraction that allows us to adapt to different trust infrastructures easily, e.g.:

- DID:x509 for QTSP's of the EU trust list of list
- DID:ebsi for identities anchored in a qualified distributed ledger based on the European Blockchain Services Infrastructure (EBSI)
- DID:web for identities anchored in DNS (e.g. commonly used by data spaces)
- …

DID also allows to address different levels of security:

- DID:web – DNS
- DID:webvh - DNS with verifiable history

## 4. Risks and gaps in the LPID issuing process

Bolagsverket looked at risks and gaps in the LPID issuing process, with a focus on meeting the requirements for LoA High in the context of the EUDI Wallet and eIDAS 2.0. The analysis highlights practical challenges that business registers face – particularly those that do not usually act as identity providers – when it comes to authentication, verifying applicant authority, cryptographic binding, and validating wallets. The approach is operational rather than technical, aiming to support authorities in understanding what's needed for secure and compliant issuance. Among the risks identified are weak identity checks, unclear controls around who is allowed to request credentials, and gaps in how wallets are trusted and bound to the organisation. These are areas that will need further attention as the ecosystem matures.





Co-funded by the European Union

The report can be found in Annex II of this document.

# 5. Annex I Rulebooks and Data Schemas

## 5.1 Legal Person Identification Data (LPID)

### 5.1.1 LPID rulebook

The LPID rulebook can be found here. It contains requirements specific to the LPID and its issuance process.

eudi-wallet-rulebooks-and-schemas/rulebooks/rb001-legal-person-identification-data.md at main · EWC-consortium/eudi-wallet-rulebooks-and-schemas · GitHub

### 5.1.2 RFC-005

RFC-005 implements the OID4VCI workflow for issuing Legal Person Identification Data (LPID) credentials by government-approved identity providers within the European Wallet Ecosystem. It defines a standard process to minimize risks and ensure interoperability in issuing high-assurance LPIDs across the EUDI wallet ecosystem

eudi-wallet-rfcs/ewc-rfc005-issue-legal-person-identification-data.md at main · EWC-consortium/eudi-wallet-rfcs · GitHub

### 5.1.3 LPID Schema

The LPID data schema can be found here. It is based on the LPID attributes described in RFC-005.

eudi-wallet-rulebooks-and-schemas/data-schemas/ds004-legal-person-identification-data.json at main · EWC-consortium/eudi-wallet-rulebooks-and-schemas · GitHub

## 5.2 European Company Certificate (EUCC)

The power of attorney is work in progress and will be continued in the next LSP WE BUILD.

The EUCC data schema can be found here : https://github.com/EWC-consortium/eudi-wallet-rulebooks-and-schemas/blob/main/data-schemas/ds001-eu-company-certificate.json

The EUCC rulebook can be found here : https://github.com/EWC-consortium/eudi-wallet-rulebooks-and-schemas/blob/main/rulebooks/rb002_eu_company_certificate.md

## 5.3 Ultimate Beneficial Ownership (UBO)

The UBO data schema can be found here : https://github.com/EWC-consortium/eudi-wallet-rulebooks-and-schemas/blob/main/data-schemas/ds006-ultimate-beneficial-owners-attestation.json

The UBO rulebook can be found here : https://github.com/EWC-consortium/eudi-wallet-rulebooks-and-schemas/blob/main/rulebooks/rb_005_ultimate_beneficial_owners.md





Co-funded by the European Union

## 5.4 Signatory Rights (SR)

The Signatory rights data schema can be found here : https://github.com/EWC-consortium/eudi-wallet-rulebooks-and-schemas/blob/main/data-schemas/ds003-signatory-rights-attestation.json

The Signatory rights rulebook can be found here : https://github.com/EWC-consortium/eudi-wallet-rulebooks-and-schemas/blob/main/rulebooks/rb_004_signatory_rights.md

## 5.5 International Bank Account Number (IBAN)

The IBAN data schema can be found here : https://github.com/EWC-consortium/eudi-wallet-rulebooks-and-schemas/blob/main/data-schemas/ds002-iban-attestation.json

The IBAN rulebook can be found here : https://github.com/EWC-consortium/eudi-wallet-rulebooks-and-schemas/blob/main/rulebooks/rb003_IBAN_attestation.md

# 6. Annex II LPID issuing – risks and gaps

## 6.1 Executive summary

This report outlines the risks and gaps in the process of issuing Legal Person Identification Data (LPID) to a business wallet and within the eIDAS 2.0 framework. The report is based on the assumption that LPID issuance must reach assurance level High (LoA High). The risks and gaps identified in the report are grounded in the interpretation of LoA High for natural persons, as defined in Commission Implementing Regulation (EU) 2015/1502[2] on setting out minimum technical specifications and procedures for assurance levels for electronic identification means, which serves as the basis for assessing what is required to achieve a comparable level of assurance in the LPID issuance process. It is also assumed that the entire process is digital, with no manual intervention, that the wallet is server-based and that the LPID is a long-lived attestation.

From this starting point, the report identifies several challenges related to achieving LoA High in practice. Business registers, which are not typically identity providers, face structural difficulties in meeting the high assurance requirements for identity proofing and applicant authentication. In particular, LoA High may require physical presence or technical controls that are currently not in place and would be difficult to implement, especially when applicants are located in different countries.

In addition to authentication, there are gaps in how the authority of the applicant is verified. Today's legal frameworks do not explicitly define how authority checks should be performed in an eID scheme for organisations, nor how such checks relate to LoA requirements. There is also a lack of clarity on how to verify that the legal person requesting the LPID is indeed the one in control of the wallet receiving it. This raises risks around trust, fraud, and misuse of issued credentials.

[2] European Commission. (2015, September 8). *Commission Implementing Regulation (EU) 2015/1502 of 8 September 2015 on setting out minimum technical specifications and procedures for assurance levels for electronic identification means pursuant to Article 8(3) of Regulation (EU) No 910/2014 of the European Parliament and of the Council. Official Journal of the European Union*, L 235, 9 September 2015.





Co-funded by the European Union

Several of the gaps identified relate to the separation between the legal person (the organisation) and the natural person representatives involved in the issuance process. First, the person applying for the LPID does not need to be directly linked to the organisation but must have authority to act on its behalf. Second, the LPID itself is an identifier for the organisation, not for any individual. And third, the person who ultimately installs and manages the wallet unit for the organisation may again be a different person—also not directly linked to the organisation—yet with delegated authority to manage the wallet. These separations introduce ambiguity around responsibility, control, and traceability, which are particularly relevant when aiming to meet LoA High.

The report does not aim to provide technical solutions but highlights concerns that must be addressed to ensure secure and compliant LPID issuance. Further coordination between legal, organisational, and technical specialists is needed for a secure LPID issuance process to business wallets.

## 6.2 Introduction

As a public authority, Bolagsverket is expected to receive the assignment to issue Person Identification Data for legal persons (LPID) under the framework of the European Digital Identity Regulation (eIDAS 2.0). The implementation of LPID within the European Digital Identity Wallet (EUDI Wallet) ecosystem introduces a new more secure and standardized digital identification for organisations. It also presents challenges in ensuring compliance with regulatory requirements, managing risks, and implementing cryptographic security measures.

This report aims to address these challenges by analysing the risks, consequences, and mitigations associated with the LPID issuing process. Particular attention is given to Article 3(5) of Commission Implementing Regulation (EU) 2024/2977[3], which mandates that PID providers ensure that the person identification data they issue is cryptographically bound to the specific wallet unit of the recipient. This report provides insights from an LPID issuer perspective on risks, consequences, mitigation mechanisms, for LPID Provider tasks and in relation to binding enabling LPID providers to effectively prepare for secure, compliant, and efficient implementation.

### 6.2.1 Background

The European Digital Identity Regulation (eIDAS 2.0) introduces the EUDI Wallet, a secure and interoperable digital identity solution for natural and legal persons across the EU. The wallet allows users to store and present person identification data, also for legal persons (LPID), in a way that ensures trust and compliance with cross-border regulatory requirements.

The LPID enables legal persons to engage in authentication, and other secure digital transactions with Issuers and Relying parties. One of the key requirements, as outlined in Article 3(5) of Commission Implementing Regulation (EU) 2024/2977, is that the PID must be cryptographically bound to the specific wallet unit to which it is issued. While cryptographic binding mitigates some risks, it introduces challenges related to implementation, compliance, and usability. For instance, the architecture of the Wallet Secure Credential Device (WSCD) significantly influences the necessary binding processes and security mechanisms.

[3] European Commission. (2024, November 28). *Commission Implementing Regulation (EU) 2024/2977 of 28 November 2024 laying down rules for the application of Regulation (EU) No 910/2014 as regards the integrity and core functionalities of European Digital Identity Wallets. Official Journal of the European Union*, L 2024/2799, 4 December 2024.





Co-funded by the European Union

Furthermore, while binding mechanisms mitigate many risks, they may also impose operational constraints on organisations relying on flexibility and interoperability. These different arguments are discussed in this report.

Another regulation relevant in this context is Regulation 2015/1502, which sets out the specifications and procedures for determining the assurance levels—low, substantial, and high—for electronic identification means issued under a notified electronic identification scheme.

### 6.2.2 Goal

The goal of this document is:

1. Raise awareness of the risks and consequences related to the LPID issuance process.
2. Provide a brief background on binding to support the second goal: identifying the risks, consequences, and mitigation mechanisms associated with the PID provider IA requirement on binding.
3. Evaluate binding mechanisms in relation to usability constraints and wallet functionality, ensuring they are adapted to the needs of legal persons.

### 6.2.3 Target audience

This report is intended for individuals involved in processes within business registries related to LPID issuance.

It is not a technical report. While anyone may read it, the primary audience consists of business developers and project managers, rather than technical experts.

### 6.2.4 Delimitations

This report does not focus on how to mitigate risks and consequences. Instead, it is written from an operational perspective, providing only select technical details to help understand the implications of binding.

The report does not aim to provide a detailed analysis of binding mechanisms. Rather, it offers a broad overview of commonly referenced binding types in relation to LPID processes and highlights the associated risks they are designed to mitigate.

Since Bolagsverket is not an expert in IT-och cryptographic security, the risks and consequences of leaving out controls in processes are listed, but not mitigation measures. This is left to the experts in this field.

### 6.2.5 Assumptive premises

It is assumed that:

- the LPID issuing process is entirely digital and no manual controls are needed;
- the LP wallet is a server-based wallet;
- LoA High is needed for LPID issuance, but not necessarily for LPID use;
- the LPID is a long-lived attestation.





Co-funded by the European Union

## 6.3 Risks connected to the LPID issuing process

The LPID issuance process may involve several activity and control requirements that are critical for meeting the criteria of LoA High. It is assumed that all the whole process is digital, so that no manual verification is needed. This section outlines the activities and controls involved in the LPID issuance process, as well as the current gaps in requirements or interpretations related to assurance level High. The figure below presents a generic flow for applying for an LPID in a business register eService.

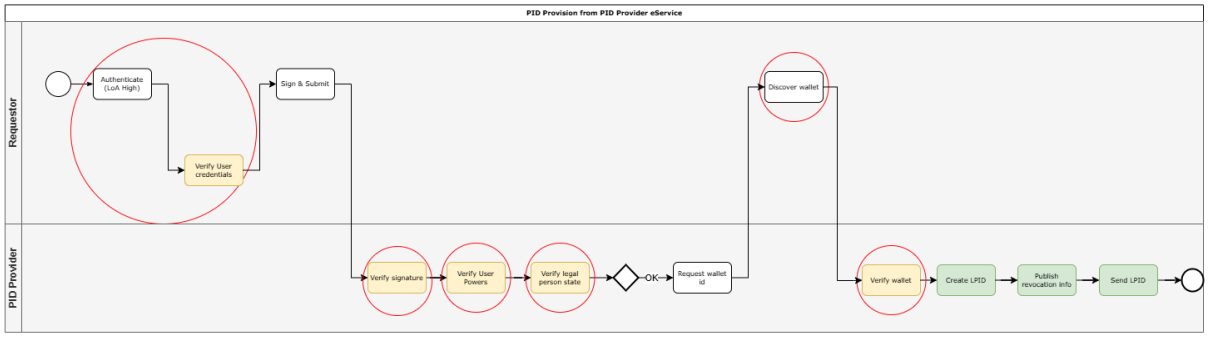


*Figure 1: Generic flow for applying for an LPID in a business register e-service*

Figure 1 has several activities and controls marked in red circles. The following subsections provide a general explanation of the risks and gaps identified in the LPID issuing flow, structured by activity and corresponding controls.

The relevant activities and controls are:

1. Authenticate (sub-section 6.3.1)
2. Verify signature of person applying (sub-section 6.3.2)
3. Verify applicant powers (sub-section 6.3.3)
4. Verify legal person state (sub-section 6.3.4)
5. Discover wallet (sub-section 6.3.5)
6. Verify wallet (sub-section 6.3.6)

### 6.3.1 Authenticate

The first control is the control of authentication of the applicant for the LPID.

We know that an identification on LoA High is needed for requesting an LPID. This follows from Commission Implementing Regulation (EU) 2024/2977, article 3 (7):

*"Member States shall enroll wallet users in accordance with the requirements relating to enrolment at assurance level high, as set out in Commission Implementing Regulation (EU) 2015/1502 (11). In the context of the enrolment process, providers of person identification data shall perform identity verification of the wallet user in accordance with the requirements related to identity proofing and verification before issuing the person identification data to the wallet unit of the corresponding wallet user."*

In this step, Bolagsverket assumes that the identity proofing and verification on LoA High before LPID issuing applies to the applicant (organisation representative of some kind).

According to the existing Swedish notification scheme for eIDs for natural person (by DIGG), an eID issued on LoA High can be assumed to correspond to the Swedish level 3 or 4. An eID on level 3 requires many technical and also organisational controls to be in place, which business registration offices might have difficulty to fulfil since they traditionally have not been





Co-funded by the European Union

IDP providers. However, business registration offices could require authentication with an eID that has previously been issued on level High according to the requirements of the Swedish notification scheme (such as an NPID) in order to allow for login to apply to an LPID (requirement K.5.11, DIGG 2021[4], p.9).

However, if LoA High corresponds to level 4, this reasoning is not possible. An eID on level 4 cannot be issued remotely at all according to the current interpretation in Sweden.

Bolagsverket as an Issuer of an organisational eID on level 4 would not only need to implement all necessary technical and organisational requirement to proof identification on level High but also requesting the applicant to physically be present and have competent personal trained to verify identity documents. For an agency which has not been an identity provider before, it is a serious challenge to live up to all requirements for this task. Requesting a physical presence for organisational representatives is unlikely if board members are meant, since they could be dispersed over the whole world, especially for bigger organisations.

The risks connected to an insufficient authentication process and their consequences are presented in the table below.

*Table 1: Risks connected to an insufficient authentication process*

| Risk description | Consequence |
|---|---|
| Using a false or misleading identity, or falsely claiming to be another individual, in order to request an LPID. | If a misleading identity could be used to request an LPID, someone who is not a valid representative could be in control of an organisations' ID and issue it to a wallet controlled by the requester. This could lead to consequences like fraudulent transactions, data breaches, reputation damages and regulatory breaches. |

### 6.3.2 Verify signature of person applying

This is not a control for security reasons per se but is required in order to achieve a correct administrative process for the Swedish Business Registry. This may vary for other business registries. The signing is for the application of an LPID, not a signature on the LPID attestation itself.

Therefore, this part is not necessary to be analysed in this context.

### 6.3.3 Verify applicant powers

This control is about the verification of rights which the applicant has in order to apply for the LPID on the organisations' behalf.

As of now, for the LPID issuance process, there is no established regulations for an eID scheme which requires the verification of an applicant's authority to apply for an LPID. However, it is assumed that such verification will be required.

- Since Regulation 2015/1502 only outlines the controls required for identity proofing and verification of the subject of the eID itself, there is a gap in relation to security

[4] DIGG. (2021). LoA Mapping: The Swedish Trust Framework (Dnr: 2020-1972). Myndigheten för digital förvaltning. https://www.digg.se





Co-funded by the European Union

controls for the applicant of the LPID – who, in the case of legal persons, is a distinct entity from the subject of the LPID (i.e. the organisation).

- Which kind of representatives are allowed to apply for an LPID? (only board member, anyone with a PoA, CEO, ...)
- Which rules are valid for representatives to apply (alone, or jointly according to MS requirements?)
- Could a (digital) power of attorney be used to apply and which are the requirements on such a PoA? How is the PoA verified and validated? (Note: Could an EU digital PoA according to the Company Law Directive be used for such a purpose?)

Potential verification methods could include:

- Checking official registries that list the legal representatives of an organisation.
- Accepting a power of attorney, provided it is properly signed by authorised representatives of the organisation and has a trust anchor.

This ensures that only individuals with legitimate authority can apply for an LPID and those controls are already being done today, although manually.

The tables below present the identified gaps for controls of applicant powers and how to analyse and the risks connected to an insufficient verification of applicant power and their consequences.

*Table 2: Identified gaps for controls of applicant powers*

| Gap | To analyse |
|---|---|
| There are currently no regulatory requirements mandating control of an applicant's authority to request an LPID in accordance with an eID scheme at LoA High. | • How can Regulation 2015/1502 be connected to controls that verify an applicant's authority to apply for an organisational eID?<br>• How can such authority checks be translated into LoA requirements within an eID scheme governing the issuance of organisational identities? |

*Table 3: Risks connected to an insufficient verification of applicant powers*

| Risk description | Consequence |
|---|---|
| There is a risk that a a person with an unauthorised role applies for an LPID either directly or by power of attorney. | The process for power verification always involves a control against the register for the signatories. If a person does not have the role of signatory or is not allowed to sign alone, the process would stop at that moment.<br><br>Regarding digital power of attorneys, at the time of writing, there is too little known in terms of regulation to understand how controls for the right authorisation could be done.<br><br>Consequences for insufficient controls would be that an LPID was issued to an organisation wallet which did not apply for one and which might be controlled by the fraudulent applicant. Possible aftermaths could be that organisational attestations could be misused. It would undermine trust in the wallets and LPID, it would have legal and regulatory repercussions and probably even financial and operational consequences. |





Co-funded by the European Union

### 6.3.4 Verify legal person state

According to 2015/1502, it is part of the identity proofing and verification of legal person to assure that "*The legal person is not known by an authoritative source to be in a status that would prevent it from acting as that legal person.*"

During a workshop with several business registries in the EWC, there was a shared understanding that reusing the statuses defined in the EU project BRIS for the PID issuance process would be beneficial—particularly by limiting LPID eligibility to businesses classified as "economically active." Since all EU Member States have already mapped their national statuses to the BRIS definitions, this approach would not entail additional implementation effort.

### 6.3.5 Discover wallet

In current processes involving individual person wallets, a QR code is typically displayed to the user for scanning, allowing the wallet to retrieve the endpoint where an attestation should be submitted by the eService.

The other way around, when the presentation offer is initiated from a person wallet, the person wallet would need to know the e-service endpoint to which to send the presentation. Dynamic endpoint discovery is not currently supported in the OpenID4VP protocols and would require additional infrastructure or protocol extensions.

In addition, for business wallet communication with an e-service, dynamic endpoint discovery would need to be supported both ways, initiated by the e-service, but also initiated by the business wallet.

The tables below present the identified gaps for controls of applicant powers and how to analyse and the risks connected to an insufficient verification of applicant power and their consequences.

*Table 4: Identified gaps for wallet discovery*

| Gap | To analyse |
|---|---|
| Dynamic endpoint discovery is not supported in the OpenID4VP protocols. | • For an eService to request a presentation from a business wallet, the eService would need to know the wallets endpoint<br>• For a business wallet to send a presentation offer to an eService the business wallet would need to know the eServices' endpoint |

*Table 5: Risks connected to dynamic wallet discovery*

| Risk description | Consequence |
|---|---|
| As with any dynamic endpoint discovery mechanism, the added complexity of locating and establishing trust in endpoints introduces risks such as spamming, exposure to malicious or spoofed endpoints, user tracking through endpoint | If a wallet interacts with a malicious or spoofed endpoint, it may inadvertently disclose sensitive verifiable credentials, leading to unauthorised access, impersonation, or data breaches. Additionally, endpoint metadata can be exploited for tracking users or organisations, undermining privacy and potentially violating regulations such as GDPR. Poorly protected endpoints may also be vulnerable to spam or denial-of-service attacks, affecting service availability. Furthermore, without clear trust and protocol alignment, dynamic discovery |





Co-funded by the European Union

| | |
|---|---|
| metadata, and other related security and privacy threats. | can result in inconsistent or failed credential exchanges, creating user frustration and interoperability issues. These challenges may also expose ecosystem actors to legal and compliance risks. |

### 6.3.6 Verify wallet

This is a process where two distinct regulations meet and overlap.

As known, the Implementing Regulation 2015/1502 determines LoA levels by describing requirements for an electronic identification scheme.

The EU Cybersecurity Act (Regulation (EU) 2019/881) establishes a European cybersecurity certification framework for ICT products such as the (business) EUDIW with the role of ENISA to develop European cybersecurity schemes (amongst other). The European Commission has recently asked ENISA to develop such a scheme for the EUDIW (*EU Digital Identity Wallet: A leap towards secure and trusted electronic identification through certification* | [Press Release] ENISA[5]).

The overlap between the cybersecurity certification scheme and regulation 2015/1502 is described in paragraph 11 "*IT security certification based on international standards is an important tool for verifying the security compliance of products with the requirements of this implementing act*."

Furthermore, regulation 2015/1502 describes in section 2.2.1 of the Annex that the characteristics and design of the LoA high eID means shall be such that:

1. *The electronic identification means protects against duplication and tampering as well as against attackers with high attack potential*
2. *The electronic identification means is designed so that it can be reliably protected by the person to whom it belongs against use by others.*

It is assumed that the business wallet is an electronic identification means. This entails that the regulation 2015/1502 has requirements on the business wallet in the context of the electronic identification scheme, amongst other to protect against "high attack potential". Within a CSA scheme, AVA_VAN [6] levels are evaluated in order to measure against attack potential amongst other.

Therefore, while it should be possible to establish a stand-alone cybersecurity scheme for the wallet, the different steps in the electronic identification scheme to achieve LoA High likely have security requirements regarding how an eID is issued to a specific wallet unit.

While interpretation of 2015/1502 has not yet been explored for organisations, this chapter will highlight some possible security controls involving intersections between the wallet- and the LPID-Issuer side that could be part of an electronic identification scheme for achieving LoA High in the issuance process.

---

[5] https://www.enisa.europa.eu/news/eu-digital-identity-wallet-a-leap-towards-secure-and-trusted-electronic-identification-through-certification

[6] AVA_VAN levels indicate the extent of cybersecurity evaluation performed to assess resistance to potential exploitation in the operational environment, as defined by the Common Criteria





Co-funded by the European Union

Before the issuance of an LPID to a wallet unit, it is desirable for the Issuer to understand a number of security aspects. The issuer wants to know:

1. If they talk to a EUDI certified wallet (that is intact and has not been tampered with).
2. If the key material is secure enough according to Issuer policies.
3. That the legal person in control of the wallet unit is also the same legal person described in the LPID which is about to be issued to the wallet unit.

Regarding points 1 and 2, for natural persons, experts in the field have an idea to solve both with attestation-based client authentication. At the time of writing, the solution is not finalized, but it is discussed if points 1 and 2 should be one and the same attestation or if to separate these into two attestations: 1) an attestation for trust evidence for the wallet unit and the wallet provider (footnote: proof of a certification of a wallet solution will probably have to be verified via a verifiable data registry) and 2) a key attestation.

It is not yet explored if such a solution would work for a business wallet with a remote WSCD and no frontend.

The table below presents the identified gaps for verifying the wallet authenticity and security.

*Table 6: Identified gaps for verifying the wallet authenticity and security*

| Gap | To analyse |
|---|---|
| For mobile based NP wallets, it has been identified which types of secure storages can be applied for (hardware based) storage of wallet keys in order to achieve a required high level of security. | The same analysis needs to be be done for storage of keys for server-based wallets. |
| For mobile based NP wallets, APIs provided by the platform (f.ex. Play Integrity API from Google) are envisioned to prove that no one has tampered with the app. | If applicable, equivalent methods would need to be in place for server-based wallets. |
| Certification is needed for any wallets | Certification needs to be discussed even for server-based wallets and their components. |

Regarding point 3, the problem is distinct for legal person wallets. It is explained more in detail in the next subsection.

#### 6.3.6.1 Problem statement: Ensuring the legal person controlling a wallet unit matches the LPID being issued

Before issuing an LPID to a Wallet Unit, the Issuer should ensure that the legal person controlling the wallet unit is indeed the same legal person that the LPID describes (proof of ownership of a business wallet). This verification step prevents situations where an LPID for Organisation A is obtained and misused by Organisation B, leading to fraudulent transactions, identity impersonation, or unauthorised access to business services.

This problem arises due to the separation of identities in the LPID issuing and the wallet control mechanism:

1. The person who applies for the LPID does not have to have a direct link to the organisation, instead they need to have authority to act on behalf of the organisation.
2. The LPID is an identifier only for the organisation (not any people associated to it).





Co-funded by the European Union

3. The person applying and installing a wallet unit for the organsisation is another person without necessarily a direct link to the organisation, but with authority to handle the wallet unit on behalf of the organisation.

However, there is no inherent technical trust-link between the entity (organisation) controlling the Wallet Unit and the entity described in the LPID unless such an explicit verification step is performed at issuance.

In step 3 (see above) the Issuer has already verified that the applicant has the authority to apply for an LPID.

The LPID Issuer directly or indirectly needs to know that an organisation is in control of the wallet/has ownership of the wallet. Ideally, this assurance can be established through information included in the wallet's request to the LPID issuer prior to issuance—such as a shared secret or a cryptographic proof, such as proof of the organisation's private wallet keys. An alternative, indirect approach could involve the issuer sending a secure verification code to the organisation through a trusted channel, which is then returned via the wallet to confirm that the organisation is indeed in control of the wallet unit.

It would not be an issue for a wallet to provide evidence to an Issuer of which organisation is in control of a business wallet. Traceability and correlatability in the LPID issuance process are generally not considered problematic for organisations in the same way they are for natural persons. This is primarily because legal entities are established to operate in identifiable and accountable ways, supporting auditability and regulatory compliance, amongst other. Legal entity identifiers, such as company registration numbers or VAT IDs, are often publicly available through national business registers, meaning that a certain degree of transparency is built into how organisations function.

Furthermore, in order to increase security, the Issuer could get proof from the business wallet (e.g. signatures) of authorised representatives with access to the business wallet prior to issuing an LPID.

Even the possibility to activate an LPID after issuing could be a security mechanism, provided that other controls for fulfilling the required level of security are being done in the meantime.

The table below presents identified gaps for achieving LoA High if organisations were to follow current proposed process for NPID LoA High.

*Table 7: Identified gaps for achieving LoA High if organisations were to follow current proposed process for NPID LoA High*

| Gap | To analyse |
|---|---|
| For mobile based NP wallets, remote authentication (of a user before issuing an NPID) is considered a high risk and probably not compliant for LoA High. | For business wallets, remote authentication of a representative for the organisation is necessary or it should be allowed to be represented by yet another person in this process. Official representatives for larger businesses will not be bothered to appear physically for proving their identity. |
| For mobile based NP wallets, user binding is required to prove ownership and achieve LoA High | User binding, as applied in person wallets, is not directly transferable to business wallets, where the "user" is the organisation itself rather than an individual. Binding a business wallet to a specific individual representative is also problematic, as representatives frequently change due to staff turnover or shifts in responsibilities. Such |





Co-funded by the European Union

| | |
|---|---|
| | bindings could introduce operational and security risks—for example, it could result in unauthorised access or misrepresentation.<br><br>A business wallet must therefore support more dynamic and role-based delegation models that reflect the organisation's structure and governance. |
| For mobile based NP wallets, ownership of a mobile based wallet is one of the authentication factors. | Ownership needs to be proven in other ways for server-based wallets. |
| For mobile based NP wallets, a PIN or biometrics serve as a second authentication factor. | For business wallets, it is evident that MFA cannot be implemented the same way as for NP. Other means of securing LoA High need to be established. |

Note: The wallet in this process also wants to know the Issuer policies (e.g. security requirements).

## 6.4 Summary

The findings highlight some of the more prominent risks and gaps in the LPID issuance process, particularly in relation to meeting the requirements for LoA High. Challenges include reliable authentication of the applicant, verification of their authority to act on behalf of the organisation, and secure linkage between the LPID and the organisational wallet. These issues are amplified by the separation between the legal entity and their natural person representatives involved in the process. To ensure a secure and trusted model for LPID issuance, continued dialogue and coordination between technical, organisational, and legal experts is essential. The current gaps in technical specifications need to be addressed and adapted to the LPID issuance to business wallets. Furthermore, a dialogue is needed on how LoA High could be achieved when business representatives are involved and the need for them to act remotely, while keeping a high level of security for the issuance process.





Co-funded by the European Union