

## IMPORTANT NOTICE

### What is the Application Form?

The Application Form is the template for EU grants applications; it must be submitted via the EU Funding & Tenders Portal before the call deadline.

The Form consists of 2 parts:

- Part A contains structured administrative information
- Part B is a narrative technical description of the project.

Part A is generated by the IT system. It is based on the information that you enter into the Portal Submission System screens.

Part B needs to be uploaded as PDF (+ annexes) in the Submission System. The templates to use are available there.

### How to prepare and submit it?

The Application Form must be prepared by the consortium and submitted by a representative. Once submitted, you will receive a confirmation.

#### Character and page limits:

- page limit normally **70** pages (unless otherwise provided in the Call document)
- supporting documents can be provided as an annex and do not count towards the page limit
- minimum font size — Arial **9** points
- page size: A4
- margins (top, bottom, left and right): at least 15 mm (not including headers & footers).

Please abide by the formatting rules. They are NOT a target! Keep your text as concise as possible. Do not use hyperlinks to show information that is an essential part of your application.

**⚠** If you attempt to upload an application that exceeds the specified limit, you will receive an automatic warning asking you to shorten and re-upload your application. For applications that are not shortened, the excess pages will be made invisible and thus disregarded by the evaluators.

**⚠ Please do NOT delete any instructions in the document. The overall page limit has been raised to ensure equal treatment of all applicants.**

**⚠ This document is tagged. Be careful not to delete the tags; they are needed for the processing.**

## TECHNICAL DESCRIPTION (PART B)

### COVER PAGE

*Part B of the Application Form must be downloaded from the Portal Submission System, completed and then assembled and re-uploaded as PDF in the system. Page 1 with the grey IMPORTANT NOTICE box should be deleted before uploading.*

**Note:** Please read carefully the conditions set out in the Call document (for open calls: published on the Portal). Pay particular attention to the award criteria; they explain how the application will be evaluated.

PROJECT	
<b>Project name:</b>	European Digital Identity Wallet - Partnership for Alignment, Certification & Testing
<b>Project acronym:</b>	EUDIW PACT
<b>Coordinator contact:</b>	Florent TOURNOIS, ANTS, Agence Nationale des Titres Sécurisés / Programme France Identité Numérique

### TABLE OF CONTENTS

<b>TECHNICAL DESCRIPTION (PART B) .....</b>	<b>2</b>
<b>COVER PAGE .....</b>	<b>2</b>
<b>PROJECT SUMMARY .....</b>	<b>3</b>
<b>1. RELEVANCE .....</b>	<b>3</b>
1.1 Objectives and activities.....	3
1.2 Contribution to long-term policy objectives, policies and strategies — Synergies .....	5
1.3 Digital technology supply chain .....	6
1.4 Financial obstacles .....	7
<b>2. IMPLEMENTATION .....</b>	<b>7</b>
2.1 Maturity.....	7
2.2 Implementation plan and efficient use of resources.....	8
2.3 Capacity to carry out the proposed work .....	14
<b>3. IMPACT .....</b>	<b>23</b>
3.1 Expected outcomes and deliverables — Dissemination and communication.....	23
3.2 Competitiveness and benefits for society .....	24
3.3 Environmental sustainability and contribution to European Green Deal goals .....	25
<b>4. WORK PLAN, WORK PACKAGES, ACTIVITIES, RESOURCES AND TIMING .....</b>	<b>26</b>
4.1 Work plan .....	26
4.2 Work packages, activities, resources and timing .....	27
Work Package 1 .....	28
Work Package 2 .....	33
Work Package 3.....	37
Work Package 4.....	44
Work Package 5.....	48
Staff effort (n/a for Lump Sum Grants).....	52
Subcontracting (n/a for prefixed Lump Sum Grants).....	56
Purchases and equipment.....	59
Other cost categories .....	62
Timetable .....	62
<b>5. OTHER .....</b>	<b>65</b>
5.1 Ethics.....	66
5.2 Security.....	66
<b>6. DECLARATIONS .....</b>	<b>66</b>
<b>ANNEXES .....</b>	<b>66</b>

#@APP-FORM-DEP@#

#@PRJ-SUM-PS@# [This document is tagged. Do not delete the tags; they are needed for the processing.]

## PROJECT SUMMARY

Project summary
See Abstract (Application Form Part A).

#\$PRJ-SUM-PS\$# #@REL-EVA-RE@# #@PRJ-OBJ-PO@#

## 1. RELEVANCE

### 1.1 Objectives and activities

#### Objectives and activities

*Describe how the project is aligned with the objectives and activities as described in the Call document.*

*How does the project address the general objectives and themes and priorities of the call? What is the project's contribution to the overall Digital Europe Programme objectives?*

The European Union has made the deployment of a trusted, secure, and interoperable digital identity framework a strategic priority for the digital decade. The revised **eIDAS Regulation (Regulation (EU) 910/2014 as amended by Regulation (EU) 1183/2024)** establishes the legal foundation for the **European Digital Identity Wallet (EUDI Wallet)**, a cornerstone of the EU's ambition to empower citizens and businesses with sovereign control over their digital identity and credentials. To ensure trust, security, and cross-border interoperability, the Regulation mandates that all Member States issue certified EUDI Wallets by **25 December 2026**.

This regulatory ambition is supported by a comprehensive technical and governance framework, including the **Architecture and Reference Framework (ARF)**, a set of **Implementing Acts**, and the development of a common conformance testing infrastructure. **Certification plays a pivotal role in this ecosystem:** it ensures that wallet solutions meet stringent functional, cybersecurity, and privacy requirements, and that they can be trusted across borders by relying parties and end-users alike.

In this context, the consortium aims to contribute decisively to the European effort to deploy certified and interoperable EUDI Wallets across Member States by the regulatory deadline, set to December 2026. It brings together a group of committed Member States stakeholders (wallet providers, PID issuers, NCCAs) and technical partners (Conformity assessment bodies, experts), building on the operational and policy frameworks established during the last months on EUDIW and certification.

The project pursues four complementary and interdependent objectives:

#### 1. Certify at least one EUDI Wallet by December 2026

The primary objective of the project is to support participating Member States in bringing at least one EUDI Wallet to conformity and certification in accordance with the Regulation and relevant Implementing Acts. The project will provide technical, methodological, and coordination support to facilitate the process required for certification readiness and successful certification. This includes:

- Supporting the development, integration, and validation of an EUDI Wallet aligned with the Architecture and Reference Framework (ARF) and relevant Implementing Acts;
- Supporting integration with national infrastructures where applicable (e.g. PID issuance systems, relying parties registries, attestation providers, etc);
- Supporting conformity assessment activities under applicable national certification schemes, in cooperation with national authorities, accreditation bodies, and Conformity Assessment Bodies (CABs);

- Supporting issuance or recognition of the wallets developed by participating Member States to support the fulfilment of their obligations under the Regulation.

The certified wallet will serve as a concrete reference case, demonstrating certification in practice and generating reusable knowledge to support harmonized approaches to EUDI Wallet certification across Member States. By the end of the project (later than the December 2026 deadline), it is expected to have more than one certified wallet.

## 2. Accelerate the establishment and coordinate application of national certification schemes

Whilst a common European cybersecurity certification scheme is developed by ENISA, Member States have to rely on national certification schemes before the common scheme is in place and to cover functional and privacy requirements not covered by the common scheme. The consortium will support the creation and coordinate application of national certification schemes for EUDI Wallets. These schemes will:

- Cover relevant requirements stipulated by both European and national legislations;
- Be developed in alignment with the ARF, the EU Cybersecurity Act, and ISO standards around certification;
- By introducing modularity of the scheme, it will be applied jointly across several Member States to build on the common body of knowledge and to streamline evaluation as well as certification activities.

The project also aims to support the definition of evaluation plans, audit frameworks, and lifecycle management procedures, in close collaboration with national accreditation bodies and Conformity Assessment Bodies (CABs).

## 3. Leverage European Commission support actions

The project is fully aligned with the three pillars of support outlined by the European Commission:

- **Common Conformance Testing Framework:** The consortium will rely on Commission's test specifications, tools, and infrastructure, including the Test Book and ecosystem test bed if applicable and made available in time.
- **Joint development and certification:** The project will foster cooperation between Member States to accelerate wallet development and certification, in line with the Call objectives.
- **Adoption support:** The consortium will promote wallet adoption through stakeholder engagement, alignment with EUDIW ecosystem and other LSPs, and alignment with use-case manuals published by the Commission. It is planned to have dedicated boards between the European Commission stakeholders around EUDIW and project members.

## 4. Benefit from previous EU-funded projects to leverage learnings and synergies and value-added effects

The project will:

- Build on the infrastructures, reference implementations, and testbeds developed under previous and current EU-funded initiatives, notably *APTITUDE* and *We Build*;
- Reuse technical documentation, governance models, and certification frameworks already piloted;

Additionally, the project is aimed at achieving the following effects:

- Provide structured feedback to the Commission to support the evolution of the EUDI Wallet ecosystem.

- Promote mutual recognition of certified wallets and stakeholders, reducing duplication and enhancing trust.

To achieve these objectives, the project will implement a set of targeted activities structured around five work packages:

- **WP1 – Governance:** Strategic oversight, coordination between Member States, and alignment with the Commission's roadmap.
- **WP2 – Sandbox:** Playground environment allowing for preliminary testing of the wallet. Develop joint methods to validate components and processes.
- **WP3 – Certification:** Definition and application of joint certification schemes, in collaboration with CABs and national authorities.
- **WP4 –Support:** Development and use of a catalogue of open-source components used to develop modular wallet solutions.
- **WP5 – Trustiness:** Strengthening the long-term security, trust, and resilience of the EUDI Wallet beyond the initial MVP.

#@COM-PLE-CP@#

## 1.2 Contribution to long-term policy objectives, policies and strategies — Synergies

### Contribution to long-term policy objectives, policies and strategies — Synergies

*Describe how the project contributes to long-term policy objectives of the call's domain/area and to the relevant policies and strategies, and how it is based on a sound needs analysis in line with the activities at European and national level.*

*What challenge does the project aim to address?*

*The objectives should be specific, measurable, achievable, relevant and time-bound within the duration of the project.*

#### Long-term policies:

The project contributes to the long-term policy objectives of the European Union in the field of digital identity. In line with the Digital Decade Policy Programme 2030, the EU aims for at least 80% of citizens to use a digital identity solution by 2030. The amended eIDAS Regulation (eIDAS 2.0) establishes the EUDI Wallet as the central instrument to achieve this target and sets a binding deadline for Member States to issue certified wallets by 25 December 2026. The consortium directly supports this ambition by focusing on the two pillars that are essential for long-term trust and adoption: **issuance and certification**. The project accelerates the delivery of compliant wallets, strengthens interoperability and mutual recognition, and thereby enables the creation of a truly European wide digital identity ecosystem.

The project also contributes to the overarching objectives of the EU Digital Strategy and "Shaping Europe's Digital Future", by transforming the legal and technical foundations of eIDAS 2.0 into practical, operational deployments. In doing so, it delivers predictability and operational benefits for all actors (public authorities, conformity assessment bodies, wallet providers) in a context where both the regulatory framework and the technology are still in a dynamic and evolving state.

#### Contribution to relevant strategies and synergies:

At the European level, the project is aligned with the Commission's support actions and builds on the large-scale pilots (APITUDE and We Build). It leverages their infrastructures, governance models, and reference implementations, while extending their scope to accelerate certification and issuance. This ensures continuity, avoids duplication, and creates synergies between national efforts and EU-wide frameworks.

At the national level, Member States face the challenge of issuing certified wallets within a short time frame and under strict regulatory and technical conditions, and within the conformity assessment framework. The consortium addresses this need by supporting and/or providing:

- Reusable modular wallet components that can be integrated into national infrastructures;

- Certification modular schemes that reduce duplication, ensure consistency, and foster mutual recognition; these certification schemes will rely on existing work being done on the national level and the consortium's input, where relevant;
- Practical evaluation and testing activities using the Commission's test infrastructure and LSPs test infrastructures to validate national implementations against EU requirements.

#### **Needs analysis and relevance:**

The consortium aims to answer to those concrete needs/challenges:

- **Tight regulatory deadline:** (25 December 2026). Member States are at very different stages of readiness. Some have advanced pilots and infrastructures, while others are only beginning preparations. Without strong coordination, many Member States risk delays in issuing wallets, which would undermine the application of the Regulation and the EU's Digital Decade targets. The consortium reduces this fragmentation by offering common components, certification schemes, and mutual recognition mechanisms, thereby ensuring convergence towards a uniform assurance level thus avoiding fragmentation and heterogeneity. The consortium provides a collective mechanism to accelerate issuance and certification of Wallets in at least two Member States.
- **Certification and trust gaps:** Certification of wallets is both technically complex and resource intensive. Without joint schemes and mutual recognition, certification efforts could become duplicated, inconsistent, or delayed. The project directly addresses this by pooling expertise from Member States, accreditation bodies, and conformity assessment bodies, creating robust and harmonised certification processes that benefit all participants.
- **Cybersecurity and privacy requirements:** EUDI Wallets must comply not only with functional specifications but also with stringent cybersecurity obligations (EU Cybersecurity Act) and data protection obligations (GDPR). Member States may lack sufficient expertise or resources to integrate these aspects into their national schemes on their own. The project provides the necessary frameworks, evaluation plans, and guidance to ensure wallets are both legally and technically compliant.

By addressing these needs, the consortium ensures that wallet issuance, certification, and recognition are not only achieved by the deadline but also embedded in a sustainable governance and technical framework that serves Europe's long-term policy objectives.

#### **SMART objectives:**

**Specific (S):** Support the issuance and certification of interoperable EUDI Wallets in compliance with eIDAS 2.0 by developing harmonised certification schemes and modular wallet solutions.

**Measurable (M):** Achieve successful EU conformance testing and mutual recognition of certified EUDI Wallets across participating Member States.

**Achievable (A):** Build on existing regulatory frameworks, technical standards, and Member State expertise to deliver certifiable and interoperable wallet implementations.

**Relevant (R):** Directly contribute to the EU Digital Decade objective of reaching 80% digital identity usage by 2030 through trusted and interoperable EUDI Wallets.

**Time-bound (T):** Complete issuance support, certification alignment, and conformance validation for at least one wallet by 25 December 2026.

#\$COM-PLE-CP\$#

### **1.3 Digital technology supply chain**

#### **Digital technology supply chain**

*Explain to what extent the project would reinforce and secure the digital technology supply chain in the EU.*

 This criterion might not be applicable to all topics — for details refer to the Call document.

**N/A**

## 1.4 Financial obstacles

### Financial obstacles

*Describe to what extent the project can overcome financial obstacles such as the lack of market finance.*

 This criterion might not be applicable to all topics — for details refer to the Call document.

**N/A**

#\$PRJ-OBJ-PO\$# #\$REL-EVA-RE\$# #@QUA-LIT-QL@# #@MAT-URI-MU@#

## 2. IMPLEMENTATION

### 2.1 Maturity

#### Maturity

*Explain the maturity of the project, i.e. the state of preparation and the readiness to start the implementation of the proposed activities.*

From both an organisational and technical perspective, the project background and ecosystem are mature and ready to start implementation. The consortium brings together Member State authorities and technical partners who have all actively participated in the previous Large-Scale Pilots (LSPs) and in the EUDI Cooperation Group. This combination ensures solid governance, a deep understanding of the regulatory and technical ecosystem, and strong readiness to operationalize the next phase of the European Digital Identity framework.

On the technical side, the project builds on a significantly more mature foundation than during previous pilot calls.

- The revised eIDAS Regulation (EU) 1183/2024 is now providing a legal basis for the issuance of the EUDI Wallet.
- The Architecture and Reference Framework (ARF) has reached a consolidated version. It will be updated again.
- The Reference Implementation (RI), developed by the European Commission, is more mature and being continuously improved with upcoming releases.
- Several Implementing Acts have been published, notably the Implementing Regulation (EU) 2024/2981, defining certification requirements for EUDI Wallets and the expected role of Conformity Assessment Bodies. Not all Implementing acts are in place while some will be reopened as well.
- Existing national certification schemes or systems can be reused as a basis

On the organisational side, the consortium's readiness is equally high. Most participating Member States have established national governance structures for the EUDI Wallet.

#\$MAT-URI-MU\$# #@CON-MET-CM@# #@PRJ-MGT-PM@# #@FIN-MGT-FM@# #@RSK-MGT-RM@#

## 2.2 Implementation plan and efficient use of resources

### Implementation plan

Show that the implementation work plan is sound by explaining the rationale behind the proposed work packages and how they contribute to achieve the objectives of the project.

Explain the coherence between the objectives, activities, planned resources and project management processes.

Show how the project integrates, builds on and follows up on any pre-existing work or EU funded projects. Provide details (including architecture and deliverables) about pre-existing technical solutions.

### Rationale between the proposed project and the achievement of objectives:

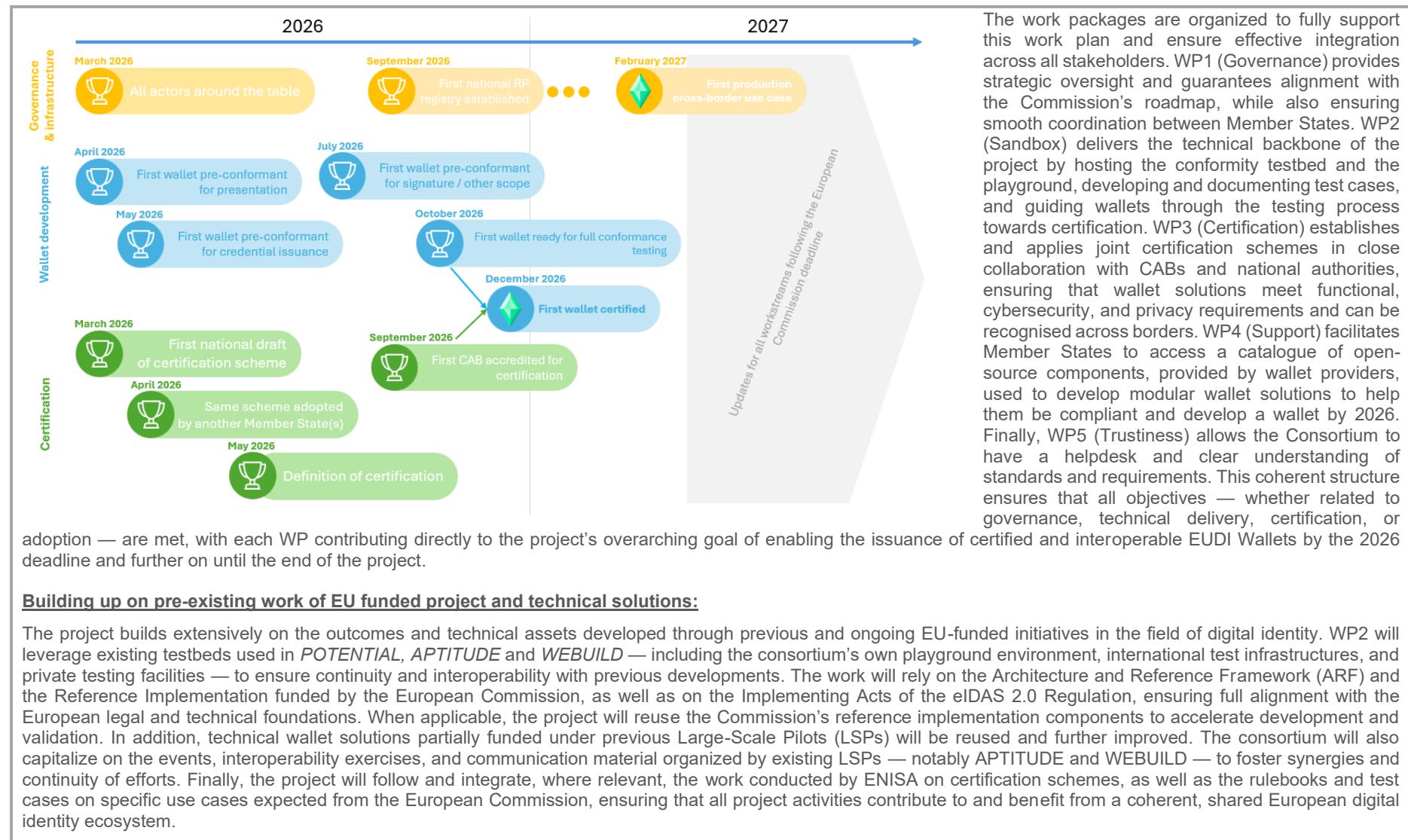
The project is designed around several Work Packages (WPs) to ensure the seamless execution of the objectives related to the development, certification, issuance, and adoption of the European Digital Identity Wallet (EUDIW). The primary objective behind the chosen WPs is to ensure that Member States' wallets are compliant with core functionalities, successfully certified under national schemes, interoperable across borders, and recognised by other Member States. While each WP is structured to address a specific dimension of the project — such as wallet development, certification frameworks, conformance testing, or Member States support — it is crucial that these WPs are closely coordinated to guarantee operational efficiency and uniformity across the ecosystem. This coordination will facilitate consistent implementation across Member States, enabling the consortium to leverage synergies and best practices, while maintaining strict alignment with both technical specifications (ARF, Implementing Acts, Commission expectation) and legal compliance (eIDAS 2.0, GDPR, Cybersecurity Act). By doing so, the project will ensure that all relevant stakeholders are effectively engaged.

The project's work plan is structured to ensure alignment with the objectives outlined in Section 1.1 and involves close collaboration with multiple stakeholders, including Member State authorities responsible for the issuance of the EUDI Wallet, agencies and entities responsible for certification (NCCAs, CABs), and legal public entities ensuring regulatory oversight and compliance. The work packages are designed to meet the needs of these stakeholders and ensure that the wallet solutions developed are fully compliant with the European Digital Identity Framework and can be certified and issued by Member States by the end of 2026. Different actors evolving around EUDIW issuance and certifications needs to be around the table: Waller Providers, PID Providers, NCCAs, CABs, experts. This justifies the composition of the consortium and the resources mobilised in the proposal.

The project follows five main work packages focusing on the objectives and needs of the call, all following their specific workstream. Still, all work packages and all workstreams of the project are around the three main topics:

- Governance and infrastructure
- Wallet development
- Certification

Below is an illustration of the high-level milestones the project aims to reach to stay in line with the European Commission expectations in regards to issuance and certification. *Those milestones are objectives that need to be reached, but do not represent a clear and concise commitment.*



### **Project management, quality assurance and monitoring and evaluation strategy**

*Describe the measures planned to ensure that the project implementation is of high quality and completed in time.*

*Describe the methods to ensure good quality of monitoring, planning and control activities.*

*Describe the evaluation methods and indicators (quantitative and qualitative) to monitor and verify the outreach and coverage of the activities and results. The indicators proposed to measure progress should be specific, measurable, achievable, relevant and time-bound.*

To ensure high-quality project implementation and timely completion, the consortium will establish a robust project management framework under WP1 – Governance. This framework will include clear procedures for planning, monitoring, reporting, and quality control. WP1 will oversee the progress of all other WPs, coordinate resources, track timelines and deliverables, and ensure compliance with both the Grant Agreement (GA) and the Consortium Agreement (CA).

Dedicated tools will be used to provide full visibility of progress. Regular project reviews (internal and external) will ensure that deviations are detected early and corrective measures are applied. Quality assurance is embedded across all WPs: each WP leader will be responsible for ensuring that deliverables meet defined quality criteria before submission. A peer-review mechanism within the consortium will reinforce this process, while external feedback (from the Commission and relevant expert groups) will be integrated to guarantee alignment with evolving EU requirements.

### **Monitoring and evaluation methods**

The project's monitoring and evaluation (M&E) strategy combines **quantitative indicators (KPIs)** with **qualitative performance measures**. Data will be collected systematically at WP level and consolidated by WP1 to ensure comparability and accuracy. WP1 will oversee the validation of inputs and the production of consolidated progress reports.

#### **Quantitative indicators (KPIs):**

- Number of wallet providers in line with Article 3 of Implementing Regulation (EU) 2025/849 integrated into the project;
- Number of conformity assessment bodies (CABs) as defined in Article 2(13) of Regulation (EU) 765/2008 involved and accredited;
- Number of national certification schemes for the EU Digital Identity Wallet developed and applied;
- Number of EU Digital Wallet solutions developed and certified;
- Number of certified EU Digital Identity Wallets issued or recognised by Member States;

#### **Qualitative indicators:**

- Level of engagement of Member States and national stakeholders;
- Quality and completeness of certification schemes developed;
- Degree of compliance with ARF, Implementing Acts and Commission test specifications;
- Evidence of mutual recognition agreements and cross-border interoperability;
- Readiness for large-scale adoption and feedback from end-users and relying parties.

These indicators are specific, measurable, achievable, relevant and time-bound (SMART). They will be monitored continuously throughout the project lifecycle, with interim evaluations at the end of each project year, and a final evaluation at project close.

### **Roles and responsibilities**

Each WP will ensure the implementation of QA and M&E standards within its scope and will provide structured data for central reporting. WP leaders will submit periodic WP-specific reports. At national level, Single Points of Contact (SPOCs) have been identified. Each Member State will nominate a SPOC acting as official representative, consolidating national positions, and ensuring alignment with project objectives. Most of the time, SPOCs are from the entity in charge of eIDAS 2 implementation and/or Wallet Provider. SPOCs will:

- Monitor implementation of wallet issuance and certification at national level;
- Ensure alignment with the technical and operational requirements defined by the project;
- Bridge communication between national stakeholders and the consortium;
- Monitor risks and escalate issues to WP1 for resolution;
- Ensure national contributions adhere to the consortium's QA framework.

#### **Risk management and corrective actions**

Risk management will be integrated into project governance. WP1 will maintain a risk register, reviewed quarterly, identifying potential risks (e.g., delays in Commission deliverables, accreditation bottlenecks, technical integration challenges) and proposing mitigation measures. Corrective action plans will be developed and monitored via the consortium's dashboards.

#### **Evaluation strategy**

Evaluation will focus both on outputs (deliverables, milestones achieved, certified wallets issued) and outcomes (adoption readiness, trust, interoperability). The evaluation process will be documented in an Evaluation Framework prepared in the first 3 months of the project, detailing methodologies, responsibilities, and timelines.

Final evaluation will assess the extent to which the project has:

- Enabled at least one certified wallets to be issued in by December 2026, and enabled additional certified wallet by the end of the pilot;
- Delivered certification schemes;
- Contributed to the Member States capabilities of issuing their own national wallet, based on the Reference Implementation if applicable;

#### **Cost effectiveness and financial management (n/a for prefixed Lump Sum Grants)**

*Describe the measures adopted to ensure that the proposed results and objectives will be achieved in the most cost-effective way.*

*Indicate the arrangements adopted for the financial management of the project and, in particular, how the financial resources will be allocated and managed within the consortium.*

**⚠ Do NOT compare and justify the costs of each work package but summarize briefly why your budget is cost effective.**

The COO through its affiliated entity **CIVIPOL oversees budget management and monitoring and assists beneficiaries and affiliated entities with financial procedures**.

Due to the large number of partners and to ensure that the budget is managed properly, **CIVIPOL will develop a tool in which partners can input their expenditures and adjustments**. This allows CIVIPOL to **assess the budget and anticipate changes** and it gives the partners a common tool that they can use throughout the project to ensure good financial management. The completeness of this tool by partners will be requested **every 12 months through the reporting periods** to enable CIVIPOL to assess the partners' familiarity with budget monitoring and financial rules. It will also be the opportunity to ensure timely identification of deviations and the application of corrective actions.

In addition, this will allow the partners to better understand the financial expectations of the European Commission, facilitating more effective financial management and ensuring that official financial reports are prepared more efficiently.

Financial **information sessions will be held by CIVIPOL** in the beginning of the project and mid-way through the project, to disseminate the knowledge on the rules for the financial reporting and sensitize them on the process to provide their financial statements on the European Commission portal. These sessions will ensure that all the partners are informed of the budget monitoring and the content of the periodic reports.

Documentation such as FAQs and presentations will be made available to partners to enable them to access financial information at any time. CIVIPOL will be available to answer questions and organise meetings whenever a partner identifies a need related to FM. In case of deviations, respective issues shall be raised and discussed in the governing bodies where possible decisions for reallocation or re-focusing may be taken. Regular financial reports are foreseen to ensure timely identification of deviations and the application of corrective actions.

Then, **financial updates will be shared** to ensure that information circulates smoothly. Finally, the **coordinating team will be responsible for distributing the European Commission's grant funds** to the beneficiaries and affiliated entities through CIVIPOL.

#### **Additional allocation mechanisms for WP1 and WP4**

Within WP1 and WP4, specific budget envelopes are planned to support participating Member States through dedicated funding mechanisms. Funding is allocated to partners already participating in the consortium and is not distributed upfront. Instead, the project applies a **best value for money** approach, whereby resources are allocated based on concrete technical and financial proposals submitted during the project and aligned with work package objectives.

#### Objectives

- Support Member States in addressing clearly identified technical needs related to the development, certification and deployment of national EUDIW wallets
- Ensure that funding is allocated based on demonstrated needs and evaluated proposals, rather than fixed pre-allocations
- Maximize best value for money by selecting cost-effective and technically relevant solutions

#### Expected results

- Development of software components such as code modules, SDKs or technical building blocks
- Access to external services (e.g. technical expertise, development, testing or security support) where required
- Tangible outputs contributing to the conformity, interoperability and security of national wallets

#### Modalities

- For WP1, funding is performance-based. Member States that achieve milestones in line with the ambitious project roadmap will be eligible for additional budget allocations. All expenditure must be justified through technical and financial contributions, demonstrating concrete progress and results. Funding is linked to milestone completion and validated deliverables, ensuring that resources reward achievement and drive the project forward.

- For WP4, funding is granted based on technical and financial proposals addressing specific project needs. Proposals are evaluated jointly by Work Package Leaders and the COO, with priority given to solutions that are cost-effective, technically relevant, and aligned with project objectives. Implementation is monitored under the project governance framework, with the mandated public entity remaining the primary beneficiary even if subcontractors are involved.
- Direct beneficiaries are public entities or entities mandated by Member States and established in the EU; if subcontracting is used, the mandated public entity remains the primary beneficiary
- Final funding decisions are taken jointly by relevant stakeholders (eg. WPLs, COO)
- Implementation and validation of funded activities are monitored within the project governance framework, in line with European Commission rules

The detailed principles and rules for budget allocation, milestone validation, and eligible activities will be formally defined in the Consortium Agreement. It is to be noted that these envelopes will be allocated to public entities within the Consortium, which do not consist in financial support to third parties (not allowed within this call for proposals).

<b>Critical risks and risk management strategy</b> Describe critical risks, uncertainties or difficulties related to the implementation of your project, and your measures/strategy for addressing them. Indicate for each risk (in the description) the impact and the likelihood that the risk will materialise (high, medium, low), even after taking into account the mitigating measures. <b>Note:</b> Uncertainties and unexpected events occur in all organisations, even if very well-run. The risk analysis will help you to predict issues that could delay or hinder project activities. A good risk management strategy is essential for good project management.				
No	Description	Likelihood impact	WP No	Proposed risk-mitigation measures
1	Insufficient stakeholders' engagement or departure of key partners for different reasons	Medium	All	Project goals, milestones, deliverables, and progress updates will be regularly communicated to all SPOCs and WP Leaders to maintain transparency. Designated SPOCs are responsible for maintaining communication with their national stakeholders, addressing concerns, and ensuring their continued participation. The coordination team will monitor engagement and report any risk of withdrawal early.
2	Costs overrun compared to initial estimates	High	WP1	A robust financial monitoring system will be implemented under WP1 to track expenditures and resource allocation. Regular financial reviews will allow early detection and mitigation of deviations.
3	Delays in the delivery of technical specifications or conformance testing artefacts by the European Commission (e.g., Test Book, Testbed access)	High	WP2, WP3	Maintain close coordination with the Commission and Cooperation Group. Prepare early integration plans based on draft versions of the specifications and ensure flexibility to update components once the final versions are released. Schedule buffer periods before critical milestones.
4	Instability or frequent updates of technical specifications	Medium	WP2	The project will "freeze" internal specifications to ensure stability. Alignment meetings with the Commission will ensure up-to-date compliance without excessive rework.
5	Limited availability or readiness of Conformity Assessment Bodies (CABs) to perform certification within project timelines	High	WP3	Engage CABs early as consortium partners. Provide technical documentation and training material on wallet certification. Prepare joint templates and checklists to

				reduce evaluation time. Encourage cross-border collaboration between CABs to share capacity.
6	Divergent national certification schemes leading to limited mutual recognition	High	WP3	Organise workshops between national authorities and CABs to ensure convergence. Ensure all schemes are validated against common criteria and ARF requirements.
7	Poor compliance results or failure of wallet components during conformance testing	Medium	WP2	Rely on the Commission's Reference Implementation as a baseline. Use the project's hosted testbed to ensure early validation. Conduct multiple test iterations (component, system, cross-border) before official certification rounds. Use of guidelines given by WP5.
8	Delays in integration of national infrastructures impacting testing and issuance	Medium	WP2	Conduct regular coordination calls and knowledge-sharing sessions between partners. Develop joint guidance materials to support less mature participants. Ensure flexible work allocation to accommodate national readiness levels.
9	Varying maturity levels and readiness between participating Member States	Medium	All	Support from WP4 aims to reduce that varying maturity level when possible
10	Overlapping commitments with previous or parallel projects (APTITUDE, We Build) leading to resource constraints	Medium	All	Maintain integrated scheduling with the Cooperation Group. Identify shared resources early and establish contingency planning for overlapping tasks. Coordinate with project managers of related initiatives to avoid conflicts.
11	Delayed specifications, contradictory releases, ambiguity or lack of clarity when implementing new requirements of the ARF	Medium	WP2, WP3	Close collaboration with EC and expert groups for alignment of timelines and specifications; leverage of national wallets for UC tests; early involvement of experienced developer team.

#\$CON-MET-CMS# #\$PRJ-MGT-PM# #\$FIN-MGT-FM# #\$RSK-MGT-RM# #@CON-SOR-CS@#

### 2.3 Capacity to carry out the proposed work

#### Consortium cooperation and division of roles (if applicable)

Describe the participants (Beneficiaries, Affiliated Entities and Associated Partners, if any) and explain how they will work together to implement the project. How will they bring together the necessary expertise? How will they complement each other?

In what way does each of the participants contribute to the project? Show that each has a valid role and adequate resources to fulfil that role.

Note: When building your consortium you should think of organisations that can help you reach objectives and solve problems.

**FR:** Ministère de l'Intérieur (Moi) will participate in this Consortium as the public body representing both the French EUDIW provider (AE - ANTS), and financial manager (AE - CIVIPOL). They are in charge of France Identité application, and participating in WP1, WP2, WP4, WP5 and as COO. ANSSI is the national cybersecurity agency (also in charge of conformity and certification when it comes to eidas). They will actively participate in WP3. Additionally, French CABs CLR Labs, Elitt, RedAlert, LSTI will participate within WP3.

**BE:** The Belgian NCCA, part of the Centre for Cybersecurity Belgium (CCB), provides guidance and support to Belgian companies in the EU cybersecurity certification process and oversees and monitors compliance with the scheme of certificates issued by Conformity Assessment Bodies. In the context of eIDAS2 the NCCA is responsible for the development of the certification system. In this project the Belgian NCCA will act as the national SPOC, and will participate in WP1, and in WP3 as the Leader. FOD BOSA, as wallet provider, will participate in WP2. FOD IBZ, as PID provider, will participate in WP3.

**CZ:** ARICOMA (Aricoma Digital s.r.o) participated on developed the Czech eWallet prototype, eDoklady, and focuses on identity and access management. It acts as a technical consultant and coordinator for Czechia with close links to the public ministries competent in digital identity. They will provide contribution to WP1 through WP4. DIA (Digital and Information Agency) is a public institution that drives digital transformation of Czech entities and operates the Czech eWallet prototype (eDoklady). EZU

**(Electrotechnical Testing Institute)** offers the services of the accredited testing laboratory and the certification body for products and management systems and the accredited metrological laboratory. It is the authorized body no. 201. They are commissioned to carry out tests of motor vehicles, their systems, parts and separate technical units in accordance with EC technical regulations. They are a state-owned company established in accordance with Act no. 77/1997 Coll. on State-Owned Companies. Our founder is the Czech Ministry of Industry and Trade. They are engaged in the execution of public testing activities in accordance with Act no. 90/2016 Coll. on Technical Requirements for Products and the amendments of certain acts, in the scope defined by the authorization of the Czech Office for Standards Metrology and Testing. **Tayllorcox s.r.o.** will serve as the dedicated Certification and Training Partner within the consortium. Leveraging its accreditation as a Registered Certification Body (RCB) and Conformity Assessment Body (CAB) for eIDAS-trust services, Tayllorcox will participate on the development and execution of the audit and certification framework for the digital identity wallet ecosystem. By combining certification, audit methodology and capacity-building services, Tayllorcox helps to ensure that the project's outputs (certified wallets) are not only technically compliant but embedded in a sustainable assurance ecosystem across Europe.

**EE:** Estonian **Ministry of Justice and Digital Affairs (JDM)** is the national SPOC for this Consortium. The JDM is in charge of coordinating national efforts around the EUDI Wallet, writing national legislation related to the eIDAS2 Regulation or its Implementing Acts, providing EUDI Wallet, and is the owner of the **EUDI Wallet national certification scheme**. The JDM will participate in WP1, WP2, WP3, WP4.

**ES:** From Spain, **UC3M** will act as the coordinator of all activities dealing with Spanish partners, as well as national coordination with other actors, outside of the project partners (e.g., Wallet provider, PID providers, etc.). This means that in addition to the work in WP1, it will also have a minor participation in WP2 and WP3. UC3M will be also a major partner in WP5, as its Principal Investigator, Prof. Raul Sanchez-Reillo, is one of the most relevant players in the field of standardization, not only in ISO/IEC, but also in ETSI and CEN, holding the co-convenorship of CEN TC224 WG20 on "European Digital Identity Wallets". CCN is the Spanish NCCA and the responsible for the national certification scheme. Its participation in WP1, WP2 and WP3 will bring a high and positive impact to the project. Two of the Spanish CABs, **A+LGAI** and **DEKRA**, participate in the project in WP3.

**GR:** The **National Infrastructures for Research and Technology (GRNET)** is in charge of developing the Greek National Wallet. It will be working as a WP4L and within WP1 as a Wallet Provider. Additionally, **MoDG** will take part in the Consortium work as well. Finally, **QMCERT** will act as a Greek CABs for the certification topics.

**HR: Ministry of Justice, Public Administration and Digital Transformation** acting as the national SPOC and the issuer of Croatian EUDI Wallet, will participate in WP1 contributing to the governance of the project and monitoring and reporting on the progress of the development status of national wallet initiative, and WP3, developing national and establishing joint certification scheme.

**HU:** On the Hungarian side, **Idomsoft Ltd.**, the 100% state-owned development organization developing and providing the national solution of the EU digital wallet (as spoc), as well as the national authority responsible for certification, the **National Media and Communications Authority**, and the trusted service provider responsible for critical infrastructure, the **National Infocommunication Service Provider Ltd.**, are joining the joint work. Idomsoft Zrt. is participating in WP1 and WP3, and the National Media and Communications Authority and the National Infocommunication Service Provider Ltd. are participating in WP3. Idomsoft Ltd. is the largest state development company in addition to its tasks related to the EU digital wallet. Idomsoft develops and operates most of the large state public registers and is responsible for cross-border services. It is also the developer and implementer of the Digital Citizenship Program.

**IT:** Italy contributes through a broad consortium reflecting its multi-stakeholder wallet ecosystem. The Department for Digital Transformation of the Italian Presidency of the Council of Ministers (PDCM-DTD), acting as the Single Point of Contact for all Italian beneficiaries, will participate in WP1, ensuring coordination across all work packages. PagoPA S.p.A., as the national public wallet provider responsible for developing and operating the public IT-Wallet, will participate in WP1 and WP4, supporting the definition of technical specifications and contributing to the support package for wallet deployment. Istituto Poligrafico e Zecca dello Stato (IPZS), as the national PID provider, will participate as observer in WP3, contributing expertise in identity attributes and high-assurance processes. The Agenzia per la Cybersicurezza Nazionale (ACN), acting as Italy's National Cybersecurity Certification Authority (NCCA), will participate in WP3 and will co-lead Task 3.4 (Cybersecurity Certification of EUDI Wallet), bringing expertise in security governance, Common Criteria certification, and alignment with national and EU-level certification frameworks. ACN is already coordinating the development of the national EUDIW-IT certification scheme, working closely with DTD. The private wallet providers, namely Namirial, InfoCert, Aruba (with its affiliated entity Aruba Software) and

Intesi Group, will participate across multiple work packages. These entities are established Qualified Trust Service Providers and will become accredited private wallet providers under the Italian hybrid ecosystem, alongside the public solution. They will contribute to sandbox testing (WP2), support activities (WP4), and standardisation efforts (WP5). Fondazione Bruno Kessler (FBK), a leading research institution in cybersecurity with over a decade of experience in digital identity solutions, will participate in WP5 (Trustiness). FBK has been working closely with ACN and PagoPA on the Italian wallet security architecture and certification scheme, and will contribute to tasks on Relying Party Authorization, Wallet Trust Anchor Framework, and zero-knowledge technologies. ANAC, the Italian National Anti-Corruption Authority responsible for oversight and regulation of public procurement in Italy, will participate in WP1 as a Trust Provider, with a focus on governance aspects and potential future involvement in e-procurement use cases. Politecnico di Milano (PoliMi) will lead a dedicated task within WP1, contributing to the monitoring of national wallet initiatives through the design and development of an interactive dashboard that will support continuous assessment and cross-country comparison throughout the project lifecycle.

**LT:** Lithuania participates through the Ministry of the Economy and Innovation (**EIMIN**) and the State Digital Solutions Agency (**SDSA**), with SDSA acting as the national SPOC. The Lithuanian partners contribute to WP1, WP2 and WP3.

**LU:** Luxembourg participates with only one entity, the **Ministry for Digitalisation**, in WP3 on Certification. The status is Associated Partner. The Ministry is in charge of coordinating national efforts around the EUDI Wallet, writing national legislation related to the eIDAS2 Regulation or its Implementing Acts, and is the owner of the EUDI Wallet national certification scheme.

**LV:** The **Latvian State Digital Development Agency (VDAA)**, acting as the national SPOC and the issuer of the Latvian EUDI Wallet, will participate in WP1 and WP2, contributing with technical governance, coordination and implementation leadership. The **Ministry of Defence (MoD)** will contribute specialised cybersecurity expertise within WP3, ensuring the alignment of the solution with high-assurance security. Together, the partners provide complementary capabilities essential for a secure and interoperable wallet deployment.

**MD:** The **Moldovan e-Governance Agency (MEGA)**, in its capacity of National Wallet Provider responsible for coordinating national activities related to wallet deployment and interoperability, participates in the consortium as a Beneficiary. In this project MEGA will act as Single Point of Contact (SPOC) for Moldova and will contribute to WP1 (Governance), WP2 (Sandbox), and WP4 (Support), ensuring alignment with the Architecture and Reference Framework (ARF) and facilitating the reuse of open-source solutions for national implementation.

**MT:** The **Malta Digital Innovation Authority (MDIA)**, is a Public Body acting as a SPOC for Malta and is also designated as the Maltese EUDI Wallet Provider and Access Certificate Authority. The MDIA will participate in WP1, WP2, WP3, and WP5. The **Malta Communication Authority (MCA)** is the designated Scheme owner and NCCA, as well as the supervisory authority for trust services and the wallet. The MCA will participate in WP1, WP2, WP3 and WP5.

**NL:** The **Dutch Foundation ICTU** host the bureau Large Scale Pilots which facilitates and coordinates WPs wide multiple partner in various roles in LSPs. Additionally, The **Ministry of the Interior and Kingdom Relations (BZK)** acts as Dutch Wallet Provider. Both entities will be working in WP1, while in WP3, there will be **RDI** acting as a NCCA and **Trust CB, SGS Brightsight, Keysight and FIME** that will be operating as CABs, working on certification.

**PL:** **Ministerstwo Cyfryzacji (MC)** along with **Centralny Ośrodek Informatyki (COI)** will participate as a national public Wallet Provider as they are responsible for mObywatel application- Polish eWallet. MC will participate in WP1 and WP3. COI will participate in WP1, WP2 and WP4.

**NIT** - the entity designated by the Minister of Digital Affairs to create Polish certification scheme for DI Wallet - will provide relevant contribution to WP3. The contribution will be based on experience gained by our expert during ENISA's projects on EUCC and EU5G cybersecurity certification schemes. Further, NIT is directly involvement in several standardization projects related to EUDI Wallet developed in CEN (TC224) and ETSI (Signature and Electronic Signature). Having long term experience in international and European standardization in the field of cybersecurity, NIT will contribute to WP5 regarding fulfilling identified standardization gaps and contributing to projects which are already in development. Moreover, NIT will participate in WP1 and WP3.

**NASK-PIB** (Research and Academic Computer Network): National Research Institute under the supervision of the Polish Ministry of Digital Affairs. It facilitates the development of ICT networks' cybersecurity. NASK-PIB is a highly specialized department dedicated to cybersecurity certification and standardisation efforts. NASK-

PIB's Certification Body is accredited by the Polish National Accreditation Body (PCA) and is managed in compliance with ISO/IEC 17065 (Conformity Assessment Body standard, CAB). NASK-PIB will participate in WP2 and WP3.

**PT:** The **State Technological Reform Agency (ARTE)** is a public institute responsible for directing, coordinating, and executing the technological transformation and digitalization of Public Administration in Portugal, including interoperability and digital identity. It is responsible for the ongoing development of the EUDIW, which is being built upon the national eID wallet GOV.pt, also developed and provided by the Agency. ARTE is enrolled in all WPs as the SPOC for the Portuguese participation in this consortium, which also includes the **National Cabinet of Security (GNS)** who will participate in WP3 as Supervisory Body on Trust Service (tasks related with the trust services of the QTSP in the Portuguese market) and the **Portuguese Certification Association (APCER)** with its affiliated entity **APCER SA**, two private entities who will participate in WP3 as Conformity Assessment Bodies (CAB).

**RO:** **ADR** (Autoritatea Pentru Digitalizarea Romaniei) and **MAI** (Ministry of Internal Affairs) will take part in WP1. ADR will be acting as a SPOC, while MAI is the national PID Provider. and is in charge of the wallet development. while **DNSC** acting as the NCCA in Romania and **RENAR** acting as a NAB will both take part in WP3.

**SE:** The **Agency for Digital Government (DIGG)** is responsible for developing the Swedish national wallet and for developing the national certification scheme for the wallet, thus in effect acting as NCCA for Sweden regarding EUDIW. DIGG has established cooperation with the Swedish Defence Materiel Administration that is responsible for cybersecurity certification in Sweden, the national accreditation body Swedac and the Swedish Police that is tasked with developing the national e-ID. Part of the work will be made in cooperation with these agencies. As Sweden has an open market model concerning CABs, DIGG has invited Swedish CABs with the required competencies to join the project and two of these; **Atsec** and **Rise**, have chosen to join the pilot.

**SI:** The **Ministry of Digital Transformation (MDT)** plays multiple roles in the EUDIW ecosystem because it oversees various activities under its umbrella. Within the SI-TRUST (Trust Services Authority of Slovenia), which is part of MDT, it acts as an EUDIW provider, a PID provider, and a provider of other trust services. In another directorate with separate roles, MDT serves as the owner of the national certification scheme for EUDIW. Regarding the national certification scheme for EUDIW, MDT also coordinates with URSIV, which is the Slovenian NCCA. The technical implementation and development of EUDIW for MDT's needs is carried out by the company **SETCCE**, which is also a member of the consortium. MDT and SETCCE will therefore collaborate on activities related to wallet provisioning (WP1), ensuring compliance (WP2), providing necessary information and explanations for establishing the national scheme (WP3), and also as potential users of the developed EUDIW components (WP4). Additionally, MDT, in its role as the scheme owner, will actively work on establishing the national certification scheme, which will be based on the common certification system (WP3). **SIQ** has expressed interest in performing the EUDIW conformity assessment, as it is also the conformity assessment body for trust services under eIDAS. Therefore, SIQ is included in the consortium as a CAB in WP3. MDT will also take the role of SPOC for Slovenian partners. **University of Maribor** intention is to provide open source SW components for re-use within WP4.

**SK:** **National Security Authority** will participate in WP2 in the role of national contact point for wallet providers. NSA will be responsible for guiding wallets providers through the testing process towards certification. NSA will also participate in WP3 in order to prepare the National Cybersecurity Certification Authority for adoption of the European Digital Identity Wallet (EUDI Wallet). This will entail training of the relevant personnel on the subject matter of the European Digital Identity Wallet (EUDI Wallet) and establishment of **national certification schemes**. Also, national CAB will be established within WP3 (In accordance with Slovak Law No. 69/2018 on cyber security, only the NSA's Certification Authority can be an accredited certification body for cyber security certification at the high assurance level. Part of these tasks will be delegated (through subcontracting) to body, which is appointed by law, namely UNMS (Slovak Office of Standards, Metrology and Testing) which is responsible for methodology and practical management of processes of adoption of technical norms in Slovakia. It entails translation, quality check including involvement.

**UA:** **Ministry of Digital Transformation of Ukraine (MDTU)** participates in the consortium as a main regulator responsible for harmonisation of the eIDAS 2.0 requirements in Ukraine, in the status of the Associated Partner. State Enterprise Diia is participating as the wallet provider and PID provider, in the status of the beneficiary. There are no CABs in Ukraine that operate in the sphere of eID and trust services.

<b>Project teams and staff</b>		
<p>Describe the project teams and how they will work together to implement the project.</p> <p>List the staff included in the project budget (budget category A) by function/profile (e.g. project manager, senior expert/advisor/researcher, junior expert/advisor/researcher, trainers/teachers, technical personnel, administrative personnel etc. — use the same profiles as in the detailed budget table, if any (<i>n/a</i> for prefixed Lump Sum Grants)) and describe briefly their tasks.</p>		
Name and function	Organisation	Role/tasks/professional profile and expertise
<b>WP1 – Leads</b>		
<b>Florent TOURNOIS</b> Head of overall coordination	<b>FR: ANTS</b>	Overall and administrative coordination; reporting and submission of deliverables to EC; monitor that the action is implemented properly; meetings and coordination of WP1 activities
<b>Philippe NIETO</b> Deputy head of overall coordination and FR SPOC	<b>FR: ANTS</b>	Day-to-day project management; meetings and coordination of WP1 activities. Continuous management of monitoring and quality assurance activities; follow-up with participants on monitoring and evaluation responsibilities; submissions consolidation from other participants and dashboard maintaining; updates preparing for Steering Committee and Board of Beneficiaries meetings. Overall risks management. Animation and coordination of the French partners ecosystem.
<b>Leïla SAIDI</b> FM Officer	<b>FR: CIVIPOL</b>	Management of EU funds for the project, reporting to the head of overall coordination, kick-off meeting organization
<b>POLIMI</b>	<b>IT: POLIMI</b>	Monitoring and analysis of the current status and trends of EUDIW issuance and certification across EU Member States through desk research, data collection, and stakeholder interviews; preparation of analytical reports and development of visualization tools to support continuous monitoring and evidence-based insights, leveraging academic expertise in policy evaluation, comparative research, and data analysis.
<b>WP2 – Leads</b>		
<b>Anthony CARMOY</b>	<b>FR: ANTS</b>	In charge of leading WP2 and supporting the delivery of the sandbox. Overall coordination and liaison with all stakeholders
<b>WP3 – Leads</b>		
<b>Johan KLYKENS</b> Head of NCCA Belgium	<b>BE: CCB</b>	Certification scheme coordination, criteria definition oversight, harmonisation facilitation, interaction with authorities.
<b>Chris DE VUYST</b> Senior Certification Expert	<b>BE: CCB</b>	Certification scheme coordination, criteria definition oversight, harmonisation facilitation, interaction with authorities.
<b>Dorien STEVENS</b> Project manager	<b>BE: CCB</b>	Coordination of the activities at the national level, supporting the implementation of Work Package 3 and reporting progress and outcomes to the project coordinator.
<b>WP4 – Leads</b>		
<b>Panos LOURIDAS</b>	<b>EL: GRNET</b>	In charge of leading WP4 and supporting the delivery of expected MiS/deliverables. Overall coordination and liaison with all stakeholders
<b>WP5 – Leads</b>		
<b>Raul SANCHEZ REILLO</b>	<b>ES: UC3M</b>	In charge of leading WP5 and supporting the delivery of expected MiS/deliverables. Overall coordination and liaison with all stakeholders

**Outside resources (subcontracting, seconded staff, etc)**

*If you do not have all skills/resources in-house, describe how you intend to get them (contributions of members, partner organisations, subcontracting, etc.) and for which role/tasks/professional profile/expertise*

*If there is subcontracting, please also complete the table in section 4.*

WP1: Outside resources will be used by ANTS, Ministry of Justice and Digital Affairs, MJPADT, MDIA, COI, DIGG and MDT, for:

- Project management and reporting support
- Wallet provision as a service
- Specialist expertise in eIDAS, trust infrastructure, certification and standards
- Core expertise to complement internal capability gaps

WP2: Outside resources will be used by ANTS, Ministry of Justice and Digital Affairs, MCA, MDIA, COI, DIGG and MDT for:

- Wallet provision as a service, procured via public procurement
- Testing activities, including compliance and PEN testing
- Interoperability validation
- Wallet certification activities
- Core expertise to complement internal capability gaps
- Scheme design and certification expertise
- Provision of Sandbox expected for the project tests

WP3: Outside resources will be used by the Ministry of Justice and Digital Affairs, MoDG, MCA, DIGG and MDT for:

- Certification-related activities outsourced, due to the absence of local NAB/CAB/CBs
- National certification scheme (NCCA) development
- Expertise in eIDAS, certification and standards
- Scheme design and conformity assessment expertise

WP4: Outside resources will be used by ANTS

- Support related to SDKs development for the modular solutions

WP5: Not concerned

**Consortium management and decision-making (if applicable)**

*Explain the management structures and decision-making mechanisms within the consortium. Describe how decisions will be taken and how regular and effective communication will be ensured. Describe methods to ensure planning and control.*

**Note:** The concept (including organisational structure and decision-making mechanisms) must be adapted to the complexity and scale of the project.

The management structure of the EUDIW PACT project is designed to be **simple, efficient, and proportionate** to the scope and objectives of the action, while taking into account the number of partners involved and the diversity of sectors represented in the consortium.

The Consortium Agreement (CA) establishes clear and transparent guidelines covering roles and responsibilities, governance principles, decision-making processes, and procedures for implementing changes where necessary. It also defines provisions related to participant inclusion or exclusion, liabilities and duties of the parties involved, and financial arrangements. This ensures a shared understanding among all partners while keeping administrative requirements to a minimum.

Overall coordination and project management are ensured through **Work Package 1 (WP1)**, led by **FR**, with **ANTS** acting as **Chief Operating Officer (COO)** and **CIVIPOL supporting financial management**. WP1 is responsible for the day-to-day management and smooth operation of the project, including:

- Monitoring progress against the agreed roadmap
- Supporting participating Member States and other partners
- Monitoring risks and mitigation measures
- Ensuring that appropriate project management and collaboration tools are available

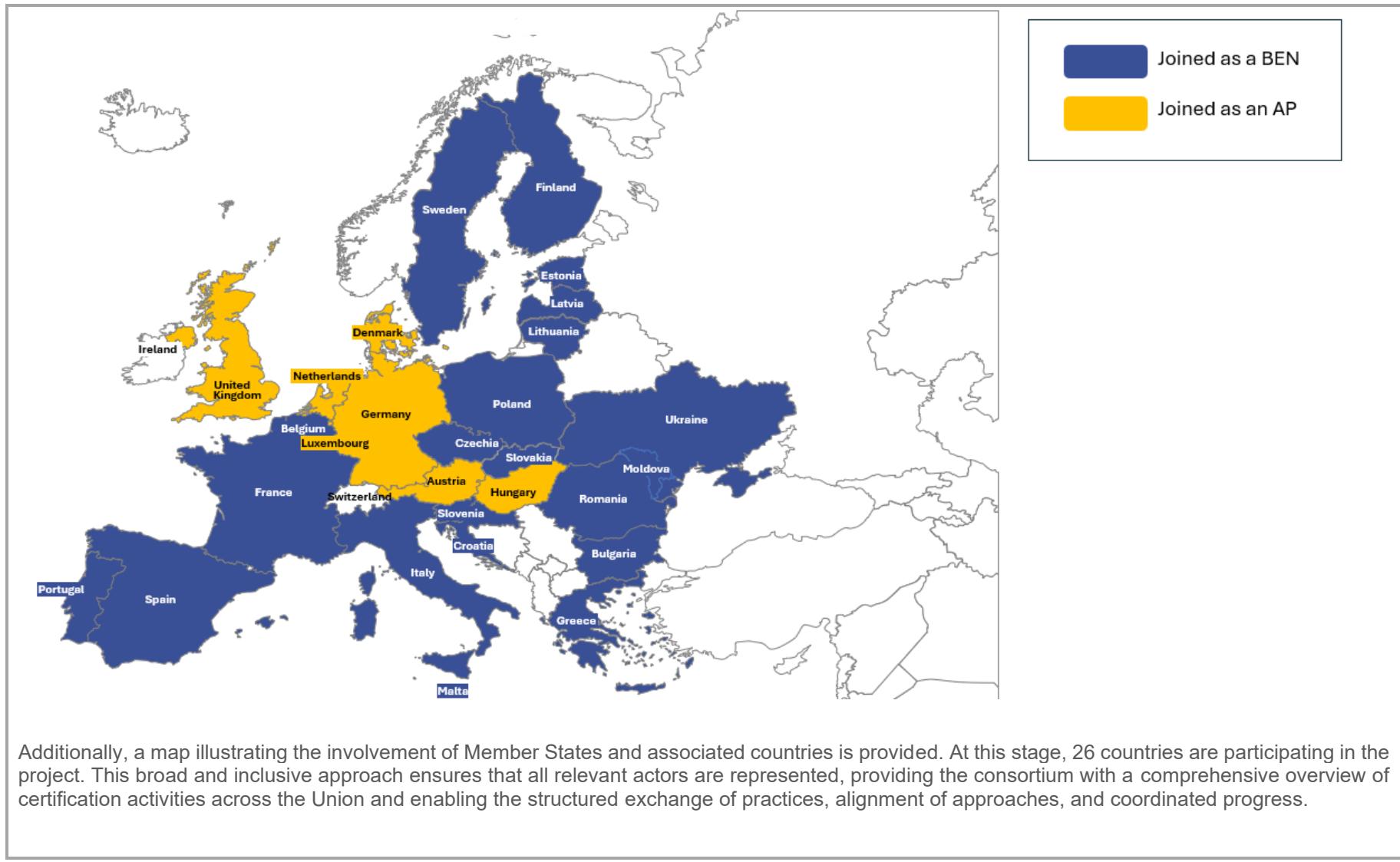
Decision-making within the consortium follows a **collaborative and consensus-based approach**. Key project decisions are discussed during regular coordination meetings involving the relevant partners and Member State representatives. This approach ensures that all partners can contribute to decisions affecting their activities, while avoiding the creation of heavy governance bodies.

Regular and effective communication is ensured through periodic online meetings, written updates, and shared access to project documentation. Planning and control are based on the agreed work plan, milestones, and deliverables, allowing progress to be monitored efficiently and adjustments to be made when needed, in line with the project's scale and complexity.

Member States (and countries) contribute according to their expertise and level of involvement in specific project activities. Additionally, each entity is assigned to different tasks and different Work Packages based on their roles (e.g. Wallet Providers within WP1, NCCAs and CABs within WP3, etc). The roles and contributions of each Member State are clearly described in a dedicated table, available below:

	WP1 Governance	WP2 Sandbox	WP3 Certification	WP4 Support	WP5 Trustiness
FRA – France	Lead	Lead	X		
AT – Austria			X		
BEL – Belgium	X	X	Lead		
CZE – Czech Republic	X	X	X		
DE – Germany	X				
DNK – Denmark	X		X		
EST – Estonia	X	X	X		
ESP – Spain	X	X	X		Lead
FIN – Finland	X		X		
GRC – Greece	X		X	Lead	
HRV – Croatia	X		X		
HUN – Hungary	X		X		
ITA – Italy	X	X	X		
LTU – Lithuania	X	X	X		
LU – Luxembourg	X		X		
LVA – Latvia	X	X	X		
MD – Moldova	X	X			
MLT – Malta	X	X	X		
NLD – Netherlands	X		X		
POL – Poland	X	X	X		
PRT – Portugal	X	X	X		
ROM – Romania	X				
SVN – Slovenia	X	X	X		
SVK – Slovakia	X	X	X		
SWE – Sweden	X	X	X		
UKR – Ukraine	X	X	X		

\*For WP4, the Consortium will be able to take part of WP4 following solicitations the envelope



#\$CON-SOR-CS§# §§QUA-LIT-QL§# #@IMP-ACT-IA@# @@COM-DIS-VIS-CDV@#

### 3. IMPACT

#### 3.1 Expected outcomes and deliverables — Dissemination and communication

##### Expected outcomes and deliverables

*Define and explain the extent to which the project will achieve the expected impacts listed in Call document.*

The project will deliver a focused and coherent set of outcomes that support Member States in meeting their obligation under the eIDAS 2.0 Regulation to make an EU Digital Identity Wallet available by the end of 2026. The project acts as an **enabler and accelerator**, fostering close cooperation between Member States, the European Commission, wallet providers and certification actors, and supporting them through the final steps towards issuance and certification.

A primary expected outcome is the **establishment and operationalization of joint certification approaches** for EU Digital Identity Wallets or wallet modules. In close cooperation with national authorities, accreditation bodies and Conformity Assessment Bodies (CABs), the project will support the definition, alignment and practical application of national certification schemes, contributing to harmonisation, mutual recognition and reduced fragmentation across the Union.

The project will further support **modular wallet solutions and their supporting services**, aligned with the Architecture and Reference Framework (ARF) and relevant implementing acts. Through sandboxing, pre-conformance activities and coordinated testing, Member States and wallet providers will be supported in progressing towards compliance while retaining flexibility in national implementation choices.

By December 2026, the project aims to **support the certification of at least one EU Digital Identity Wallet**, serving as a concrete proof point for the feasibility of certification within the regulatory timeframe. In a subsequent phase, the governance, processes and technical enablers established by the project will facilitate the certification of additional wallets, extending the impact beyond the initial milestone.

Overall, the project's main outcome is to provide **practical support, coordination and confidence** to Member States facing the 2026 deadline. By aligning certification practices, enabling cooperation and reducing implementation risks, the project contributes to trust, interoperability and readiness of the EU Digital Identity Wallet ecosystem, while leaving long-term ownership and operation with the Member States.

##### Dissemination and communication of the project and its results

*If relevant, describe the communication and dissemination activities, activities (target groups, main messages, tools, and channels) which are planned in order to promote the activities/results and maximise the impact. The aim is to inform and reach out to society and show the activities performed, and the use and the benefits the project will have for citizens. Clarify how you will reach the target groups, relevant stakeholders, policymakers and the general public and explain the choice of the dissemination channels.*

*Describe how the visibility of EU funding will be ensured.*

 *In case your proposal is selected for funding, you will have to provide a more detailed plan for these activities (dissemination and communication plan), within 6 months after grant signature. This plan will have to be periodically updated; in line with the project progress.*

The dissemination and communication activities of the project will be proportionate to its scope and objectives and will mainly rely on existing EUDIW LSPs, national EUDI Wallet initiatives, and the established communication channels of the participating organizations. The overall objective is to inform relevant stakeholders, policymakers, and the broader EUDI Wallet ecosystem about the project activities and results, and to demonstrate the value of EUDI Wallet certification in terms of trust, security, interoperability, and usability for citizens and service providers. Regular updates on the progress of the project will be shared through these existing channels as the work advances.

The project will not set up extensive standalone communication actions to citizens, as the focus is not on use cases but on development, certification and conformity. Dissemination will instead take place through ongoing LSP and national initiative activities, stakeholder and expert networks, and participation in relevant coordination meetings, workshops, and events at national and EU level. These channels are well suited to reach wallet providers, public authorities, and other key actors already involved in the deployment of the European Digital Identity framework. Where appropriate, short written updates or contributions may be shared through existing websites, newsletters, or event materials to report on milestones, intermediate results, and lessons learned.

The visibility of EU funding will be ensured in line with EU communication requirements by clearly acknowledging EU support and displaying the EU emblem on any public project material, presentations, or written outputs, as well as in communications carried out through LSPs and national initiatives when referring to the project. In case the proposal is selected for funding, a more detailed dissemination and communication plan will be provided within six months after grant signature and will be periodically updated to reflect the progress of the project and emerging dissemination opportunities.

#SCOM-DIS-VIS-CDV\$#

### 3.2 Competitiveness and benefits for society

#### Competitiveness and benefits for the society

*Describe the extent to which the project will strengthen competitiveness and bring important benefits for society*

The proposed initiative will significantly strengthen the competitiveness of the European Union's digital identity industry and bring tangible benefits to European society, particularly to citizens and public administrations. By focusing on the certification, testing, and large-scale deployment of secure and interoperable EUDI Wallets, the project contributes directly to the European Commission's **Digital Decade targets** and supports the creation of a sovereign, trusted, and user-centric digital identity infrastructure across the Union.

##### Strengthen competitiveness:

At the European level, the project enhances the **strategic and technological competitiveness** of Member States by consolidating common frameworks for certification, testing, and interoperability. Through the creation of joint certification schemes and a shared conformity testing environment, the initiative establishes a **level playing field** for wallet providers and Conformity Assessment Bodies (CABs), ensuring that European actors can compete and innovate within a harmonised regulatory and technical landscape.

By reducing fragmentation between national approaches, the project facilitates **cross-border scalability** and **mutual recognition** of certified wallets, thereby opening opportunities for both public and private stakeholders. Wallet providers, cybersecurity experts, and SMEs will be able to develop, validate, and deploy their solutions across several Member States without facing redundant certification processes. This will lower costs, shorten time-to-market, and stimulate innovation within the European digital identity and cybersecurity industries.

In addition, the project reinforces Europe's **technological sovereignty** by ensuring that critical components of the EUDI Wallet ecosystem—testing infrastructures, certification schemes, and interoperability frameworks—are developed and governed under European control. In an international context where major non-European actors are entering the digital identity domain, Europe's ability to establish its own secure, standardized, and certified solutions becomes a decisive competitive advantage. The

initiative therefore supports the EU's strategic autonomy, strengthens the resilience of its digital infrastructure, and positions Europe as a global reference for trustworthy digital identity management.

**Benefits for society:**

Beyond its economic and strategic dimensions, the project delivers essential benefits for European citizens and society at large. By establishing the technical and governance foundations for certified and interoperable wallets, the project ensures that citizens will gain access to **trusted, privacy-preserving, and user-controlled digital identity solutions**. This will simplify access to online public and private services, enhance security against identity theft and fraud, and provide greater control over personal data in compliance with the **General Data Protection Regulation (GDPR)**.

The project also promotes **inclusiveness and cohesion** across the Union. By supporting Member States with varying levels of readiness, it ensures that all citizens—regardless of their country of residence—can benefit from the same level of trust, security, and interoperability. This approach helps reduce the digital divide and reinforces the sense of a shared European identity.

Finally, by fostering transparency, accountability, and collaboration between governments, CABs, and technology providers, the project strengthens **citizens' trust** in public digital services. The deployment of certified EUDI Wallets will make digital interactions more secure, efficient, and transparent, while preserving fundamental rights and European values.

Through these combined impacts, the project not only enhances Europe's competitiveness in the digital identity sector but also ensures that its citizens enjoy the concrete benefits of a **secure, inclusive, and sovereign digital society**, where trust, interoperability, and innovation advance together in the European public interest.

### 3.3 Environmental sustainability and contribution to European Green Deal goals

**Environmental sustainability and contribution to European Green Deal goals**

*Describe the extent to which the project will contribute to environmental sustainability and in particular to European Green Deal goals*

 *This might not be applicable to all topics — for details refer to the Call document.*

N/A

#\$IMP-ACT-IA\$#

#@WRK-PLA-WP#@#

## 4. WORK PLAN, WORK PACKAGES, ACTIVITIES, RESOURCES AND TIMING

### 4.1 Work plan

#### Work plan

*Provide a brief description of the overall structure of the work plan (list of work packages or graphical presentation (Pert chart or similar)).*

The work plan is structured into **five interlinked work packages**, designed to run partly in parallel and converge towards a **common milestone: supporting the certification of at least one EU Digital Identity Wallet by December 2026**, in line with the expectations of the European Commission. The structure reflects the natural progression from wallet development, to testing, and finally to certification, while providing continuous coordination and support.

- **WP1 – Governance**

WP1 establishes the overall governance and coordination framework and brings together Member States, wallet providers, certification actors, and the European Commission, ensuring alignment with implementing acts, the ARF, and EU governance structures. Beyond governance, WP1 actively structures and steers the technical and operational contributions of wallet providers, including the translation of regulatory requirements into development roadmaps and the coordination of dependencies with testing and certification activities. The European Commission acts in an advisory role, providing strategic guidance and regulatory clarification to support coherent implementation and risk mitigation across wallet development activities.

- **WP2 – Sandbox**

WP2 provides a sandbox environment where wallet solutions developed by providers involved in WP1 can be tested in realistic conditions. It supports pre-conformance and technical testing of issuance, presentation and signature functionalities, using Commission test artefacts and aligned test scenarios. This work package acts as the bridge between development and certification by identifying gaps and ensuring readiness for formal assessment.

- **WP3 – Certification**

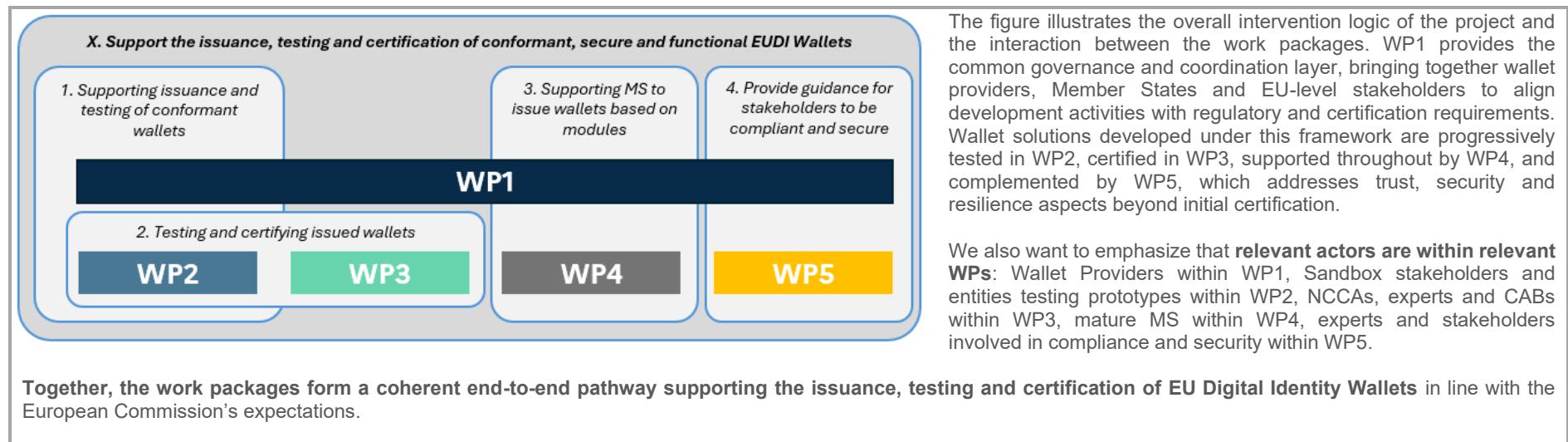
WP3 supports the execution of wallet certification, in close cooperation with national authorities and Conformity Assessment Bodies. It builds on the results of WP2 to enable conformity assessments under national certification schemes and supports their practical implementation. WP3 is the focal point for achieving the certification of at least one EU Digital Identity Wallet by December 2026, and additional ones further on.

- **WP4 – Support**

WP4 provides continuous technical and procedural support across all project phases, assisting wallet providers, Member States, and certification actors throughout development activities. It proactively addresses technical and procedural issues, facilitates cross-stakeholder coordination, and mitigates risks that could otherwise delay progress towards the shared implementation deadline.

- **WP5 – Trustiness**

WP5 addresses trust, security and resilience aspects of the EUDIW in the context of evolving technical and legal background. It complements WP3 by focusing on forward-looking topics beyond initial certification, including interactions with relying parties and emerging technical requirements critical for maintaining LoA high. WP5 provides guidance and shared interpretations to support consistent, mature and trustworthy implementations across Member States and ecosystem actors.



## 4.2 Work packages, activities, resources and timing

<b>Objectives</b> List the specific objectives to which the work package aims to achieve.
<b>Activities and division of work (WP description)</b> Provide a concise overview of the work (planned tasks). Be specific and give a short name and number for each task. Show who is participating in each task: Coordinator (COO), Beneficiaries (BEN), Affiliated Entities (AE), Associated Partners (AP), indicating <b>in bold</b> the task leader. Add information on other participants' involvement in the project e.g. subcontractors, in-kind contributions. <b>Note:</b> In-kind contributions: In-kind contributions for free are cost-neutral, i.e. cannot be declared as cost. Please indicate the in-kind contributions that are provided in the context of the work package. The Coordinator remains fully responsible for the coordination tasks, even if they are delegated to someone else. Coordinator tasks cannot be subcontracted. If there is subcontracting, please also complete the table below.
<b>Milestones and deliverables (outputs/outcomes)</b> Milestones are control points in the project that help to chart progress (e.g. completion of a key deliverable allowing the next phase of the work to begin). Use them only for major outputs in complex projects, otherwise leave the section empty. Please limit the number of milestones by work package. Means of verification are how you intend to prove that a milestone has been reached. If appropriate, you can also refer to indicators. Deliverables are project outputs which are submitted to show project progress (any format). Refer only to major outputs. Do not include minor sub-items, internal working papers, meeting minutes, etc. Limit the number of deliverables to max 10-15 for the entire project. You may be asked to further reduce the number during grant preparation. For deliverables such as meetings, events, seminars, trainings, workshops, webinars, conferences, etc., enter each deliverable separately and provide the following in the 'Description' field: invitation, agenda, signed presence list, target group, number of estimated participants, duration of the event, report of the event, training material package, presentations, evaluation report, feedback questionnaire. For deliverables such as manuals, toolkits, guides, reports, leaflets, brochures, training materials etc., add in the 'Description' field: format (electronic or printed), language(s), approximate number of pages and estimated number of copies of publications (if any).

For each deliverable you will have to indicate a due month by when you commit to upload it in the Portal. The due month of the deliverable cannot be outside the duration of the work package and must be in line with the timeline provided below. Month 1 marks the start of the project and all deadlines should be related to this starting date.

The labels used mean:

Public — fully open (⚠ automatically posted online on the Project Results platforms)

Sensitive — limited under the conditions of the Grant Agreement

EU classified — RESTREINT-UE/EU-RESTRICTED, CONFIDENTIEL-UE/EU-CONFIDENTIAL, SECRET-UE/EU-SECRET under Decision [2015/444](#). For items classified under other rules (e.g. national or international organisation), please select the equivalent EU classification level.

## Work Package 1

Work Package 1: Governance			
Duration:	M1 – M24	Lead Beneficiary:	ANTS
<b>Objectives</b>			
WP1 aims to ensure the effective governance, coordination, and support of all project partners, with a particular focus on wallet providers, while facilitating smooth project management, compliance, and certification processes. It provides the foundational structures necessary for the successful delivery of the EUDIW PACI project, ensuring alignment with European Commission expectations and the overall project roadmap. The main objectives of WP1 are to: <ul style="list-style-type: none"><li>Establish a clear governance and coordination framework for all wallet providers and relevant stakeholders. This includes defining roles, responsibilities, decision-making processes, and communication channels to ensure transparency, alignment, and efficient collaboration throughout the project lifecycle.</li><li>Support wallet providers in their development and compliance activities, offering guidance on technical prerequisites, best practices, and requirements to achieve conformity. WP1 will facilitate readiness for sandbox testing (WP2) and certification (WP3), ensuring that all wallets meet the defined standards and quality benchmarks.</li><li>Coordinate knowledge exchange and collaboration among project partners, the two LSPs (APITUDE and WE BUILD), the EDICG, and the European Commission. Structured feedback loops will link development, sandbox testing, and certification activities to accelerate progress and maximize impact.</li><li>Implement monitoring and observatory tasks, led by POLIMI, to track the state of play of all partners, identify challenges, and provide actionable insights. This ensures informed governance and timely interventions where needed.</li><li>Manage financial and administrative aspects of the project, including budget allocation, monitoring, and reporting, ensuring full compliance with European Commission regulations and project requirements.</li><li>Ensure timely reporting, quality assurance, and risk management, including the submission of deliverables and milestones, continuous monitoring of project progress, and proactive mitigation of risks to safeguard the project's outcomes.</li></ul> An Advisory Board gathering project stakeholders and representatives from the European Commission will allow stakeholders to share insights and state of play of the project.			

Activities and division of work (WP description)					
Task No (continuous numbering linked to WP)	Task Name	Description	Participants		In-kind Contributions and Subcontracting (Yes/No and which)
			Name	Role (COO, BEN, AE, AP, OTHER)	
T1.1	Project steering and management	Interface with the European Commission (HaDEA) on the administrative and financial aspects, manage changes in Grant and Consortium Agreements, follow-up regularly and ensure the project is progressing as expected.	ANTS (Lead) + contributors	AE	
T1.2	Collaboration with the European Commission and the LSPs	Set up regular feedback and open discussions meetings with representatives of the European Commission related to EUDIW (DGCONNECT). Additionally, organize regular meetings with Large Scale Pilots to explore the synergies of our use cases and learn from each other.	ANTS (Lead) + contributors	AE	
T1.3	Financial management and reporting	Manage and monitor the project budget. Allocating European Commission funds to beneficiaries and affiliated entities according to the payment plan. Act as the primary contact for beneficiaries and affiliated entities and the European Commission regarding financial issues. Follow up with beneficiaries and affiliated entities on financial management and budget planning. Supervise the submission of financial reports by beneficiaries via the online portal.	CIVIPOL (Lead) + contributors	AE	
T1.4	Observatory and reporting task	Define monitors and report regularly the status and trends on EUDIW issuance and certification. Continuous follow-up and communication with stakeholders, partners and European Commission.	POLIMI	BEN	

T1.5	Wallet development and issuance from Member States	Continuous development of national Wallet issued by entities from Member States to reach conformity related to eIDAS 2 regulation. Related to continuous development, shared objective of reaching prototypes able to be tested and certified through other WPs. Evaluation of milestones reached by Member States and management of the associated incentive financial mechanism.	ANTS CIVIPOL	AE AE		
T1.6	Risks management, quality assurance, monitoring and evaluation	Continuously develop and monitor quality assurance, monitoring and evaluation, and project risks through Work Package Leaders. Prepare tools and templates for QA and M&E. Consolidate and visualize data regarding KPIs. Track the progress with the WPLs and identify work plan deviations. Raise relevant issues and set up risk management working sessions in Steering Committees to update the risk tracking and contingency plan.	ANTS (Lead) + contributors	AE		
<b>Milestones and deliverables (outputs/outcomes)</b>						
Milestone No (continuous numbering not linked to WP)	Milestone Name	Work Package No	Lead Beneficiary	Description	Due Date (month number)	Means of Verification
MS1	Launch of the project	1	ANTS	Ensuring all stakeholders and activities are ready to be launched	M2	Board of Beneficiaries 1
MS2	Issuance of a certified wallet	1	ANTS	Issuance of at least 1 certified wallet in line with the EC deadline	M11	Issuance of a solution certified
MS3	Closing of the project	1	ANTS	Ensuring all stakeholders and activities are finalized	M24	Board of Beneficiaries 3
Deliverable No (continuous numbering linked to WP)	Deliverable Name	Work Package No	Lead Beneficiary	Type	Dissemination Level	Due Date (month number)  Description (including format and language)

D1.1	Roadmap and sustainability strategy	1	ANTS	R — Report	SEN — Sensitive	M12	PDF doc, English Outlines a clear plan and long-term approach to ensure the adoption and continuation of EUDIW certification.
D1.2	Observatory – Reporting on MS State of play	1	POLIMI	R — Report	PU — Public	M20	PDF doc, English Monitors and reports on the current status and trends of EUDIW issuance certification across Member States.

Estimated budget — Resources										
Participant	Costs ( <i>n/a for Lump Sum Grants</i> )									
	A. Personnel	B. Subcontracting	C.1 Travel and subsistence	C.2 Equipment	C.3 Other goods, works and services	D.1 Financial support to third parties	D.2 Internally invoiced goods and services	D.3 PAC procurement costs <i>(for PAC Grants for Procurement )</i>	E. Indirect costs	Total costs
ANTS	84	€ 965,000	€ 400,000	€ 4,673					€ 109,877	€ 1,679,550
CIVIPOL	36	€ 235,000		€ 4,673		€ 2,000,000			€ 156,777	€ 2,396,450
INGroupe	10	€ 100,000							€ 7,000	€ 107,000
ARICOMA	20	€ 100,000		€ 4,673					€ 7,327	€ 112,000
Ministry of Justice and Digital Affairs	15	€ 75,000	€ 110,000	€ 4,673					€ 13,277	€ 202,950

A+LGAI				€ 4,673						€ 327	€ 5,000
CCN	10	€ 60,000		€ 4,673						€ 4,527	€ 69,200
DEKRA				€ 4,673						€ 327	€ 5,000
GRNET	25	€ 175,000		€ 4,673						€ 12,577	€ 192,250
MoDG	1	€ 3,200		€ 2,000						€ 364	€ 5,564
QMSCERT	0.2	€ 2,000		€ 2,000						€ 280	€ 4,280
MJPADT	16	€ 51,520	€ 60,000	€ 4,673						€ 8,134	€ 124,327
PagoPA	10	€ 41,667		€ 3,125						€ 3,135	€ 47,927
Namirial	2	€ 6,250								€ 438	€ 6,688
POLIMI	78	€ 276,120		€ 4,000		€ 1,000				€ 19,678	€ 300,798
ANAC	1	€ 6,250		€ 1,875						€ 569	€ 8,694
InfoCert	11	€ 54,000	€ 0	€ 3,125						€ 3,999	€ 61,124
Intesi Group	12	€ 71,250	€ 0	€ 3,125						€ 5,206	€ 79,581
EIMIN	20	€ 84,000		€ 4,673						€ 6,207	€ 94,880
SDSA	25	€ 150,000		€ 4,673						€ 10,827	€ 165,500
VDA	43	€ 184,900		€ 4,673						€ 13,270	€ 202,843
eGov Moldova	2	€ 8,400		€ 2,000						€ 728	€ 11,128
MDIA	27	€ 156,384	€ 25,000	€ 4,673						€ 13,024	€ 199,081
COI	6	€ 46,696	€ 18,650	€ 4,673						€ 4,901	€ 74,920
MC	6	€ 22,980		€ 4,673						€ 1,936	€ 29,589

NIT	15	€ 97,825		€ 4,673						€ 7,175	€ 109,673
ARTE	15	€ 75,000		€ 4,673						€ 5,577	€ 85,250
ADR	48	€ 105,600		€ 4,673						€ 7,719	€ 117,992
MAI	48	€ 96,000		€ 4,673						€ 7,047	€ 107,720
DNSC / NCCA				€ 4,673						€ 327	€ 5,000
DIGG	8	€ 86,400	€ 100,516	€ 4,673						€ 13,411	€ 205,000
MDT	3	€ 15,000	€ 40,000	€ 4,673						€ 4,177	€ 63,850
SETCCE	22	€ 132,000		€ 4,673						€ 9,567	€ 146,240
University of Maribor				€ 4,673						€ 327	€ 5,000
NSA	9	€ 74,000		€ 2,500		€ 12,500				€ 6,230	€ 95,230
Diia	43	€ 191,866								€ 13,431	€ 205,297
DSGV	10	€ 100,000								€ 7,000	€ 107,000
DVV	24	€ 186,000		€ 4,673						€ 13,347	€ 204,020
<b>Total</b>	705	€ 4,035,308	€ 754,166	€ 140,575		€ 2,013,500				€ 486,048	€ 7,429,597

For Lump Sum Grants, see detailed budget table/calculator (annex 1 to Part B; see [Portal Reference Documents](#)).

## Work Package 2

<b>Work Package 2: Sandbox</b>			
<b>Duration:</b>	M1 – M24	<b>Lead Beneficiary:</b>	ANTS

<b>Objectives</b>					
<p>WP2 is devoted to the definition, implementation, and operation of a common sandbox and testbed environment that will support Member States in testing, validating, and certifying their EUDI Wallet solutions. The WP ensures technical alignment, interoperability, and consistency across national implementations and modular wallet components. WP2 activities include the definition of common test cases, the setup of the test, and the provision of access and support services for Member States and stakeholders using the sandbox environment. The specific objectives that WP2 aims at are:</p> <ul style="list-style-type: none"> <li>• Definition of a common testing framework and methodology, including the design of shared test cases and conformance criteria aligned with the EUDI Wallet reference architecture, eIDAS ARF, and relevant implementing acts.</li> <li>• Establishment of a secure and scalable sandbox and testbed infrastructure providing simulation and interoperability testing capabilities.</li> <li>• Provision of access to the sandbox environment for Member States, enabling the validation of wallet implementations and modular wallet components.</li> <li>• Collection and reporting of test and compliance results to support continuous improvement and certification readiness of national solutions.</li> <li>• Technical support and guidance for Member States in conducting interoperability and conformance tests.</li> </ul>					
<b>Activities and division of work (WP description)</b>					
Task No (continuous numbering linked to WP)	Task Name	Description	Participants		In-kind Contributions and Subcontracting (Yes/No and which)
			Name	Role (COO, BEN, AE, AP, OTHER)	
T2.1	Definition of the testing framework and methodology	Development of the overall testing framework: methodology, conformance criteria, test scenarios and performance indicators	ANTS (Lead) + contributors	AE	
T2.2	Design and setup of the sandbox and testbed infrastructure	Technical design and deployment of the sandbox architecture	ANTS (Lead) + contributors	AE	
T2.3	Operation and access management of the sandbox	Management of user access, infrastructure maintenance, updates of the test repository and supervision of onboarding and usage processes.	ANTS (Lead) + contributors	AE	
T2.4	Support and capacity building for Member States	Provision of technical assistance, hands-on training sessions and documentation to help Member States use the sandbox efficiently.	ANTS (Lead) + contributors	AE	
<b>Milestones and deliverables (outputs/outcomes)</b>					

Milestone No (continuous numbering not linked to WP)	Milestone Name	Work Package No	Lead Beneficiary	Description		Due Date (month number)	Means of Verification
MS4	Sandbox architecture validated	2	ANTS	Technical validation of the sandbox architecture and specifications		M3	Architecture design document approved by consortium
MS5	Sandbox operational and accessible	2	ANTS	Sandbox environment deployed and available to Member States		M4	Successful deployment of the sandbox environment and confirmation of operational status.
MS6	Modular wallet solutions validated	2	ANTS	One EUDIW solution validated in sandbox		M12	First tests results by the partners
Deliverable No (continuous numbering linked to WP)	Deliverable Name	Work Package No	Lead Beneficiary	Type	Dissemination Level	Due Date (month number)	Description (including format and language)
D2.1	Common testing framework, methodology and sandbox infra. design	2	ANTS	R — Report	SEN — Sensitive	M4	English - Report defining the common testing framework, methodology, performance indicators, and the technical and functional design of the sandbox infrastructure and its architecture.
D2.2	Sandbox environment and resting capabilities	2	ANTS	DEM — Prototype	PU — Public	M8	Development and deployment of the sandbox environment and its associated testing capabilities for wallet interoperability, including documentation and support toolkit.

Estimated budget — Resources											
Participant	Costs (n/a for Lump Sum Grants)										
	A. Personnel		B. Subcontracting	C.1 Travel and subsistence	C.2 Equipment	C.3 Other goods, works and services	D.1 Financial support to third parties	D.2 Internally invoiced goods and services	D.3 PAC procurement costs (for PAC Grants for Procurement)	E. Indirect costs	Total costs
ANTS	79	€ 904,597	€ 200,000	€ 4,673						€ 63,649	€ 972,919
ARICOMA	35	€ 157,500								€ 11,025	€ 168,525
Ministry of Justice and Digital Affairs	7	€ 35,000	€ 100,000	€ 4,673						€ 9,777	€ 149,450
CCN	5	€ 30,000		€ 2,000						€ 2,240	€ 34,240
DEKRA	10	€ 82,000		€ 2,000						€ 5,880	€ 89,880
GRNET	13	€ 87,500		€ 4,673						€ 6,452	€ 98,625
MoDG	3	€ 9,600		€ 2,000						€ 812	€ 12,412
SDSA	25	€ 150,000		€ 10,000						€ 11,200	€ 171,200
EIMIN				€ 4,673						€ 327	€ 5,000
Namirial	10	€ 50,000								€ 3,500	€ 53,500
VDAA	29	€ 133,400		€ 4,673						€ 9,665	€ 147,738
MDIA	15	€ 83,745	€ 22,898	€ 4,673						€ 7,792	€ 119,108
eGov Moldova	4	€ 18,000		€ 4,000						€ 1,540	€ 23,540

MCA	2	€ 11,518	€ 12,680	€ 4,673						€ 2,021	€ 30,892
NASK	5	€ 28,020								€ 1,961	€ 29,981
ARTE	24	€ 120,000		€ 4,673						€ 8,727	€ 133,400
DIGG	4	€ 43,200	€ 92,313	€ 4,673						€ 9,813	€ 149,999
SETCCE	13	€ 75,000		€ 4,673		€ 6,000				€ 5,997	€ 91,670
MDT	3	€ 15,000	€ 40,000	€ 4,673		€ 4,000				€ 4,457	€ 68,130
NSA	16	€ 124,000				€ 15,000				€ 9,730	€ 148,730
DiiA	32	€ 142,784								€ 9,995	€ 152,779
A+LGAI	10	€ 65,000		€ 2,000						€ 4,690	€ 71,690
COI	11	€ 93,391	€ 18,650							€ 7,843	€ 119,884
Total	355	€ 2,459,255	€ 486,541	€ 73,403		€ 25,000				€ 213,094	€ 3,257,293
For Lump Sum Grants, see detailed budget table/calculator (annex 1 to Part B; see <a href="#">Portal Reference Documents</a> ).											

### Work Package 3

Work Package 3: Certification			
Duration:	M1 – M24	Lead Beneficiary:	CCB Belgium
Objectives			
WP3 is set up to prepare the full certification framework necessary for the European Digital Identity Wallet (EUDI Wallet), addressing the requirements defined by eIDAS v2 and supporting Member States and ENISA in developing national and European certification schemes. WP3 will achieve the following objectives:			

- Designing a complete certification system aligned with Article 5c and Article 12a of eIDAS v2, associated Implementing Acts, and existing EU cybersecurity certification frameworks.
- Preparing certification programs covering:
  - Functional conformity certification of EUDI Wallet implementations.
  - Cybersecurity conformity certification according to the EU Cybersecurity Act.
  - eID Scheme certification, focused on cybersecurity compliance.
- Supporting Member States in the creation of national certification schemes and providing guidance for ENISA expert groups.
- Developing lifecycle management rules and security audit frameworks for recertification and continuous updates.
- Building tooling and operational frameworks supporting execution of audits, testing, and security analysis.
- Designing formal security proofs, Protection Profiles (WSCA, WSCD), and a modular certification approach enabling harmonization and scalability.

*Within the project and the wider EUDI Wallet ecosystem, we want to see that certification is conceived as a common European approach: where national Conformity Assessment Bodies (CABs) are not available in all Member States, the framework enables cross-border certification, allowing a certification scheme or CAB designated in one Member State to assess and certify EUDI Wallets developed in another.*

#### Activities and division of work (WP description)

Task No (continuous numbering linked to WP)	Task Name	Description	Participants		In-kind Contributions and Subcontracting (Yes/No and which)
			Name	Role (COO, BEN, AE, AP, OTHER)	
T3.1	Regulatory & Implementing Acts Compliance Matrix	Review applicable regulations and implementing acts and produce a compliance checklist supporting systematic assessment	CCB Belgium (Lead) + contributors		
T3.2	Certification System Preparation	Design certification system based on eIDAS v2 regulation, CSA Article 54, ISO/IEC 17065 & 17067	CCB Belgium (Lead) + contributors		
T3.3	Functional EUDI Wallet Certification	Functional conformity program including testing, audits and gap analysis: <ul style="list-style-type: none"> <li>• Functional Requirements Verification : Execution of functional tests and validation of specification conformity.</li> </ul>	ANTS (Lead) + contributors		

		<ul style="list-style-type: none"> <li>• Functional Audit Framework Design : Definition of testing methods, audit criteria, and assessment tools.</li> <li>• Functional Audit Execution and Gap Analysis : Full audit implementation and identification of non-conformities.</li> </ul>		
T3.4	Cybersecurity Certification (EUDI Wallet)	Evaluate security and define cybersecurity audit frameworks : <ul style="list-style-type: none"> <li>• Security Requirements Analysis</li> <li>• Cybersecurity Audit Framework Definition</li> <li>• Security Testing and Security Audit Execution</li> </ul>	RDI (Lead) + contributors	
T3.5	eID Scheme Certification	Conformity assessment and validation with eIDAS 2.0 requirements : <ul style="list-style-type: none"> <li>• eID Scheme Requirements Analysis</li> <li>• eID Audit Framework Definition</li> <li>• eID Audits and Validation Tests</li> </ul>	ANSSI (Lead) + contributors	
T3.6	Life-Cycle Management (LCM)	Define policies governing maintenance, monitoring, updates & recertification	RDI (Lead) + contributors	
T3.7	Security Formal Proof	Develop formal security proofs for core protocols	MC (Lead) + contributors	
T3.8	WSCA / WSCD Protection Profiles & Certification	Develop & certify PP for WSCA & WSCD : <ul style="list-style-type: none"> <li>• Definition of Security Problems (WSCA &amp; WSCD)</li> <li>• WSCA Protection Profiles Series (3 PPs)</li> <li>• WSCD Protection Profiles Series (3 PPs)</li> <li>• WSCA Protection Profiles Certification</li> <li>• WSCD Protection Profiles Certification</li> </ul>	ANSSI (Lead) + contributors	

T3.9	Modularity Framework	Define a modular certification model enabling: <ul style="list-style-type: none"><li>• Shared certification mechanisms among Member States,</li><li>• Contractual templates for the transition period,</li><li>• Collaboration with ENISA on modular certification strategies.</li></ul>	<i>Lead to be defined at a later stage (Lead) + contributors</i>		
T3.10	Operational Framework	Define operational roles & interactions CAB / NCCA / NAB / Wallet Providers	CCB Belgium (Lead) (Lead) + contributors		
T3.11	Certification Scheme LCM	Define processes ensuring the continuous maintenance and evolution of the certification scheme, including activities between certification cycles (5-year validity).	CCB Belgium + contributors		
T3.12	Security of Global User Authentication	Define and validate end-to-end secure authentication mechanisms	ANTS (Lead) + contributors		
T3.13	Tooling Development	Develop tools to support all certification activities, including: <ul style="list-style-type: none"><li>• Audit tooling</li><li>• Functional testing tools</li><li>• Security testing tools</li></ul>	UC3M (Lead) + contributors		
T3.14	Wallet Trust Anchor Framework	Wallet and key attestations (WUAs) are critical for EUDI Wallet trust but were defined under time constraints with limited analysis of trust anchors, governance, and incident handling. This task revisits WUAs through threat analysis and provides recommendations to improve related standards and governance.	UC3M (Lead) + contributors		
T3.15	Zero Knowledge 2030	Zero-Knowledge Proofs (ZKPs) have been discussed as a way to enhance privacy (e.g. for age verification), but face practical challenges such as complexity and platform support. This task assesses when ZKPs are truly needed and when simpler, deployable alternatives are sufficient, while identifying cases where ZKPs remain necessary and feasible.	UC3M (Lead) + contributors		

<b>Milestones and deliverables (outputs/outcomes)</b>							
Milestone No (continuous numbering not linked to WP)	Milestone Name	Work Package No	Lead Beneficiary	Description		Due Date (month number)	Means of Verification
MS7	Certification System Architecture Validated	3	CCB Belgium	Definition of functional, cybersecurity & eID certification frameworks		M4	Consortium approval & documented architecture
MS8	Protection Profiles Completed	3	ANSSI	Delivery of WSCA & WSCD Protection Profiles		M8	Review and expert validation
MS9	Modular and Operational Framework Validated	3	CCB Belgium	Operational model for CAB/NCCA/NAB interactions		M8	Steering Committee approval
MS10	Certification Pilot Ready	3	CCB Belgium	Preparation completed to start certification pilot of reference implementation		M11	Pilot launch readiness report
Deliverable No (continuous numbering linked to WP)	Deliverable Name	Work Package No	Lead Beneficiary	Type	Dissemination Level	Due Date (month number)	Description (including format and language)
D3.1	Certification System Specification	3	CCB Belgium	R — Report	PU — Public	M4	Detailed specification of certification architecture
D3.2	Functional Certification Framework	3	ANTS	R — Report	SEN — Sensitive	M8	Functional testing, auditing methodology & gap analysis

D1.3	Cybersecurity Certification Framework	3	RDI/CNN?	R — Report	SEN — Sensitive	M8	Security testing, requirements mapping & audit plan
D3.4	Protection Profiles WSCA / WSCD	3	BSI / ANSSI	R — Report	PU — Public	M10	Protection profiles documents and requirements
D3.5	Modularity & Operational Model	3	CCB Belgium	R — Report	PU — Public	M10	Modular certification framework & operational interactions

Participant	Costs ( <i>n/a for Lump Sum Grants</i> )									
	A. Personnel	B. Subcontracting	C.1 Travel and subsistence	C.2 Equipment	C.3 Other goods, works and services	D.1 Financial support to third parties	D.2 Internally invoiced goods and services	D.3 PAC procurement costs <i>(for PAC Grants for Procurement )</i>	E. Indirect costs	Total costs
ANSSI	19	€ 152,000							€ 10,640	€ 162,640
LSTI	10	€ 70,000							€ 4,900	€ 74,900
Red Alert Labs	10	€ 70,000							€ 4,900	€ 74,900
CLR Labs	7	€ 70,000							€ 4,900	€ 74,900
Ministry of Justice and Digital Affairs	7	€ 35,000	€ 100,000	€ 4,673					€ 9,777	€ 149,450
A+LGAI	13	€ 84,500		€ 3,000					€ 6,125	€ 93,625

CCN	15	€ 90,000		€ 3,000						€ 6,510	€ 99,510
DEKRA	13	€ 106,600		€ 3,000						€ 7,672	€ 117,272
UC3M	15	€ 113,865								€ 7,971	€ 121,836
GRNET	8	€ 56,000								€ 3,920	€ 59,920
MoDG	5	€ 16,000	€ 30,000							€ 3,220	€ 49,220
QMSCERT	8	€ 75,000		€ 2,000						€ 5,390	€ 82,390
EIMIN	25	€ 105,000								€ 7,350	€ 112,350
MOD	25	€ 132,075		€ 4,673						€ 9,572	€ 146,320
MCA	18	€ 103,662	€ 31,852	€ 4,673						€ 9,813	€ 150,000
MC	5	€ 19,150								€ 1,341	€ 20,491
NASK	10	€ 60,360		€ 4,673						€ 4,552	€ 69,585
NIT	28	€ 180,700		€ 4,673						€ 12,976	€ 198,349
APCER Association	5	€ 16,260		€ 4,673						€ 1,465	€ 22,398
APCER SA	10	€ 32,520		€ 4,673						€ 2,604	€ 39,797
GNS	28	€ 140,000		€ 4,673						€ 10,127	€ 154,800
DNSC / NCCA	25	€ 140,000		€ 4,673						€ 10,127	€ 154,800
ATSEC	10	€ 65,000		€ 4,673						€ 4,877	€ 74,550
DIGG	8	€ 86,400	€ 49,114	€ 4,673						€ 9,813	€ 150,000
RISE	6	€ 68,790		€ 4,673						€ 5,142	€ 78,605
MDT	2	€ 7,500	€ 130,000	€ 4,673						€ 9,952	€ 152,125

SIQ	9	€ 63,580		€ 4,673						€ 4,778	€ 73,031
NSA	24	€ 192,000		€ 4,673		€ 10,000				€ 14,467	€ 221,140
Total	368	€ 2,351,962	€ 340,966	€ 81,095		€ 10,000				€ 194,882	€ 2,978,905

For Lump Sum Grants, see detailed budget table/calculator (annex 1 to Part B; see [Portal Reference Documents](#)).

## Work Package 4

Work Package 4: Support			
Duration:	M1 – M24	Lead Beneficiary:	GRNET
Objectives			
This Work Package supports Member States in the secure, interoperable, and efficient deployment of their wallet. It provides methodological, technical, and operational assistance, enabling administrations to implement and certify national wallets aligned with the European framework. The WP also develops and makes available reusable SDKs, technical modules, and tools (e.g., Annex A, rHSM, ZKP, visual standards) to accelerate deployment and harmonization.			
Specific Objectives:			
<ol style="list-style-type: none"> <li>The first objective is to assess Member State needs and priorities by analysing the technical and operational requirements for wallet deployment and identifying gaps and dependencies between national frameworks and the common EUDI Wallet infrastructure.</li> <li>The second objective is to define common frameworks and methodologies for modular wallet solutions, establishing guidance for interoperability, testing, and certification processes that can be applied across Member States.</li> <li>The third objective is to provide foundational modules, SDKs, and expert support, offering reusable technical building blocks and methodological guidance to facilitate national implementations.</li> </ol>			

<p>4. The fourth objective is to enable targeted project support for Member States by providing resources, technical expertise, and access to modules through a structured and transparent process that accelerates deployment and ensures compliance, security, and interoperability across EU wallets.</p>					
<b>Activities and division of work (WP description)</b>					
Task No (continuous numbering linked to WP)	Task Name	Description	Participants		In-kind Contributions and Subcontracting (Yes/No and which)
			Name	Role (COO, BEN, AE, AP, OTHER)	
T4.1	Assessment of Member States' needs	Analyse and document the technical, operational, and policy requirements of Member States for EUDI Wallet deployment. Identify gaps and dependencies between national frameworks and the common European EUDI Wallet infrastructure.	GRNET (Lead)+ contributors		
T4.2	Definition of a common framework and methodology	Develop shared frameworks and methodologies for modular wallet solutions, interoperability, testing, and certification. Provide guidance to ensure consistent and harmonized implementation across Member States.	GRNET (Lead)+ contributors		
T4.3	Technical modules and SDK development	Design, develop, and maintain reusable SDKs, secure hardware/software modules, and tools on priority topics. Ensure modules are interoperable and ready for adoption by Member States.	GRNET (Lead)+ contributors		
T4.4	Targeted member states support	Provide targeted technical support and resources to Member States through a structured and transparent process. This includes access to technical expertise, modules, and implementation guidance to accelerate deployment, testing, and certification of national wallets.	GRNET (Lead)+ contributors		
<b>Milestones and deliverables (outputs/outcomes)</b>					

Milestone No (continuous numbering not linked to WP)	Milestone Name	Work Package No	Lead Beneficiary	Description		Due Date (month number)	Means of Verification
MS11	Needs assessment framework validated	4	GRNET	Framework for collecting Member States' needs approved by consortium.		M6	All Member State requirements analysed and documented, with gaps and dependencies identified.
MS12	Common framework and methodology adopted	4	GRNET	Agreement reached among Member States and stakeholders on the common framework for EUDIW deployment and interoperability.		M8	Shared methodological framework for modular wallet solutions, testing, and certification formally adopted.
MS13	Availability of SDKs and technical modules	4	ANTS	Availability of SDKs and technical modules to Member States		M10	All key technical modules, SDKs, and tools developed and made available to Member States for implementation and testing.
Deliverable No (continuous numbering linked to WP)	Deliverable Name	Work Package No	Lead Beneficiary	Type	Dissemination Level	Due Date (month number)	Description (including format and language)
D4.1	Member states' needs assessment report	4	GRNET	R — Report	PU — Public	M3	Comprehensive mapping of Member States' technical needs for EUDIW deployment
D4.2	Common framework and methodology for	4	GRNET	R — Report	PU — Public	M4	Defines the shared approach for modular wallet solutions,

	EUDIW deployment						interoperability, and certification.
D4.3	Best practices and lessons learned compendium	4	GRNET	R — Report	PU — Public	M12	Consolidated overview of open-source tools, testing environments, deployment experiences, and certification REX.
D4.4	Core support team operational guidelines	4	GRNET	R — Report	SEN - Sensitive	M6	Procedures and toolkit for Member States to request and benefit from support.

Estimated budget — Resources										
Participant	Costs ( <i>n/a for Lump Sum Grants</i> )									
	A. Personnel	B. Subcontracting	C.1 Travel and subsistence	C.2 Equipment	C.3 Other goods, works and services	D.1 Financial support to third parties	D.2 Internally invoiced goods and services	D.3 PAC procurement costs <i>(for PAC Grants for Procurement )</i>	E. Indirect costs	Total costs
ANTS	87	€ 1,000,000	€ 300,000	€ 4,673					€ 91,327	€ 1,396,000
CIVIPOL					€ 3,000,000				€ 210,000	€ 3,210,000
GRNET	22	€ 154,000		€ 4,673					€ 11,107	€ 169,780
COI	34	€ 280,339							€ 19,624	€ 299,963
SETCCE	31	€ 186,000							€ 13,020	€ 199,020

University of Maribor	35	€ 136,500								€ 9,555	€ 146,055
Total	209	€ 1,756,839	€ 300,000	€ 9,346		€ 3,000,000				€ 354,633	€ 5,420,818
For Lump Sum Grants, see detailed budget table/calculator (annex 1 to Part B; see <a href="#">Portal Reference Documents</a> ).											

## Work Package 5

Work Package 5: Trustiness			
Duration:	M1 – M24	Lead Beneficiary:	UC3M
<b>Objectives</b>			
Within the context of the ever-increasing complexity of the EUDI Wallet, this WP covers the needs coming out of the ever-evolving ARF. As the regulation describes, EUDI Wallets should be LoA high eID means and need to be resistant against attackers with a high attack potential. In WP3 certification is addressed in context of ensure the above-mentioned LoA high and resistance. However, this EUDI Wallet will live in a world of constantly increasing threats especially when high-value use cases come into play.			
In this ever-evolving threat landscape it is necessary to be forward looking and study topics which will be vital moving forward like:			
<ul style="list-style-type: none"> <li>• Addressing interactions with relying parties as to protect and empower the citizen even more effectively moving forward.</li> <li>• Addressing current technical specifications and needed future specifications that are key for trust/resilience/security.</li> <li>• Providing hands-on support, clarification and shared interpretations of standards to help Member States and ecosystem actors align their implementations in a consistent and compliant way.</li> </ul>			

Therefore, the overall objective of the listed tasks under this work package is to:

1. Proactively address the identified “hot-spots” for ensuring LoA high and resistance against attackers with a high attack potential “beyond the currently envisioned MVP1”
1. Provide Guidance to Wallet Implementers on listed topics as to push to high plateaus of maturity / a higher consistent level of trust.

#### Activities and division of work (WP description)

Task No (continuous numbering linked to WP)	Task Name	Description	Participants		In-kind Contributions and Subcontracting (Yes/No and which)
			Name	Role (COO, BEN, AE, AP, OTHER)	
T5.1	Relying Party Authorization	<p>One thing is to identify the QWAC or QeSeal of an issuer or relying party. But how can one establish truly if that “identity” is trustworthy? Or whether it is effectively that authorized or accredited organization one is seeking to interact with, for this a much richer identity vetting is needed, plus the ability to, for example, determine if the issuer or relying party is effectively authorized or accredited in a specific sector or for a specific service.</p> <p>This task seeks to find a model to provide a way in which citizens can be guided easily to check if they truly interact with an authorized/accredited/trustworthy partner without manually having to search all kind of registries. This model could be based on VOP in payments, registries in social security, authorization models in eHealth, safe-on-web in Belgium, etc.</p>	UC3M (Lead) + contributors		
T5.2	Ensuring Effective User control	At this moment, the EUDIW specifications defines access certificates, registration certificates, very high-level disclosure policies, etc. This happens	UC3M (Lead) + contributors	BEN	No

		<p>while IETF has it views on selective disclosure and CEN is working in its access control standard. A normal citizen will easily get lost and simply click "yes allow all".</p> <p>This task tries to come to an affective human-centric model to guide citizens through the requests they will get from relying parties and try to define citizen- and privacy-friendly strategies without over-complication.</p>			
T5.3	Standardization helpdesk	<p>This task acts as a standardization helpdesk, analysing phishing-resistant authentication and authorization solutions and providing guidance on standards and best practices to improve citizen security, privacy, and user control.</p>	UC3M (Lead) + contributors	BEN	No

**Milestones and deliverables (outputs/outcomes)**

Milestone No (continuous numbering not linked to WP)	Milestone Name	Work Package No	Lead Beneficiary	Description		Due Date (month number)	Means of Verification
Deliverable No (continuous numbering linked to WP)	Deliverable Name	Work Package No	Lead Beneficiary			Due Date (month number)	Description (including format and language)
D5.1	Establishment of (business) characteristic needed to build a "chain of trust"	5	UC3M	R — Report	PU — Public	M6	Result from T5.1, to be the input for the rest of the works in the project.
D5.2	Models for a trustable Relying Party authorization	5	UC3M	R — Report	PU — Public	M14	Result from T5.1, including models for building useful registries and for wallets to guide the citizen

D5.3	Needs, use cases, and guidelines for effective user Control	5	UC3M	R — Report	PU — Public	M6	This deliverable combines analysis of user control needs and use cases with practical guidelines for human-centric, interoperable implementation. It defines use case categories, exchange strategies, and requirements, supporting standardization activities and providing a reference for consistent user control across EUDI Wallets.
D5.4	Introduction to SDOs and EUDIW related standards	5	UC3M	R — Report	PU — Public	M6	Document to be distributed internally within the Consortium, so that all partners will have a common understanding of all standardization work, prior to start the helpdesk for assisting with standards to the whole project.

Estimated budget — Resources										
Participant	Costs ( <i>n/a for Lump Sum Grants</i> )									
	A. Personnel	B. Subcontracting	C.1 Travel and subsistence	C.2 Equipment	C.3 Other goods, works and services	D.1 Financial support to third parties	D.2 Internally invoiced goods and services	D.3 PAC procurement costs <i>(for PAC Grants for Procurement )</i>	E. Indirect costs	Total costs
ANTS	10	€ 115,000							€ 8,050	€ 123,050

A+LGAI	2	€ 13,000								€ 910	€ 13,910
UC3M	21	€ 159,411		€ 4,673						€ 11,486	€ 175,570
GRNET	20	€ 140,000								€ 9,800	€ 149,800
FBK	8	€ 46,400								€ 3,248	€ 49,648
InfoCert	9	€ 64,800								€ 4,536	€ 69,336
Intesi Group	9	€ 85,500								€ 5,985	€ 91,485
MCA	11	€ 63,349								€ 4,434	€ 67,783
NIT	21	€ 136,500								€ 9,555	€ 146,055
ARTE	5	€ 25,000								€ 1,750	€ 26,750
Total	116	€ 848,960		€ 4,673						€ 59,754	€ 913,387
For Lump Sum Grants, see detailed budget table/calculator (annex 1 to Part B; see <a href="#">Portal Reference Documents</a> ).											

**Staff effort** (*n/a* for Lump Sum Grants)

Staff effort per work package						
Fill in the summary on work package information and effort per work package.						
Work Package No	Work Package Title	Lead Participant No	Lead Participant Short Name	Start Month	End Month	Person-Months
1	Governance	2	ANTS	M1	M24	705
2	Sandbox	2	ANTS	M1	M24	355
3	Certification	12	CCB Belgium	M1	M24	368

4	Support	25	GRNET	M1	M24	209
5	Trustiness	24	UC3M	M1	M24	116
					Total Person-Months	1753

<b>Staff effort per participant</b>						
Participant		WP 1	WP 2	WP 3	WP 4	WP 5
ANTS		84	79		87	10
CIVIPOL		36				36
ANSSI				19		19
LSTI				10		10
INGroupe		10				10
Red Alert Labs				10		10
CLR Labs				7		7
ARICOMA		20	35			55
Ministry of Justice and Digital Affairs		15	7	7		29
A+LGAI			10	13	2	25

CCN	10	5	15			30
DEKRA		10	13			23
UC3M			15		21	36
GRNET	25	13	8	22	20	88
MoDG	1	3	5			9
QMSCERT	0		8			8
MJPADT	16					16
PagoPA	10					10
Namirial	2	10				12
POLIMI	78					78
ANAC	1					1
FBK					8	8
InfoCert	11	0	0	0	9	20
Intesi Group	12	0	0	0	9	21
EIMIN	20		25			45
SDSA	25	25				50
MOD			25			25
VDA	43	29				72

eGov Moldova	2	4				6
MCA		2	18		11	31
MDIA	27	15				42
COI	6	11		34		51
MC	6		5			11
NASK		5	10			15
NIT	15		28		21	64
APCER Association			5			5
APCER SA			10			10
ARTE	15	24			5	44
GNS			28			28
ADR	48					48
MAI	48					48
DNSC / NCCA			25			25
ATSEC			10			10
DIGG	8	4	8			20
RISE			6			6

MDT	3	3	2			8
SETCCE	22	13		31		66
SIQ			9			9
University of Maribor				35		35
NSA	9	16	24			49
Diiia	43	32				75
DSGV	10					10
DVV	24					24
Total Person-Months	705	355	368	209	116	1753

*Subcontracting (n/a for prefixed Lump Sum Grants)*

## Subcontracting

Give details on subcontracted project tasks (if any) and explain the reasons why (as opposed to direct implementation by the Beneficiaries/Affiliated Entities).

**Subcontracting** — Subcontracting means the implementation of ‘action tasks’, i.e. specific tasks which are part of the EU grant and are described in Annex 1 of the Grant Agreement.

**Note:** Subcontracting concerns the outsourcing of a part of the project to a party outside the consortium. It is not simply about purchasing goods or services. We normally expect that the participants have sufficient operational capacity to implement the project activities themselves. Subcontracting should therefore be exceptional.

Include only subcontracts that comply with the rules (i.e. best value for money and no conflict of interest; no subcontracting of coordinator tasks).

Work Package No	Subcontract No (continuous numbering linked to WP)	Subcontract Name (subcontracted action tasks)	Description (including task number and BEN/AE to which it is linked)	Estimated Costs (EUR)	Justification (Why is subcontracting necessary?)	Best-Value-for-Money (How do you intend to ensure it?)
WP1	SC_WP1	All tasks of WP1	ANTS (FR – BEN)	400,000€	WP1: Assistance to project coordination for a very large consortium. No core coordinator activities subcontracted.	Framework contract
WP2	SC_WP2	All tasks of WP2	ANTS (FR – BEN)	200,000€	WP2: Support to the development of the expected Sandbox	Framework contract
WP4	SC_WP4	All tasks of WP4	ANTS (FR – BEN)	300,000€	WP4: Support to the development of expected SDKs	Framework contract
WP1	SC_WP1_1	All tasks of WP1	Ministry of Justice and Digital Affairs (EE, BEN)	110,000€	Estonia will procure the Wallet provision as a service in a public procurement. Market research showed that there are existing Wallet solutions on the market that may be tailored to national needs for EUDI wallet solution.	Public tender
WP2	SC_WP2_1	All tasks of WP2	Ministry of Justice and Digital Affairs (EE, BEN)	100,000€	Estonia will procure the Wallet provision as a service in a public procurement. Testing, interoperability validation and wallet certification will be done in cooperation with the Wallet service provider, operator, procuring authority and scheme owner.	Public tender
WP3	SC_WP3_1	All tasks of WP3	Ministry of Justice and Digital Affairs (EE, BEN)	100,000€	Estonia does not have local NAB/CAB/CBs - so the certification related activities need to be outsourced	Public tender
WP3	SC_WP3_2	All tasks of WP3	MoDG (GR)	30,000€	[insert]	Public tender
WP1	SC_WP1_2	All tasks of WP1	MDIA (MT, BEN)	25,000€	To secure core expertise to complement gaps in capability within the MDIA.	Public tender

WP2	SC_WP2_2	All tasks of WP2	MDIA (MT, BEN)	22,898€	To secure core expertise to complement gaps in capability within the MDIA.	Public tender
WP2	SC_WP2_3	All tasks of WP2	MCA (MT, BEN)	12,680€	To secure core expertise in scheme design and certification to complement gaps in capability within the MCA.	Public tender
WP3	SC_WP3_3	All tasks of WP3	MCA (MT, BEN)	31,852€	To secure core expertise in scheme design and certification to complement gaps in capability within the MCA.	Public tender
WP1	SC_WP1_3	All tasks of WP1	COI (PL, AE)	18,650€	[Insert]	Public tender
WP2	SC_WP2_4	All tasks of WP2	COI (PL, AE)	18,650€	[Insert]	Public tender
WP1	SC_WP1_4	All tasks of WP3	MJPADT (HR, BEN)	60,000€	Expertise within eIDAS and certification and standards. MJPADT currently does not have access to all required competencies inhouse	Public tender
WP1	SC_WP1_4	All tasks of WP1	DIGG (SE, BEN)	100,516€	Requires efforts by specialist consultants that are already hired by DIGG to provide expertise within eIDAS, trust infrastructure, certification and standards. DIGG currently does not have access to all required competencies inhouse.	Public tender
WP2	SC_WP2_5	All tasks of WP2	DIGG (SE, BEN)	92,313€	Requires efforts by specialist consultants that are already hired by DIGG to provide expertise within eIDAS, trust infrastructure, certification and standards. DIGG currently does not have access to all required competencies inhouse	Public tender
WP3	SC_WP3_5	All tasks of WP3	DIGG (SE, BEN)	49,114€	Requires efforts by specialist consultants that are already hired by DIGG to provide expertise within eIDAS, trust infrastructure, certification and standards. DIGG currently does not have access to all required competencies inhouse.	Public tender
WP5	SC_WP5_3	All tasks of WP5	DIGG (SE, BEN)	99,895€	Requires efforts by specialist consultants that are already hired by DIGG to provide expertise within eIDAS, trust infrastructure, certification and standards. DIGG currently does not have access to all required competencies inhouse	Public tender

WP3	SC_WP3_6	All tasks of WP3	MDT (SI, BEN)	130,000€	NCCA - national schema development	Public tender
WP1	SC_WP1_5	All tasks of WP1	MDT (SI, BEN)	40,000€	WP-project management and reporting	Public tender
WP2	SC_WP2_6	All tasks of WP2	MDT (SI, BEN)	40,000€	WP-testing: compliance, PEN	Public tender
Other issues: <i>If subcontracting for the entire project goes beyond 30% of the total eligible costs, give specific reasons.</i>		N.A.				

### Purchases and equipment

<b>Purchase costs (travel and subsistence, equipment and other goods works and services)</b> <i>Details for major cost items (needed if costs declared under 'purchase costs' are higher than 15% of the claimed personnel costs). Start with the most expensive cost items, down to the 15% threshold.</i>				
Participant:	CIVIPOL (FR)			
Cost item name	Category	WP(s)	Explanations	Costs (EUR)
Envelope	Other goods and services	WP1	<p>This budget envelope is planned to support participating Member States through dedicated funding mechanisms. Funding will be allocated to partners already participating in the consortium and is not distributed upfront. Instead, the project applies a <b>best value for money principle</b>, whereby resources are allocated <b>based on concrete technical achievements</b> during the project and aligned with work package objectives.</p> <p>For <b>WP1</b>, funding will be performance-based. Member States that achieve milestones in line with the ambitious project roadmap will be eligible for additional budget allocations. All expenditures must be justified through technical and financial contributions, demonstrating concrete progress and results. Funding will be linked to milestone</p>	2,000,000€

			completion and validated deliverables, ensuring that resources reward achievement and drive the project forward.	
Envelope	Other goods and services	WP4	<p>This budget envelope is planned to support participating Member States through dedicated funding mechanisms. Funding will be allocated to partners already participating in the consortium and is not distributed upfront. Instead, the project applies <b>best value for money principle</b>, whereby resources are allocated <b>based on concrete technical and financial proposals submitted</b> during the project and aligned with work package objectives.</p> <p>For <b>WP4</b>, funding will be granted based on technical and financial proposals addressing specific project needs. Proposals are evaluated jointly by Work Package Leaders and the COO, with priority given to solutions that are cost-effective, technically relevant, and aligned with project objectives. Implementation will be monitored under the project governance framework, with the mandated public entity remaining the primary beneficiary even if subcontractors are involved.</p>	3,000,000€
				Total 5,004,673€
Participant:	ANAC (IT)			
Cost item name	Category	WP(s)	Explanations	Costs (EUR)
Events	Travel and Subsistence	WP1	Travel costs	1,875€
				Total 1,875€
Participant:	MEGA (MD)			
Cost item name	Category	WP(s)	Explanations	Costs (EUR)
Events	Travel and Subsistence	WP1	Kick-off and other intermediary meetings, as decided by the WP Lead	2,000€
Events	Travel and Subsistence	WP2	Participating in 6 interoperability events	4,000€
				6,000€

Participant:	APCER (PT)			
Cost item name	Category	WP(s)	Explanations	Costs (EUR)
Events	Travel and Subsistence	WP3	Travel costs	4,673€
				Total 4,673€
Participant:	MDT (SI)			
Cost item name	Category	WP(s)	Explanations	Costs (EUR)
Events	Travel and Subsistence	WP1	WP-travel costs to attend BBs	4,673€
Events	Travel and Subsistence	WP2	WP-travel costs to interop events for 1 person	4,673€
Events	Travel and Subsistence	WP3	NCCA-travel costs	4,673€
Material	Other goods and services	WP2	WP-testing equipment	4,000€
				Total 18,019€
Total purchase costs > 15% (all participants)				5,035,240 €
Remaining purchase costs < 15% (all participants)				317,679 €
Total purchase costs (all participants)				5,352,919 €

#### Equipment with full-cost option

For calls where full-capitalised costs are exceptionally eligible for listed equipment (see Call document), indicate below the equipment items for which you request the full-cost option, and justify your request. Ensure consistency with the budget details provided in the previous table.

Equipment Name	Description (including WP, task number and BEN/AE to which it is linked)	Estimated Costs (EUR)	Justification (why is reimbursement at full-cost needed?)	Best-Value-for-Money (how do you intend to ensure it?)

N.A.	N.A.	N.A.	N.A.	N.A.
------	------	------	------	------

### Other cost categories

Other cost categories (financial support to third parties, internally invoiced goods and services, etc)		
Participant 1:	N.A.	
Cost category	Explanations	Costs (EUR)
Financial support to third parties	N.A.	N.A.
Internally invoiced goods and services	N.A.	N.A.

### Timetable

We are expecting the project to start on 1<sup>st</sup> of February 2026.

Timetable (projects up to 2 years)																									
ACTIVITY	MONTHS																								
	M 1	M 2	M 3	M 4	M 5	M 6	M 7	M 8	M 9	M 10	M 11	M 12	M 13	M 14	M 15	M 16	M 17	M 18	M 19	M 20	M 21	M 22	M 23	M 24	

Task 1.1 - Project steering and management																										
Task 1.2 - Collaboration with the European Commission and the LSPs																										
Task 1.3 - Financial management and reporting																										
Task 1.4 – Observatory and reporting tasks																										
Task 1.5 – Wallet development and issuance from Member States																										
Task 1.6 - Risks management, quality assurance, monitoring and evaluation																										
Task 2.1 - Definition of the testing framework and methodology																										
Task 2.2 - Design and setup of the sandbox and testbed infrastructure																										
Task 2.3 - Operation and access management of the sandbox																										



Task 3.11 - Certification Scheme LCM																								
Task 3.12 - Security of Global User Authentication																								
Task 3.13 - Tooling Development																								
Task 4.1 - Assessment of Member States' needs																								
Task 4.2 - Definition of a common framework and methodology																								
Task 4.3 - Technical modules and SDK development																								
Task 4.4 - Targeted member states support																								
Task 5.1 - Relying Party Authorization																								
Task 5.2 - Ensuring Effective User control																								
Task 5.3 - Standardization helpdesk																								

#\$WRK-PLA-WP\$#

#@ETH-ICS-EI@#

## 5. OTHER

## 5.1 Ethics

<b>Ethics</b> <i>If the Call document contains a section on ethics, the ethics issues and measures you intend to take to solve/avoid them must be described in Part A.</i>
See Application Form Part A.

#\$ETH-ICS-EI§# #@SEC-URI-SU@#

## 5.2 Security

<b>Security</b> <i>The security issues and the measures you intend to take to solve/avoid them must be described in Part A.</i> <b>Note:</b> Beneficiaries must ensure that their projects are not subject to national/third country security requirements that could affect the implementation or put into question the award of the grant (e.g. technology restrictions, national security classification, etc).
See Application Form Part A.

#\$SEC-URI-SU§# #@DEC-LAR-DL@#

## 6. DECLARATIONS

<b>Double funding</b> <b>Information concerning other EU grants</b> <span style="color: red;">⚠ Please note that there is a strict prohibition of double funding from the EU budget (except under EU Synergies actions).</span>	<b>YES/NO</b>
We confirm that to our best knowledge none of the projects under the action plan as a whole or in parts have benefitted from any other EU grant ( <i>including EU funding managed by authorities in EU Member States or other funding bodies, e.g. EU Regional Funds, EU Agricultural Funds, etc</i> ). If NO, explain and provide details.	YES
We confirm that to our best knowledge none of the projects under the action plan as a whole or in parts are (nor will be) submitted for any other EU grant ( <i>including EU funding managed by authorities in EU Member States or other funding bodies, e.g. EU Regional Funds, EU Agricultural Funds, etc</i> ). If NO, explain and provide details.	YES

<b>Financial support to third parties (if applicable)</b> <i>If in your project the maximum amount per third party will be more than the threshold amount set in the Call document, justify and explain why the higher amount is necessary in order to fulfil your project's objectives.</i>	
N/A.	

#\$DEC-LAR-DL§#

## ANNEXES

### LIST OF ANNEXES

#### Standard

Detailed budget table/Calculator (annex 1 to Part B) — mandatory for certain Lump Sum Grants (see [Portal Reference Documents](#))

CVs (annex 2 to Part B) — not applicable

Annual activity reports (annex 3 to Part B) — not applicable

List of previous projects (annex 4 to Part B) — mandatory, if required in the Call document

#### Special

Other annexes (annex 5 to Part B) — mandatory, if required in the Call document

*Regarding Ownership Control Declarations, the Q&A call precises that the declarations are not applicable.*

As mentioned in the Q&As of the call for proposals, Ownership Control Declarations are not applicable in this call and should not be submitted as part of the proposal documents.

#### Annex – List of previous projects

List of previous projects Please provide a list of your previous projects for the last 4 years.					
Participant	Project Reference No and Title, Funding programme	Period (start and end date)	Role (COO, BEN, AE, OTHER)	Amount (EUR)	Website (if any)
Mol_FR ANTS Namirial ARICOMA GRNET CIVIPOL INGroupe PAGOPA Diia DIA ICTU BZK FBK SETCCE COI MC ...	Project No: 101223990 Project Title: <b>APTITUDE</b> Funding programme: Digital Europe	01/09/2025 – 01/08/2027	COO AE BEN BEN BEN AE BEN BEN BEN BEN BEN BEN BEN BEN BEN AE BEN	Grant:10.000.000 euros	<a href="#">Accueil - Aptitude - For European Digital Identity</a>
ICTU INGroupe GRNET	Project Title: <b>WEBUILD</b> Funding programme: Digital Europe	01/09/2025 – 01/08/2027	BEN BEN BEN BEN	Grant: 12.000.000	<a href="https://www.webuildconsortium.eu/">https://www.webuildconsortium.eu/</a>

Intesi Group					
Mol_FR ANTS Namirial ARICOMA BMI GRNET CIVIPOL PagoPA Diia ICTU DVV COI FBK ...	Project No: 101102655 Project Title: <b>POTENTIAL</b> Funding programme: Digital Europe	01/04/2023 - 01/09/2025	COO AE BEN BEN BEN AE BEN BEN BEN AP BEN AP BEN BEN BEN BEN AP BEN BEN	Grant: 37.000.000 euros	<a href="https://www.digital-identity-wallet.eu/">https://www.digital-identity-wallet.eu/</a>
DSGV PagoPA Infocert ...	Project No: 101102740 Project Title: <b>NOBID</b> Funding programme: Digital Europe	01/04/2023 - 01/07/2025			<a href="https://www.nobidconsortium.com">https://www.nobidconsortium.com</a>
GRNET ...	Project No: 101102611 Project Title: <b>DC4EU</b> Funding programme: Digital Europe	01/04/2023 - 01/07/2025			<a href="https://www.dc4eu.eu">https://www.dc4eu.eu</a>
Infocert ICTU GRNET ...	Project No: 101102744 Project Title: <b>EWC</b> Funding programme: Digital Europe	01/04/2023 - 01/07/2025			<a href="https://eudiwalletconsortium.org">https://eudiwalletconsortium.org</a>