



REFERENCE NUMBER:

CT2274/2026

**SERVICES -
TENDER FOR THE IMPLEMENTATION OF A
FULLY COMPLIANT EUROPEAN DIGITAL
IDENTITY WALLET (EUDIW), SUPPORTING
TRUST ECOSYSTEM AND USE CASES FOR
THE MALTA DIGITAL INNOVATION
AUTHORITY (MDIA)**

This project is being financed through local budget

Department of Contracts

Notre Dame Ravelin,
Floriana FRN 1601, Malta
Tel: 2378 1001
Email: info.contracts@gov.mt

CONTENTS

SECTION 1 - INSTRUCTIONS TO TENDERERS	3
1. General Provisions	3
2. Timetable	4
3. Lots.....	4
4. Clarification Meeting	4
5. Selection and Award Requirements	4
6. Criteria for Award.....	8
SECTION 2 - SPECIAL CONDITIONS	23
SECTION 3 - SPECIFICATIONS / TERMS OF REFERENCE (Note 3)	50
1. Background Information.....	50
2. Contract Objectives and Expected Results.....	51
3. Assumptions and Risks.....	52
4. Scope of the Work	54
5. Logistics and Timing	83
Appendix I - The National eID System and Integration Protocols.....	88
Appendix II - eID Card Integration Documentation and Sample Code	89
Appendix III - Hosting and Service Level Requirements	90
SECTION 4 - SUPPLEMENTARY DOCUMENTATION	92
1. Draft Contract Form	92
2. Specimen Performance Guarantee	92
3. Ultimate Beneficiary Owner (UBO) form	92
4. Annexes.....	92
5. General Conditions of Contract	92
6. General Rules Governing Tendering.....	92

SECTION 1 - INSTRUCTIONS TO TENDERERS

1. General Provisions

1.1 The subject of this tender is the Implementation of a Fully Compliant European Digital Identity Wallet (EUDIW) and the Supporting Trust Ecosystem. The phases for this project are as follows:

- i. Design, develop, build and deploy a wallet mobile application, hereinafter referred to as Version 1, through which the users can authenticate with the eID server, store identification data downloaded following the authentication with the eID server, include age verification functionality and other daily-life use cases, and store, present and share digital information securely, within six (6) months from the commencement of the contract. This application is to use approved branding in both Maltese and English and in line with the Accessibility Directive.

Within twenty-one (21) months from commencement of the contract, design, develop, build, assist with certification and deploy Version 2 of the Solution with the necessary integration and exchanges between the Wallet Provider, Signing Certificate Provider, Wallet Relying Party Access Certificate Authority, PID Provider, Relying Party Registrar and Wallet Solution including the verifier components and Signature Creation Application (SCA). Version 2 shall still offer the same functionalities from Version 1 (i.e. the age verification and the use cases launched) but using the standards and methodologies adopted by the [EUDI Regulation] and the ARF. Version 2 relies on the existing eID Card and the keys it contains for initial onboarding and possible signing solutions, complemented by remote Wallet Secure Cryptographic Devices to reduce the need to rely on the physical ID Card.

- ii. The integration of additional digital services, with these new use cases being added as needed by the Contracting Authority based on national priorities and obligations arising from EU legislation. These use cases are additional to the functionalities incorporated in Version 1 and Version 2.
- iii. Every three (3) years following the commissioning of Version 2 of the Solution made available to the public, a design refresh of any public facing interface of the Solution is to be undertaken.

1.2 The place of acceptance of the services shall be the Malta Digital Innovation Authority, the time-limits for the execution of the contract shall be ninety (90) months commencing on the day of the last signature on the contract, with the possibility of two (2) extensions of twenty-four (24) months each, and the INCOTERM²⁰²⁰ applicable shall be **Delivery Duty Paid (DDP)**.

1.3 The Estimated Procurement Value for this Call for Tenders has been based on comprehensive research including appropriate financial analysis. In the context of this procurement, the Estimated Procurement Value, based on market research, is that of €15,659,714.03 excluding VAT.

The purpose of this value shall be the guidance of prospective bidders when submitting their offer and is not to be considered as a binding capping price.

Therefore, the published Estimated Procurement Value is not restrictive and final on the Contracting Authority. Economic Operators are free to submit financial offers above or below the Estimated Procurement Value. However, the Contracting Authority reserves the right to accept or reject Financial Offers exceeding the Estimated Procurement Value.

1.4 The final beneficiary of this tender is the Malta Digital Innovation Authority.

2. Timetable

The timetable is as per the dates set through the Cft workspace on the ePPS.

	DATE	TIME*
Deadline for request for any additional information from the Contracting Authority.	10/08/2026	09:30am
Clarifications by registered users to be sent online through www.etenders.gov.mt		
Last date on which additional information can be issued by the Contracting Authority	15/08/2026	09:30am
Deadline for Submission of Tenders (unless otherwise modified in terms of Clause 10.1 of the General Rules Governing Tendering)	03/09/2026	09:30am
Tender Opening Session (unless otherwise modified in terms of Clause 10.1 of the General Rules Governing Tendering)	03/09/2026	10:00am
* All times Central European Time (CET)/Central European Summer Time (CEST) as applicable		

3. Lots

- 3.1 This tender is not divided into lots, and tenders must be for the whole of quantities indicated. Tenders will not be accepted for incomplete quantities. The tender cannot be divided in lots as the individual components making the overall project are undividable and intrinsically linked to each other. The successful outcome of the project depends on the service being provided by one contractor.

4. Clarification Meeting

- 4.1 No clarification meeting/site visit is planned.

5. Selection and Award Requirements

In order to be considered eligible for the award of the contract, economic operators must provide evidence that they meet or exceed certain minimum criteria described hereunder.

High-Risk Processing and Transfer of Personal Data by ALL Bidders (Note 2)

The contract shall only be awarded to the Bidder if it is determined that indeed the High-Risk Processing of Personal Data is secure when processed by the Bidder and/or any of its Sub-Contractors, Suppliers, Service Providers or any third parties processing such data on behalf of the Bidder.

In such case, the Bidder must submit a completed GDPR Questionnaire together with any relevant justifications and explanations as necessary, thus, evidencing that it is indeed in a position to process Personal Data in high-risk processing in line with the Regulation (EU) 2016/679 on the Protection of Natural Persons with regard to the Processing of Personal Data and on the Free Movement of such Data (better known as General Data Protection Regulation - GDPR).

In terms of the Article 28(1) of the GDPR, the Contracting Authority is performing a due diligence exercise to obtain sufficient understanding from the various perspectives described in the GDPR

Compliance Questionnaire. This exercise is critical from a good governance and risk management perspective, and to ensure that the Bidder and/or any of its Sub-Contractors, Suppliers, Service Providers or any third parties (in their role as Data Processors) provide sufficient guarantees to implement appropriate technical and organisational measures in accordance with the GDPR.

In all cases, Bidders are to note that the Contracting Authority will require the prior written authorisation of the Data Controller to engage the Bidder as a Data Processor of the Data Controller's Personal Data, prior to award and Contract Signing. It is reiterated that the Contracting Authority cannot award the Procurement Call to any bidder unless the Data Controller provides it with such authorisation.

Accordingly, prior to Contract Signing, the Contracting Authority through the role of the Data Controller reserves the right to request the Bidder to provide it with any additional documentation and/or safeguards to verify that the Bidder or any of its Sub-Contractors, Suppliers, Service Providers or any third parties processing Personal Data in high-risk processing on behalf of the Bidder (in their role as Data Processors) are indeed in a position to process and transfer Personal Data in line with the GDPR.

All Stakeholders are reminded that Personal Data Processing (which includes also Personal Data Transfer) is defined as 'Any operation or set of operations which is performed on personal data or on sets of personal data, whether or not by automated means, such as collection, recording, organisation, structuring, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, restriction, erasure or destruction'.

In addition, a Definition of High-Risk may be reviewed from the following official link; <https://ec.europa.eu/newsroom/article29/items/611236/en>

(A) Eligibility Criteria

Economic Operators are to complete the Eligibility Section through the tender response format ^(Note 2)

- i. If applicable, the necessary forms - such as the Power of Attorney, are to be uploaded through the tender response format/ePPS/xml structure by the Economic Operator, as indicated in the relevant fields of the tender structure.

(B) Exclusion (including Blacklisting) and Selection Criteria - information to be submitted through the European Single Procurement Document (ESPD) in the tender response format ^(Note 2)

The Exclusion (including Blacklisting) criteria are to be completed by the Economic Operator in the ESPD (Tender response format) under Part III titled 'Exclusion Grounds' which includes the following:

- A. Grounds relating to Criminal Convictions
- B. Grounds relating to the payment of taxes or social security contributions
- C. Grounds relating to insolvency, conflicts of interests or professional misconduct
- D. Purely national exclusion grounds

Kindly note that the ESPD tender response format is pre-populated by the system. It is the Economic Operator's responsibility to ensure that the correct information is reflected in the ESPD tender response format for the above criteria.

Selection Criteria requirements are to be completed by the Economic Operator in the ESPD (Tender response format) under Part IV titled 'Selection Criteria' which includes the following: ^(Note 2)

- (a) **Suitability** ^(Note 2)
Not applicable.

- (b) **Economic and Financial Standing** ^(Note 2)

Average yearly turnover

The economic operator should provide its average yearly turnover for the number of years specified in the relevant procurement documents as follows:

The bidder must provide a signed declaration by a warranted Auditor appointed by the economic operator, which confirms the minimum average yearly turnover during the past three (3) financial years shall be not less than €2,500,000 - per year.

- (c) **Technical and Professional Ability** ^(Note 2)

i) For service contracts: performance of services of the specified type

The economic operator must demonstrate the successful completion of projects of a similar nature, namely the development and deployment of large-scale, software projects, limited to Trust Services, Identity solutions, and Digital Wallet solutions, completed during the last three (3) years, specifically 2023, 2024, and 2025, which satisfy the following criteria:

- (a) The minimum number of projects must not be less than two (2) projects during the period mentioned above.
- (b) The cumulative value of all the projects mentioned in (a) above, executed during the last three (3) years, must not be less than €5,000,000 (excl. VAT) in aggregate.
- (c) The bidder must provide a signed declaration by a warranted Auditor appointed by the economic operator, which confirms the successful execution and the cumulative value mentioned above in (a) and (b).

In so listing the end clients, the tenderer is giving his consent to the Evaluation Committee, so that the latter may, if it deems necessary, contact the relevant clients, with a view to obtain from them an opinion on the works provided to them, by the tenderer. The Evaluation Committee reserves the right to request additional documentation in respect of the deliveries listed.

ii) Subcontracting Proportion

Provide data concerning subcontractors and the percentage of works to be subcontracted. This information shall be included in the online ESPD form in Part IV: Selection criteria - Technical and professional ability.

Any subcontractor proposed and disclosed shall be evaluated in line with the Exclusion and Blacklisting Criteria as per these Instructions to Tenderers. Furthermore, if the sub-contractor is relied upon by the Contractor to meet the standards established in the selection criteria, apart from submitting the relevant commitments in writing, such reliance will be evaluated to verify its correctness and whether in effect these criteria are satisfied.

It is being understood that if the information being requested regarding sub-contracting is left empty, it will be assumed that no sub-contracting will take place (0% subcontracting).

(d) **Quality Assurance Schemes and Environmental Management Standards** ^(Note 2)

Certificates by independent bodies about quality assurance standards

The economic operator, as well as any subcontractors involved in the processing of data or delivery of security-relevant components, must be certified against ISO/IEC 27001. Evidence of valid certification shall be provided as part of the bid submission.

It is the Economic Operator's responsibility to ensure that the correct information is reflected in the ESPD tender response format for the above criteria.

(C) Specifications

- (i) Tenderer's Technical Offer in response to specifications to be submitted online through the prescribed Tender Response Format and by using the Tender Preparation Tool provided. ^(Note 3)

- (ii) Tenderer's Technical Offer/Organisation and Methodology ^(Note 3)

Key Experts Form, the Statement of Availability Form, the Self-declaration form for Key Experts (relating to public employees), CVs (to include the relevant experience and level of English and/or Maltese) and copy of respective certificates ^(Note 2).

Key Experts are as included in Section 3, Terms of Reference, Clause 6.1.1 - Key Experts.

- i. Key Expert 1: Project Manager
- ii. Key Expert 2: Solution Architect
- iii. Key Expert 3: Lead Developer
- iv. Key Expert 4: Cybersecurity Specialist
- v. Key Expert 5: Trust Services Specialist
- vi. Key Expert 6: Legal Specialist
- vii. Key Expert 7: Systems and Network Engineer

None of the Key Experts may occupy more than one role.

- (iii) Technical Offer Questionnaire ^(Note 3)

- (iv) GDPR Questionnaire - Technical ^(Note 3) - to be submitted online through the prescribed Tender Response Format and by using the Tender Preparation Tool provided.

- (v) **Literature** as per Form marked 'Literature List' to be submitted with the Technical offer at tendering stage. The scope of the literature is to corroborate a fully compliant technical offer. ^(Note 2)

- (vi) No Samples are being requested.

(D) Financial Offer

- (i) A financial offer calculated on the basis of Delivered Duty Paid (DDP) (Grand Total) for the services tendered as per Tender Response Format. ^(Note 3)

- (ii) A filled-in Financial Bid Form as per Tender Response Format. ^(Note 3)

In case of any discrepancy between what the bidder inputs as a total in the respective space directly in the .xml tender structure (and reflected in the Opening of Offers Schedule) and what

the bidder uploads as a document where requested in the Financial Section of the ePPS, the total in the .xml shall prevail for global-priced/lump sum financial offers.

On the other hand, where the financial offers to be uploaded constitute a Bill of Quantities (BoQ) or financial bid forms which contain rates/quantities/total prices broken down where the total can be arithmetically worked out and/or corrected, the total financial values worked out within the uploaded document in the Financial Section of the ePPS will prevail.

Notes to Clause 5:

1. Tenderers will be requested to clarify/rectify, within five (5) working days from notification, the tender guarantee only in the following four circumstances: incorrect validity date, and/or incorrect value, and/or incorrect addressee and incorrect name of the bidder. Rectification in respect of the Tender Guarantee (Bid Bond) is free of charge. (currently Bid Bonds are not applicable)

2. Tenderers will be requested to either clarify/rectify any incorrect and/or incomplete documentation, and/or submit any missing documents within five (5) working days from notification.

3. No rectifications shall be allowed. Only clarifications on the submitted information may be requested. Tenderers will be requested to clarify the submitted information within five (5) working days from notification.

Requests for Clarifications and/or Rectifications concerning a previous request dealing with the same shortcoming shall not be entertained.

6. Criteria for Award

- 6.1 The contract will be awarded to the bidder submitting the offer with the Best Price/Quality Ratio (BPQR) in accordance with the below.

Each technical offer will be evaluated in accordance with the award criteria and the associated weighting as detailed in the evaluation grid of this tender document. No other award criteria will be used. The award criteria will be examined in accordance with the requirements as indicated in the Technical Specifications.

The (BPQR) is established by weighing technical quality against price on a 70/30 basis respectively. This is done by multiplying:

- the technical scores awarded to the offers by 0.70
- the financial scores awarded to the offers by 0.30

- 6.2 The evaluation process:

At this step of the evaluation process, the Evaluation Committee will analyse the administratively-compliant tenders' technical conformity in relation to the published Terms of Reference/Technical Specifications.

When evaluating technical offers, each evaluator awards for each criterion/sub-criterion a score out of a maximum of 100 in accordance with the technical criteria and any sub-criteria as outlined in the evaluation grid.

If thresholds are set for each/any of the criteria/sub-criteria by setting a value out of 100, those offers that do not obtain the set threshold for the individual criterion/sub-criterion will be eliminated.

Tenderers must achieve an average technical score of 60%. The average technical score is arrived at by adding the individual weighted scores of each evaluator divided by the number of evaluators. Those tenderers that do not obtain the minimum set average technical score will be eliminated.

The offer achieving the highest technical score will be awarded 100% of the technical weight. The other offers will be awarded scores in proportion to the offer with the highest technical score as per below formula;

$$\text{Technical score} = \frac{\text{Average Technical Score of the Respective Offer}}{\text{Highest Average Technical Score}} \times \text{Technical Weight}$$

The financial offers for tenders which were not eliminated during the technical evaluation (i.e., those which have achieved an average technical score of 60% or more and/or those which have achieved the set threshold for individual criterion/sub-criterion) will be evaluated. The Evaluation Committee will also check that the financial offers contain no arithmetical errors.

The offer with the lowest price will be awarded 100% of the financial weight. The other offers will be awarded scores in proportion to the offer with the lowest price as per below formula;

$$\text{Financial score} = \frac{\text{Lowest Priced Offer}}{\text{Financial Offer of the Tender Being Considered}} \times \text{Financial Weight}$$

The BPQR will be awarded to the offer that has obtained the highest score after adding the respective technical and financial scores as visualised below;

Overall Best Price Quality Ratio (BPQR) evaluation

Conclusion of tender evaluation under BPQR:

$$\text{Score}_i = \left(\left(\frac{\text{Tech}_i}{\text{Tech}_{\max}} \times W_{\text{Tech}} \right) + \left(\frac{\text{Fin}_{\min}}{\text{Fin}_i} \times W_{\text{Fin}} \right) \right)$$

Where:

- ◆ Tech_i is the technical score of the supplier
- ◆ $\text{Tech}_{\max}$ is the maximum technical score achieved amongst all suppliers
- ◆ $\text{Fin}_{\min}$ is the minimum financial price offered amongst all suppliers
- ◆ Fin_i is the financial price of the supplier
- ◆ W_{Tech} is the weight of the technical envelope
- ◆ W_{Fin} is the weight of the financial envelope

BPQR Criteria

For Mandatory criteria, unless otherwise specified in the individual criterion, if the declaration / Proof / List / Picture / Template/ Write-up (or any other information as requested in each criterion) is not provided or else it is not in line with the specified requirements, automatically a score of '0' shall be allotted and the bidder shall be disqualified.

For other Mandatory criteria, whereby the specific criterion within the BPQR allows for a gradation of marks (Maximum of 100%) a range from 0 up to 100% of the marks per criterion may be allotted. If a score of '0' shall be allotted, the Bidder shall be disqualified.

For Add-On criteria, if the Declaration / Proof / List / Picture / Template / Write-up (or any other information as requested in each criterion) is not provided or else it is not in line with the specified requirements, automatically, a score of 1% shall be allotted.

Ref	Description	Marks	Marks on ePPS
	All criteria - unless otherwise stipulated in the table itself - will have a score allotment within a spectrum from 0 to 100%. All criteria are of a Mandatory nature. If the contents of the documentation exceed all minimum requirements, thus offering a higher quality bid, higher points will be allotted (up to the maximum score). Points shall be awarded in such a manner to reflect proportionately the level of effort undertaken to exceed the minimum requirements. Also, the submissions will be evaluated in terms of appropriateness and relevance of the proposed approach with conciseness, internal coherence and with a level of detail. The write-up/description should be concise and cross referenced to the provisions detailed in the ToR and the BPQR Award Criteria Table. It is up to the bidder to identify the most appropriate length of the write-up/description <u>in respect of each criterion below</u>, as applicable, with the proviso that the write-up/description should address all requirements accordingly. If the minimum requirements are not met, the offer will be deemed as Technically not-Compliant and disqualified. In this respect, a '0' score shall be allotted if the requested documentation is not submitted and/or the content of the documentation submitted does not meet all minimum requirements and the relative criteria/sub-criteria. If a zero is allotted to any criteria - the bid shall be disqualified. For Add-on requirements, if the requested information is not provided or else is not in line with the specific requirements, automatically the score of '1%' shall be allotted.		
1. Solution, Legal, and Operational Domains		100	
1.1 Mobile Application (Version 1) Functionalities and Technical Specifications		12	
a.	In accordance with Section 3 Clause 4.2.1.1, the bidder shall provide a technical architecture and supporting documentation (including write-up and e.g. flowcharts, standards compliance matrix) evidencing the proposed design of the mobile application (Version 1) and implementation of authentication with Malta's national eID infrastructure, privacy-preserving age verification and use cases (mandatory).	Max of 2 marks	Max of 100%

b.	In accordance with Section 3 Clause 4.2.1.1, the bidder shall describe all proposed functions (frontend and backend), interactions and capabilities in a clear and comprehensive manner (mandatory).	Max of 2 marks	Max of 100%
c.	In accordance with Section 3 Clause 4.2.1.1, the bidder shall provide descriptions of proposed use cases for the mobile application (Version 1) describing technical feasibility, whilst clearly outlining assumptions made, demonstrating familiarity with and relevance to the local context (mandatory).	Max of 2 marks	Max of 100%
d.	In accordance with Section 3 Clause 4.2.1.1, the bidder shall provide a plan, which includes both technical and UX aspects, for a smooth changeover from Version 1 to the EUDIW Solution (Version 2) in a way for the functionality of Version 1 to be available in Version 2 from first release (mandatory).	Max of 2 marks	Max of 100%
e.	In accordance with Section 3 Clause 4.2.1.1, the bidder provides a Version 1 that authenticates with Malta's national eID infrastructure at LoA High on launch (addon).	2 marks	1% or 100%
f.	In accordance with Section 3 Clauses 4.2.1.1 and 4.2.1.3.3, the bidder shall show how the age verification will be implemented in a way that is as conformant as possible with the latest version of the harmonised Age Verification solution blueprint developed by the European Commission, and that makes it as viable as possible to reuse in Version 2 (addon).	2 marks	1% or 100%
1.2 Legal and Compliance (mandatory)		6	
a.	Compliance with [EUDI Regulation] (for Version 2) The bidder shall provide a write-up outlining the technical, operational and organisational matters it will implement to achieve Legal Compliance covering all defined EUDIW functionalities of the [EUDI Regulation] and relevant Implementing Acts. This write-up shall extend to all components within the Solution including all relevant hosting.	Max of 3 marks	Max of 100%
b.	Compliance with other EU and National legislative frameworks (Version 1 and Version 2) For all the components in both Version 1 and Version 2, the bid shall describe regulatory compliance in reference to the legislation that is in the public domain on the date of the publication of this tender, showing the bidder's clear understanding of the legal and regulatory requirements it shall abide to which do not stem from the [EUDI Regulation].	Max of 3 marks	Max of 100%
1.3. Hosting and Operation (mandatory) The bidder shall demonstrate by means of a write-up (approximately 1000 words) how:		10	

a.	they shall deliver, operate, maintain, and support the solutions over the duration of the contract, in accordance with Section 3 Clause 4.2.3.11.8. The following needs to be included: - Operational continuity and service delivery plan - Maintenance and support framework - Scalability and extension readiness - Monitoring, reporting, and governance	Max of 4 marks	Max of 100%
b.	they shall maintain and update documentation for ongoing operations, support, and continuous improvement, including incident logs, maintenance schedules, performance reports, and user support materials, in accordance with Section 3 Clause 4.2.3.11.9.	Max of 2 marks	Max of 100%
c.	the proposed solution will be hosted in the GoM's secure hosting environment, in full compliance with specified security protocols, whilst supporting [EUDI Regulation] requirements, and meeting the defined service levels and volumetric requirements, in accordance with Section 3 Clause 4.2.3.11.10.	Max of 2 marks	Max of 100%
d.	the proposed solution leverages HSMs for secure key management, meets the defined service levels and volumetric requirements, and ensures disaster recovery capabilities. The explanation shall confirm full recovery of PID secret keys and high availability for identity operations, in accordance with Section 3 Clause 4.2.2.	Max of 2 marks	Max of 100%
1.4 Documentation and Training (mandatory)		5	
a.	The bidder shall demonstrate by means of a write-up (approximately 300 words) how it will meet the documentation and training requirements in accordance with Section 3 Clause 4.2.3.11.9 for Design Stage and Implementation Stage Documentation [3 marks].	Max of 3 marks	Max of 100%
b.	The bidder shall demonstrate by means of a write-up (approximately 200 words) how it will meet the documentation and training requirements in accordance with Section 3 Clause 4.2.3.11.9 for Operations & Support Documentation and Training including but not limited to knowledge base articles, support portals, and interactive user training modules [2 marks].	Max of 2 marks	Max of 100%
1.5 Project plan (mandatory) The bidder shall demonstrate by means of a write-up (approximately 2500 words) its initial proposed Project Plan and Resource Allocation Plan as per Section 3, Specification / Terms of Reference, including the following elements. The plan can be refined following initial meetings with the Contracting Authority.		15	
a.	Resource Allocation, Roles, and Responsibilities: provide a clear description of key resources and personnel assigned to the project, clearly identifying	Max of 3 marks	Max of 100%

	each role, its defined responsibilities and the expected level of effort throughout the project lifecycle.		
b.	Provide a detailed approach for each milestone, including detailed tasks and activities, realistic timelines and checkpoints. The description needs to take into account the respective components needed for each milestone.	Max of 3 marks	Max of 100%
c.	Key Deliverables and Dependencies: The bidder shall outline all key deliverables, any dependencies linked to each deliverable.	Max of 3 marks	Max of 100%
d.	Risk Identification, Severity, and Mitigation: identify potential risks, indicating severity (high, medium, low), likelihood, mitigation measures proposed and expected impact on the achievement of the contract's objectives.	Max of 3 marks	Max of 100%
e.	Methodology (e.g. Agile, Iterative): describe the methodology proposed for project delivery, including the mechanisms to ensure continuous improvement and how the approach will achieve or exceed the contract's objectives.	Max of 3 marks	Max of 100%
1.6 Security and Software Development Lifecycle		30	
a.	As per Section 3 Clause 4.2.1.3.7.1, the bidder shall demonstrate by means of a write-up (approximately 250 words) the proposed security architecture reviews including the frequency they will occur. The exact frequency of the security architecture review during the operational phase will be agreed upon to ensure alignment with the EU best practices [2 marks mandatory].	Max of 2 marks	Max of 100%
b.	As per Section 3 Clause 4.2.1.3.7.2, the bidder, shall demonstrate by means of a write-up (approximately 250 words) how they will perform Static Application Security Testing (SAST) and Dynamic Application Security Testing (DAST) prior to major releases or deployments. In the same write-up, the bidder shall describe whether and how: - they will perform SAST and DAST on every deployment including minor ones and - integrate such operations into secure CI/CD pipelines [2 marks addn].	2 marks	1% or 100%
c.	As per Section 3 Clause 4.2.1.3.7.3, in a write-up (approximately 250 words) the bidder shall demonstrate how penetration testing shall take place [1 mark mandatory]. Penetration testing takes place at least annually [1 mark addn]. Penetration testing by independent third parties [1 mark addn].	1 mark 2 marks	0% or 100% 1% as a minimum

d.	As per Section 3 Clause 4.2.1.3.7.5, in a write-up (approximately 250 words) the bidder shall indicate which industry-recognised and role-appropriate security training the key developers have completed prior to commencement of work [1 mark mandatory]. In the same write-up, the bidder shall describe whether the: • Security training includes achieving a recognised certification [1 mark add-on]. • Ongoing security training will be held at least annually [1 mark add-on].	Max of 3 marks	Max of 100%
e.	As per Section 3 Clause 4.2.1.3.7.8, the bidder shall demonstrate by means of a write-up (approximately 400 words) the approach to creating detailed User Acceptance Criteria following the GHERKIN format (or equivalent), performing regression testing and verification of applicable security controls [1 mark or 0] (mandatory). The bidder shall, in the same write-up, provide a description on how it will perform Smoke tests and User Acceptance Testing (UAT) on system and application changes [1 mark add-on]. The bidder shall also specify which software component(s) will be tested in an automated manner and how [2 marks add-on].	Max of 4 marks as per Add-On gradation	Max of 100% as per Add-On gradation 1% as a minimum
f.	As per Section 3 Clause 4.2.1.3.7.10, the bidder shall provide in a write-up (approximately 250 words) the mechanisms that will be implemented to detect tampering with the secure storage areas and attempts to access protected data outside authorised channels [2 marks mandatory].	Max of 2 marks	Max of 100%
g.	As per Section 3 Clause 4.2.1.3.7.11, the bidder shall explain by means of a write-up (approximately 250 words) the use of Runtime Application Self-Protection (RASP) capabilities to detect and react to suspicious activity [2 marks add-on].	Max of 2 marks	Max of 100%
h.	As per Section 3 Clause 4.2.1.3.7.12, the bidder shall provide a write-up (approximately 150 words), describing how logs shall be protected from unauthorised access. The response shall describe the methods employed to preserve logs integrity, availability and prevent tampering [2 marks mandatory].	Max of 2 marks	Max of 100%
i.	As per Section 3 Clause 4.2.1.3.7.13 the bidder shall demonstrate by means of a write-up (approximately 250 words) plans for regular incident response drills and simulations, clearly specifying the scope and time intervals between simulations including the methodology and proposed frequency of such Incident Response Drills [2 marks].	Max of 2 marks	Max of 100%
j.	As per Section 3 Clause 4.2.1.3.7.14 the bidder shall specify in a write-up (approximately 250 words) which subscription to relevant cybersecurity threat intelligence feeds will be used and how [1 mark mandatory]. In the same write-up, the bidder shall describe:	1 mark or 0	0% or 100%

	• Whether they will use two or more relevant cybersecurity threat intelligence feeds [1 mark addon]. • How the threat intelligence will be integrated into security monitoring and incident response processes [1 mark addon].	2 marks	1% as a minimum
k.	As per Section 3 Clause 4.2.1.3.7.15 the bidder shall provide a write-up (approximately 400 words) describing how regular assessments of security controls will take place, following a recognised framework, clearly indicating the scope and which of the audits will be held independently. In the same write-up, the bidder shall identify the risk levels, which audits will take place and the frequency of audits for different risk areas [2 marks mandatory].	2 marks	Max of 100%
l.	As per Section 3 Clause 4.2.1.3.7.16, the bidder shall provide a write-up (approximately 250 words) describing the approach, details and expected outcomes for anomaly detection [2 marks mandatory]. The bidder shall also explain how predictive modelling based on historical data, Machine Learning and AI models for behavioural biometrics will be used to support anomaly detection [1 mark addon].	Max of 2 marks 1 mark	Max of 100% 1% as a minimum
1.7 Key Experts The Key Experts may only hold the distinct role assigned and cannot be nominated for multiple roles simultaneously.		22	
a.	Key Expert 1 - Project Manager Responsible for the day-to-day management of the project including project initiation, planning, execution, monitoring, controlling, risk identification and resolution and closure throughout the duration of the Contract and possessing the minimum requirements, as per Section 3 Clause 6.1.1: • In possession of an academic qualification equivalent to MQF level 6 (or equivalent) in a field related to Management, or Information Communication Technology, or Engineering or a comparable subject field; • Has a minimum of 5 to 7 years' experience in ICT or related field of study [1 mark or 0] (mandatory). Add-On • Possession of an academic qualification equivalent to MQF level 7 (or equivalent) or higher in a field related to Management, or Information Communication Technology, or Engineering or a comparable subject field [1 mark addon]. • Have more than 8 years' experience in ICT or related area [1 mark addon]. • Have a minimum of 1 year experience in EUDIW Large Scale Pilots [1 mark addon]. • Be based in Malta for the duration of the project [1 mark addon].	Max of 5 marks as per Add-On gradation	Max of 100% as per Add-On gradation A minimum of 1% is to be allotted

b.	Key Expert 2 - Solution Architect Lead the architecture stream of the project, to ensure that the system design adheres to industry's best practices and in line with requirements set out in this tender and possessing the minimum requirements, as per Section 3 Clause 6.1.1 • In possession of an academic qualification equivalent to MQF level 6 (or equivalent) in a field related to Information Communication Technology or a comparable subject field; • Has a minimum of 5 to 7 years' experience in ICT or related area, out of which have a minimum 3 to 5 years' experience designing mobile and backend solutions. [1 mark or 0] (mandatory). Add-On • Possession of an academic qualification equivalent to MQF level 7 (or equivalent) or higher in a field related to Information Communication Technology or a comparable subject field [1 mark add-on]. • Have more than 8 years' experience in ICT or related area, out of which more than 3 years' experience relates to designing mobile and backend solutions [1 mark add-on].	Max of 3 marks as per Add-On gradation	Max of 100% as per Add-On gradation A minimum of 1% is to be allotted
c.	Key Expert 3 - Lead Developer A senior technical expert responsible for overseeing the end-to-end development of both mobile applications and backend systems, including API architecture and integration and possessing the minimum requirements, as per Section 3 Clause 6.1.1 • In possession of an academic qualification equivalent to MQF level 6 (or equivalent) in a field related to Software Development, or Information Communication Technology, or Engineering or a comparable subject field; • Has a minimum of 5 to 7 years' experience in software development or related area; [1 mark or 0] (mandatory). Add-On • Possession of an academic qualification equivalent to MQF level 7 (or equivalent) or higher in a field related to Software Development, or Information Communication Technology, or Engineering or a comparable subject field [1 mark add-on]. • Has more than 8 years' experience in software development or a related area [1 mark add-on].	Max of 3 marks as per Add-On gradation	Max of 100% as per Add-On gradation A minimum of 1% is to be allotted
d.	Key Expert 4 - Cybersecurity Specialist Responsible for ensuring the security and integrity of all digital assets within the project, including mobile applications, backend systems, and APIs and possessing the minimum requirements, as per Section 3 Clause 6.1.1. This	Max of 3 marks as per Add-	Max of 100% as per Add-

	role involves conducting risk assessments, defining security requirements, and implementing best practices to protect against cyber threats. The expert leads incident response efforts and provides guidance to development teams on secure coding and architecture • In possession of an academic qualification equivalent to MQF level 6 (or equivalent) in a field related to Cybersecurity, or Information Communication Technology, or Engineering or a comparable subject field; • Has a minimum of 3 to 5 years' experience in cybersecurity or related area; [1 mark or 0] (mandatory). Add-On • Possession of an academic qualification equivalent to MQF level 7 (or equivalent) or higher in a field related to Cybersecurity, or Information Communication Technology, or Engineering or a comparable subject field [1 mark add-on]. • Have more than 5 years' experience in cybersecurity or related area [1 mark add-on].	On gradation	On gradation
e.	Key Expert 5 - Trust Services Specialist Responsible for the setup, operation, and ongoing management of trust services as required by the [EUDI Regulation] and possessing the minimum requirements, as per Section 3 Clause 6.1.1. This expert possesses deep knowledge of Public Key Infrastructure (PKI), digital signatures, electronic seals, and related trust services. The role includes designing secure trust service architectures and overseeing the issuance and management of digital certificates. • In possession of an academic qualification equivalent to MQF level 6 (or equivalent) in a field related to Information Communication Technology, or Engineering or a comparable subject field; • Has a minimum of 3 to 5 years' experience in trust services or related area; [1 mark or 0] (mandatory). Add-On • Possession of an academic qualification equivalent to MQF level 7 (or equivalent) or higher in a field related to Information Communication Technology, or Engineering or a comparable subject field [1 mark add-on]. • Has more than 5 years' experience in trust services or related area [1 mark add-on].	Max of 3 marks as per Add-On gradation	Max of 100% as per Add-On gradation. A minimum of 1% is to be allotted
f.	Key Expert 6 - Legal Specialist Responsible for ensuring that all project components comply with the [EUDI Regulation] and other relevant legal frameworks, as per Section 3 Clause 6.1.1. This expert oversees the certification process for trust services, digital	Max of 3 marks as per Add-	Max of 100% as per add-on gradation.

	identity solutions, and related systems, ensuring alignment with regulatory requirements. Possession of the minimum requirements listed as per Section 3 Clause 6.1.1: • In possession of a recognised academic qualification to MQF Level 6 (or equivalent) (subject to a minimum of 180 ECTS/ECVET credits or equivalent) in Law; • Has a minimum of 3 to 5 years' experience in technology law, EU regulation; [1 mark or 0] (mandatory). Add-On • Has more than 5 years' experience in technology law, or EU regulation or related area [1 mark addon]. • Have been involved in technology and trust services for at least two related project worth over €1 million, indicating the roles performed on this project [1 mark addon].	On gradation	A minimum of 1% is to be allotted
g.	Key Expert 7 - Systems and Network Engineer Responsible for overseeing oversees the deployment, configuration, hardening, operation and monitoring of all project infrastructure as per Section 3 Clause 6.1.1. This expert works closely with other engineers in ensuring alignment with regulatory requirements. Possession of the minimum requirements listed as per Section 3 Clause 6.1.1: • In possession of an academic qualification equivalent to MQF level 6 (or equivalent) in a field related to Information Communication Technology, or Engineering or a comparable subject field; • Has a minimum of 3 to 5 years' experience in in mission-critical, high availability, and security sensitive environments; [1 mark or 0] (mandatory). Add-On • Has more than 5 years' experience in in mission-critical, high availability, and security sensitive environments [1 mark addon].	Max of 2 marks as per Add-On gradation	Max of 100% as per add-on gradation. A minimum of 1% is to be allotted
2. Components for Version 2		100	
2.1 EUDIW (Version 2) Functionalities, HLD and Technical Specifications (mandatory) In accordance with Section 3 Clauses 4.2.1.2, 4.2.2, 4.2.2.2 and 4.2.3 the bidder shall provide:		14	
a.	A technical architecture diagram [2 marks], sequence diagrams [2 marks] and a supporting write-up that includes details about third-party licences (in particular for the operation, maintenance, monitoring and support) and that outlines how the proposed implementation of the EUDIW Solution will be technically conformant [2 marks]. It should also include a detailed description of the integration between the various components [2 marks] and	Max of 10 marks	Max of 100%

	how the Solution will be integrated with Maltese ecosystem architecture, national services and infrastructure [2 marks].		
b.	A description of how the architecture is designed in such a way that it provides flexibility to the local government to assign ownership of individual architectural components to different public bodies.	Max of 2 marks	Max of 100%
c.	A mapping identifying the link between the applicable standards and the technical architectural components. It is to be noted that the Contracting Authority is cognisant that standards may change during the term of the contract and therefore the bidder is expected to refer to standards that have been adopted or are under discussion as of date of publication of this CfT.	Max of 2 marks	Max of 100%
2.2. Wallet Provider The bidder shall, by means of a write-up (approximately 1500 words) demonstrating attainment of the following evaluation criteria as applicable: • Cybersecurity • EUDIW Cross-border interoperability • Use of industry best-practices		16	
a.	Describe how the proposed Wallet Provider component will deliver and maintain conformance with the ARF specifications in accordance with Section 3 Clause 4.2.3.10.3 (mandatory).	Max of 3 marks	Max of 100%
b.	Describe how the proposed solution will issue attestation in the correct format, content, transport, signing, lifecycle, and revocation mechanisms in accordance with Section 3 Clause 4.2.3.2 (mandatory).	Max of 3 marks	Max of 100%
c.	Describe how the proposed solution will collect data and which data it will collect for wallet Solution maintenance, fraud detection and risk signal monitoring using privacy by design and security by design principles (mandatory).	Max of 3 marks	Max of 100%
d.	Describe the proposed provision and operation of a Signature Creation Application (SCA) as requested in Section 3 Clause 4.2.3.7.2 [3 marks] (mandatory), in such a way that it is external to the Wallet Provider component, in accordance with Section 3 Clauses 4.2.3.7.2 and 4.2.3.7.3 [2 marks addon].	Max of 3 marks 2 marks	Max of 100% 1% as a minimum
e.	The proposed approach to supporting QES using the XAdES, JAdES, CAdES, and ASiC formats (in addition to the mandatory support of the PAdES format to sign PDF files) in accordance with Section 3 Clause 4.2.3.7.1 [2 marks addon].	2 marks	1% or 100%
2.3 Relying Party Registrar The bidder shall demonstrate by means of a write-up (approximately 500-1000 words) and supporting technical architecture where applicable how they shall:		10	

a.	Establish and maintain the national register of RPs in Malta, in accordance with Section 3 Clause 4.2.3.10.6 (mandatory).	Max of 3 marks	Max of 100%
b.	Enable RPs to request and validate PIDs/EAs and verify the authenticity and validity of EUDIWs, as requested in Section 3 Clause 4.2.1.2 (mandatory).	Max of 2 marks	Max of 100%
c.	Provide, where applicable, an optional component for issuing and managing registration certificates to each registered Relying Party, the PID Provider and all attribute providers. The description shall at least include: • How this will integrate in the technical architecture [1 mark add-on] • Details about the component implementation [3 marks add-on] • A description of the policy that it will operate under [1 mark add-on]	5 marks	1% or 100%
2.4. PID Provider (mandatory) The bidder shall provide a write-up (approximately 1250 words), including sequence diagrams and supporting documentation where applicable, describing how they shall deliver a PID Provider component that:		12	
a.	Issues unique PIDs leveraging Malta's national eID infrastructure and OpenID Connect protocol, at LoA High authentication, in accordance with Section 3 Clause 4.2.2.	Max of 3 marks	Max of 100%
b.	Performs validation of the Wallet Unit prior to PID issuance through the required verifications.	Max of 3 marks	Max of 100%
c.	Provides mechanisms for secure PID issuance, including ensuring that a new PID can only end up on the device used by the subject of the PID.	Max of 3 marks	Max of 100%
d.	Revokes PIDs securely in accordance with Section 3 Clause 4.2.3.10.4.	Max of 3 marks	Max of 100%
2.5. Public Key Infrastructure (mandatory) In accordance with Section 3 Clause 4.2.3.10.5, the bidder shall demonstrate by means of technical architecture and supporting documentation (approximately 750 words) how they shall:		6	
a.	Provide, deploy, and integrate a PKI solution within the GoM's secure hosting environment ensuring attainment of service level requirements and operational readiness.	Max of 3 marks	Max of 100%
b.	Support certificate issuance including WRACs, ensuring conformance and compliance of the PKI solution.	Max of 3 marks	Max of 100%
2.6. Wallet Unit (mandatory)		20	

The bidder shall provide technical architecture and supporting documentation (approximately 2000 words) describing how their design, development and deployment of the Wallet Unit shall:			
a.	Integrate with the eID Card to enable secure communication via PACE protocol over NFC on Android and iOS in accordance with Section 3 Clause 4.2.2 (and relevant subclauses) and access the external QSCD for QES creation, in accordance with Section 3 Clause 4.2.3.7.3.	Max of 3 marks	Max of 100%
b.	Use secure authentication mechanisms, in accordance with Section 3 Clause 4.2.3.1.	Max of 2 marks	Max of 100%
c.	Include secure cryptographic communication using the TEE (with SE detection) for attestations in accordance with Section 3 Clause 4.2.3.4.1 and Clause 4.2.3.4.2.	Max of 2 marks	Max of 100%
d.	Use remote and proximity attribute presentation protocols, compliant with ISO/IEC 18013-5/7 and OpenID4VP, in accordance with Section 3 Clause 4.2.3.5.	Max of 2 marks	Max of 100%
e.	Be interoperable across NFC-enabled mobile devices and operating systems, including Android and iOS, in accordance with Section 3 Clause 4.2.3.11.2.	Max of 2 marks	Max of 100%
f.	Enable secure backup and recovery in accordance with Section 3 Clause 4.2.3.9.	Max of 2 marks	Max of 100%
g.	Generate pseudonyms in accordance with Section 3 Clause 4.2.3.11.3.	Max of 2 marks	Max of 100%
h.	Support PID-based authentication flows, nonce validation, and secure back-channel transmission, in accordance with Section 3 Clause 4.2.3.6.	Max of 3 marks	Max of 100%
i.	Include selective disclosure, in accordance with Section 3 Clause 4.2.3.6.	Max of 2 marks	Max of 100%
2.7. Remote Wallet Secure Cryptographic Device (mandatory) The bidder shall demonstrate by means of a technical write-up (approximately 1500 words) including sequence diagrams (for the RWSCD operation) depicting at a minimum the Registration, PID Secret Key Generation and PID Issuance, how the proposed RWSCD operation shall:		16	
a.	Meet the functional, security, privacy requirements [2 marks], and industry best practices for robust cryptographic algorithms to address emerging threats (such as quantum computing risks) [2 marks] in accordance with Section 3 Clause 4.2.2 (and relevant subclauses).	Max of 4 marks	Max of 100%
b.	Support a secure RWSCD registration process including two-factor authentication (hardware-bound key and PIN), prevention of replay attacks,	Max of 4 marks	Max of 100%

	and management of PIN retry counters in accordance with Section 3 Clause 4.2.2.1.		
c.	Securely: • generate, • store, • rotate, and • revoke PID secret keys within the RWSCD while ensuring that keys remain confidential, prevent key exposure outside the RWSCD environment, maintain integrity. The description is to include a high-level description of the key lifecycle management policies in accordance with Section 3 Clause 4.2.2.3.	Max of 4 marks	Max of 100%
d.	Sign Verifiable Presentations using the PID secret key. The description must confirm secure execution, privacy preservation, selective disclosure and prevention of key export or misuse, in accordance with Section 3 Clause 4.2.2.4.	Max of 4 marks	Max of 100%
2.8 Intellectual Property		6	
a.	The bidder shall describe the title in Intellectual Property for Version 1 confirming full ownership (addon).	3 marks	1% or 100%
b.	The bidder shall describe the title in Intellectual Property for the SCA Component confirming full ownership (addon).	3 marks	1% or 100%

200

SECTION 2 - SPECIAL CONDITIONS

These conditions amplify and supplement, if necessary, the General Conditions governing the contract. Unless the Special Conditions provide otherwise, those General Conditions remain fully applicable. The numbering of the Articles of the Special Conditions is not consecutive but follows the numbering of the Articles of the General Conditions. Other Special Conditions may be indicated afterwards.

Article 1: Definition and Conventions

1.3 Definitions

1. 'Bespoke Deliverables' means all software, code, configurations, documentation, data models, and other materials that are:
 - (a) created, developed, or produced by or on behalf of the Contractor specifically for the purposes of this Contract; or
 - (b) created through material adaptation of pre-existing materials where the resulting output is tailored to this Contract and the Solution.

The term includes without limitation the wallet core and all components of Version 1 and Version 2; identity credential management logic; interfaces with national systems including the Authority and all government registers; security modules; key management systems and signing infrastructure; the credential verification engine; the Orchestration Layer in its entirety; audit and logging systems; and all technical documentation, architecture specifications, API documentation, and data models produced under this Contract. This list is non-exhaustive. Materials produced using resources paid for under this Contract are presumed to be Bespoke Deliverables unless the Contractor establishes that they were produced entirely from pre-existing materials without material adaptation. Bespoke Deliverables do not include Third-Party Components or Vendor-Retained Components.

2. 'Enhancements' means post-acceptance work that extends the capabilities of the Solution, adds new functions, or improves performance beyond the originally accepted standard.
3. 'Escrow Materials' means the materials to be deposited under Section 2 Clause 45.1, which shall, where applicable, include Version 1 and the SCA component including any documentation, policies, lifecycle management, runtime policy engine, infrastructure-as-code (IaC) definitions and configurations as applicable.
4. 'Maintenance' means post-acceptance work maintaining the Solution at its originally accepted standard, including routine bug fixes, security patches, and performance monitoring.
5. 'Solution Data' means all data generated, processed, stored in the Solution, or held by the Contractor in connection with the Solution and services under this Contract.
6. 'Orchestration Layer' means the runtime control layer coordinating the live operation of the Wallet ecosystem, including but not limited to credential issuance workflows and policy enforcement; credential verification and relying party interactions; the Revocation Propagation Mechanism; wallet instance attestation services; cryptographic policy enforcement; runtime policy engines; and all APIs, control plane components, and coordination services forming part of that layer.
7. 'Reproducible Environment Specification' means the infrastructure-as-code definitions enabling the complete Solution, including the Orchestration Layer, to be deployed in an equivalent environment without reliance on the Contractor's own infrastructure.
8. 'Revocation Propagation Mechanism' means the mechanism by which revocation signals from credential issuers are transmitted through the Solution to Wallet Instances and Relying Parties.
9. 'SBOM' means a Software Bill of Materials listing every third-party component, version, licence, and provenance.
10. 'Security Incident' means any actual or suspected: (a) compromise of availability, authenticity, integrity or confidentiality of stored, transmitted or processed data or of the services offered by, or

accessible via, network and information systems; (b) compromise or suspected compromise of cryptographic keys or signing infrastructure; or (c) event causing or likely to cause inconsistencies with the [EUDI Regulation] or applicable Implementing Acts.

11. 'Third-Party Components' means software, libraries, and frameworks owned by third parties and incorporated into the Solution under open source or commercial licences without material adaptation.
12. 'Trigger Event' means any of the events listed in Article 45.1.
13. 'Vendor-Retained Components' means the Contractor's own internal tooling not forming part of the contractual deliverable, as identified in the Ownership Matrix defined in Section 2 Article 14.7.

- 1.9** Any decision by a Court of competent jurisdiction on the invalidity, illegality or unenforceability of any conditions of this contract or part thereof for any reason whatsoever shall not affect the validity, legality or enforceability of the remaining conditions of this contract. In such a case the parties shall negotiate in good faith to agree a replacement that, to the greatest extent possible, reflects the Court's decision to fulfil the terms of the contract.

Article 2: Notices and Written Communications

- 2.4** Any communication requesting clarifications within the tendering period is to be made online via the electronic-Public Procurement System (ePPS).

Official notices and written communications following the award of contract will be received by the Contractor either through registered postal mail from the Malta Digital Innovation Authority (MDIA) representative at:

Malta Digital Innovation Authority
Twenty20 Business Centre,
Triq l-Intornjatur,
Zone 3, Central Business District,
Birkirkara, CBD 3050

or via electronic mail sent from eudi.wallet@mdia.gov.mt

The contact person shall be nominated by the Malta Digital Innovation Authority upon awarding of the contract.

The official language of the document, submittal and all written communication shall be in the English Language.

All written communication following award of the contract, should be acknowledged at the earliest possible by the parties concerned.

Any notice, consent, approval, certificate or decision made by any person required under the contract shall be in writing, unless otherwise specified, and not be unreasonably withheld or delayed.

All communication is to bear the contract reference number.

Further details shall be given if necessary, after date of last signature on contract.

- 2.5** The contract is made up of the following documents, in order of precedence:
- a) the signed agreement;
 - b) the Special Conditions;
 - c) the General Conditions;
 - d) the Contracting Authority's terms of reference and design documentation;

- e) the Contractor's technical offer, and the design documentation submitted by the Contractor (drawings);
- f) the financial bid form (after arithmetical corrections if any)/breakdown;
- g) the tender declarations in the Tender Response Format;
- h) Appendices I-III
- i) any other documents forming part of the contract.

Addenda have (including clarifications/rectifications at evaluation stage) the order of precedence of the document they are modifying.

Article 5: Supply of Information

- 5.1** Further to the provisions of the General Conditions, the Contracting Authority shall supply the Contractor promptly with any information and/or documentation at its disposal which may be relevant to the performance of the contract. Such documents shall be returned to the Contracting Authority at the end of the period of execution of the contract.

During the contract duration, any updates by MITA to the Hosting Schedule including in Appendix III will be provided by the Contracting Authority.

The Contractor, however, is expected to keep abreast with discussions within European and International Standards Fora related to new Legislations and Standards that may impact the compliance of the Solution.

Article 6: Assistance with Local Regulations

- 6.1** A per General Conditions.

Article 7: General Obligations

- 7.2** The Contractor shall perform the services under the contract with due care, efficiency and diligence, in accordance with the best professional practice maintaining proper logs and trails of action.

- 7.3** Further to the general Conditions:

Any economic operator whose contribution has a direct impact on the security posture of any technical solution developed, deployed and operated shall maintain a valid certification against ISO/IEC 27001 throughout the contract duration, evidence of which shall be provided to the Contracting Authority when requested.

The Contractor shall discuss with the Contracting Authority any conflict that the Contractor reasonably believes exists between any of the Contractor's control standards and any other obligation under this Contract and shall comply with the Contracting Authority's decision on the resolution of that conflict. The Contractor's control standards will, in no event, be interpreted so as to relieve the Contractor from its obligations under this Contract.

- 7.12** The Contractor shall, within 15 calendar days of receipt of the contract, sign and date the contract and return it together with a copy of the Performance Guarantee. The copy of the Performance Guarantee forwarded to the Central Government Authority is to be endorsed by the Contracting Authority prior to submission. The Contractor is therefore obliged to forward the original Performance Guarantee to the Contracting Authority. The amount of the guarantee shall be 4% where the amount of the total contract

value is between €10,000 and €500,000 exclusive of VAT, and 10% where the amount of the total contract value is €500,000 or above.

In the case that the value of the contract does not exceed €10,000, no Performance Guarantee is required.

Economic Operators have the possibility to provide the Contracting Authority with a Single Bond covering the Performance Guarantees for all the contracts with the same Contracting Authority. If an additional contract is awarded to a given Contractor, which results in an Economic Operator's current Cumulative Contracts Value to go beyond the contract value range currently covered by the Single Bond, the Contractor is to be requested to: either submit a separate Performance Guarantee for the additional contract; or else submit a new Single Bond to cover the new total contracts value.

The Performance Guarantee shall be held against payment to the Contracting Authority for any loss resulting from the Contractor's failure to perform his contractual obligations fully and properly. The Performance Guarantee shall be in the format given by the Contracting Authority and must be provided in the form of a bank guarantee within the stipulated timeframes.

7.15 The Performance Guarantee shall be released as follows subject to no claims by the Contracting Authority:

- On successful completion of Milestone 1 - 2% of the performance guarantee
- On successful completion of Milestone 2 - 2% of the performance guarantee
- On successful completion of Milestone 3 - 5% of the performance guarantee
- On successful completion of Milestone 4 - 2 % of the performance guarantee
- On successful completion of Milestone 5 - 10% of the performance guarantee
- On successful completion of Milestone 6 - 3% of the performance guarantee
- On successful completion of Milestone 7 - 2% of the performance guarantee
- On successful completion of Milestone 8 - 2% of the performance guarantee
- On successful completion of Milestone 9 - 2% of the performance guarantee
- On successful completion of Milestone 10 - 3% of the performance guarantee
- On successful completion of Milestone 11 - 5% of the performance guarantee
- On successful completion of Milestone 12 - 9% of the performance guarantee
- On successful completion of Milestone 13 - 9% of the performance guarantee
- On successful completion of Milestone 14 - 9% of the performance guarantee
- On successful completion of Milestone 15 - 5% of the performance guarantee
- On successful completion of Milestone 16 - 5% of the performance guarantee

Within thirty (30) calendar days from completion of the contract - 25% of the performance guarantee.

7.16 The Contractor shall ensure that throughout the term of this contract, it shall:

- a) Identify and allocate a sufficient number of personnel each of whom shall have appropriate professional experience and qualifications to provide the services in accordance with the terms of this contract;
- b) Obtain and continue to maintain all necessary approvals, consents, licenses and permissions (legal, statutory, regulatory, contractual or otherwise) to allow the Contractor to perform the services in accordance with the terms of this contract and to allow the Contracting Authority to use the Deliverables in accordance with the terms of this contract; and
- c) Provide the Contracting Authority with any reasonable assistance as the Contracting Authority may reasonably require during the term of this contract in respect of the provision of the services at no additional cost to the Contracting Authority.

- 7.17** The Contractor shall ensure that its personnel abide by the Contracting Authority's policies and procedures and that if a resource is ever present on the Contracting Authority's premises, complies with the safety, security and other reasonable rules and regulations applicable at the said premises.

This shall be extended to other Public Bodies that may take ownership of one or more component listed in the solution.

- 7.18** The Contractor acknowledges that time is of the essence for the performance of its obligations under this Contract and shall acknowledge the deadlines stipulated with the relevant EU legislation.

Article 12: Indemnification

- 12.1** At its own expense, the Contractor shall indemnify, protect and defend, the Central Government Authority and the Contracting Authority, their agents and employees and sub-licensees, from and against any and all actions, claims, losses, proceedings and/or damage arising from any act or omission by the Contractor in the performance of the services, including any violation of any legal provisions, or rights of third parties, in respect of intellectual property and intellectual property rights and personal data protection.
- 12.2** The Contractor shall indemnify and hold harmless the Contracting Authority against all losses, claims, damages, penalties, fines, and costs (including reasonable legal costs) arising from:
- a) Any defect in the Deliverables
 - b) Any failure to conform with the Contractor's warranties; or
 - c) Any act or omission of the Contractor, its subcontractors, or infrastructure providers causing the Deliverables to operate inconsistently with the [EUDI Regulation]. This indemnity applies whether the claim is brought by a relying party, credential issuer, data subject, supervisory authority, or any other party. The indemnity is not subject to the General Cap.
- 12.3** The Contractor's aggregate liability shall not exceed five times total Contract value in any 12-month period ('General Cap'), except that the General Cap shall not apply to:
- a) Fraud or wilful misconduct;
 - b) Any Security Incident resulting in compromise of credentials of 100 or more individuals;
 - c) Systematic Revocation Propagation Mechanism failure affecting more than 1000 wallet instances; or
 - d) Liability under the indemnity in Clause 12.2.

Provided that the Contracting Authority reserves the right, at its discretion, to revise the thresholds defined in 12.3 (b) and 12.3 (c) according to best practices adopted by other EU Member States or other relevant entities.

- 12.6** If the software or the services become, or in the Contracting Authority's or Contractor's opinion is likely to become, the subject of a third party claim of infringement of intellectual property or intellectual property rights which in the Contractor or the Contracting Authority's opinion will lead to or is likely to lead to the Contracting Authority or its sub-licensees being prevented from using the software as per the terms of this contract, the Contractor shall:
- a) procure for the Contracting Authority and its sub-licensees the right to continue to use the software;
 - b) or replace or modify software to make it non-infringing at no cost to the Contracting Authority or the sub-licensees.
- 12.7** This article 12 shall survive the expiration or termination of this contract for any reason.

Article 13: Medical, Insurance and Security Arrangements

- 13.2** Further to the provisions of the General Conditions, the Contractor shall also obtain a full professional indemnity and cyber insurance policy which should cover costs and resources required to respond to the Data Protection Commissioner interventions and investigations; business interruptions; civil claims for compensation brought by individuals, damage to the reputation of the Contracting Authority and cyber security expenditure of a minimum of €4,000,000 in aggregate. Renewal of the insurance policy is to be submitted yearly within a month from its due date. The insurance policy would remain in place for the duration of the whole contract.

A copy of the insurance policy is to be submitted to the Contracting Authority within 100 calendar days of the last signature on the contract.

- 13.3** As per General Conditions.

Article 14: Intellectual and Industrial Property Rights

- 14.3** Further to the provisions of the General Conditions, the Contracting Authority shall retain all Intellectual Property Rights arising from materials any documentation owned by the Contracting Authority at the time of signature of the Contract and used in the course of the provision of the Service. All data, information, text and drawings, source code and other materials which are embodied in electronic, optical, magnetic or tangible medium, and which are supplied to the Contractor by the Contracting Authority is the sole property of the Contracting Authority or relevant public bodies.

The Contractor shall not have the right to use any data, reports, works or other property owned by the Contracting Authority for its own purposes without obtaining the prior written consent of the Contracting Authority.

- 14.4** The Contractor acknowledges that functions, services, or responsibilities under this Contract may be transferred by the Government of Malta to another entity by virtue of law, government reorganisation scheme, Cabinet decision, or any other formal decision of the Government of Malta. The Contracting Authority shall give the Contractor not less than 30 days' written notice of any intended transfer. Upon transfer, the transferee entity shall assume all rights and obligations of the Contracting Authority under this Contract as if named as the original contracting party, and the Contractor shall continue performance in favour of the transferee without requiring amendment to the Contract. The transfer shall not expand, restrict, or otherwise alter the scope of services under this Contract. Any change in scope required by the transferee shall be addressed through the Contract's variation procedure and shall not be implied from the transfer alone. The Contractor shall not be entitled to additional compensation by reason only of the change in contracting entity. Upon notice of transfer, the Contractor shall provide all necessary cooperation, documentation, data in open machine-readable formats, and technical assistance to ensure continuity of services. This obligation is without prejudice to the transition assistance obligations under Article 45.3.

- 14.5** The Contractor shall deliver to the Contracting Authority, at each milestone in Section 2 Clause 18.2 and again not later than 30 days before expiry or termination, each of the following:
- a) Full source code for all Bespoke Deliverables including configuration files, infrastructure-as-code definitions, and automated test suites if applicable, in a version-controlled repository with full commit history;
 - b) Complete build and deployment instructions enabling a competent third party to compile, build, test, and deploy the Solution independently, including all build scripts and CI/CD pipeline definitions;

- c) Up-to-date technical documentation including system architecture, data flow diagrams, API specifications, and security module documentation;
- d) An SBOM in SPDX or CycloneDX format (or any other format as requested by EU and national legislation) listing every Third-Party Component, version, licence, and provenance; and
- e) A Reproducible Environment Specification comprising full infrastructure-as-code definitions enabling the complete Solution, including the Orchestration Layer, to be deployed in an equivalent environment without reliance on the Contractor's infrastructure, including container image specifications, secrets management configuration (excluding live credentials), orchestration layer definitions, and infrastructure templates deployable against any compliant provider or on-premises environment.

Milestone payments shall not fall due until the Contracting Authority has confirmed in writing that deliverables (a) through (e) are complete and satisfactory. The Contractor shall not introduce proprietary dependencies without prior written approval of the Contracting Authority.

- 14.6** The Contractor hereby assigns to the Contracting Authority, with full title guarantee, all intellectual property rights in all Bespoke Deliverables, including all present and future copyright, database rights, and related rights. This assignment is effective at the moment of creation of each Bespoke Deliverable and covers without limitation: Wallet Provider, PID Provider, Relying Party Registrar, Signing Certificate Provider (PKI), WPRAC Provider, RP Verification Component and the Wallet Instances. The Contractor shall execute all documents required to give effect to this assignment. Third-Party Components shall be licensed under terms permitting the Contracting Authority to use, modify, deploy, and sublicense without restriction. The European Union Public Licence EUPL shall be used for open-source components developed partially under this Contract where full assignment is not required. Components licensed under strong copyleft licences including the GPL and AGPL shall not be incorporated without prior written approval and a written assessment of the copyleft infection risk.

- 14.7** The title in Intellectual Property of the developed solutions shall be vested in the Contracting Authority as follows:

Category	Components	Regime
Full Ownership	Wallet Provider PID Provider Relying Party Registrar Signing Certificate Provider (PKI) WPRAC Provider RP Verification Component Wallet Instances	Full title assignment guarantee; source code delivery at every release
Perpetual Licence	Licences for third-party open-source dependencies	Permissive or EUPL licence: irrevocable right to use, modify, sublicense; no strong copyleft without prior written approval.
Vendor Retained	Contractor's own internal tooling not forming part of the deliverable; Proprietary CI/CD pipeline used internally only	Must document and provide open-source equivalent or transition pathway on termination

Reference to the above components includes any documentation, policies, lifecycle management, runtime policy engine, infrastructure-as-code (IaC) definitions and configurations as applicable.

The Contractor is to obtain and continue to maintain on behalf of the Contracting Authority all necessary approvals, consents, licences and permissions (legal, statutory, regulatory, contractual or otherwise)

for third-party licences necessary for the operation, maintenance, monitoring and support of Version 1 and Version 2. This includes, but is not limited to, Operating Systems for the on-premises hardware and containers, security and monitoring solutions, backup solutions. The Contractor is to provide proof of purchase and licences to the Contracting Authority on an annual basis and on request by the Contracting Authority.

- 14.8** All Solution Data shall be owned exclusively by the Contracting Authority. The Contractor hereby assigns to the Contracting Authority, with full title guarantee, all database rights and any other intellectual property rights in Solution Data and the databases in which it is held. The Contractor shall not retain, copy, analyse, or use Solution Data following expiry or termination, except as strictly required for transition assistance. The Contractor acts as data processor in relation to Solution Data and shall comply with all applicable data processing obligations. Within thirty (30) days of expiry or termination of the Contract, the Contractor shall deliver all Solution Data in open, machine-readable formats and permanently delete all copies from its systems, providing written certification of deletion.

Article 15: Scope of the Services

- 15.1** The scope of the services is defined in Section 3 (Terms of Reference).

Article 16: Personnel and Equipment

- 16.4** As per General Conditions.

Article 17: Replacement of Personnel and Trainees

- 17.2** Further to the provisions of the General Conditions, in the event that a Key Expert needs to be replaced throughout the performance of this contract due to legitimate sickness and/or other extenuating circumstances, including also the non-performance of such individuals as decided upon by the Contracting Authority, the Contractor is obliged to provide the Contracting Authority with a detailed profile of the individual to replace the original Key Expert for approval prior to being entrusted with any tasks related to this contract. Any replacement is to meet the tender requirements. The Contracting Authority shall notify the Contractor in writing of the given reasons for its dissatisfaction. Within no later than ten (10) calendar days of receipt by the Contractor of such notice, the Contractor shall provide a suitable replacement resource.

The Contracting Authority reserves the right to refuse the replacement/s provided by the Contractor.

Article 18: Execution of the Contract

- The contract shall commence on the day of the last signature on the contract. The Contracting Authority shall organise a Briefing meeting with the Contractor for commencement of the duties within seven (7) working days of the last signature on the contract.
- 18.1**
- 18.2** The duration of the contract shall be ninety (90) months from commencement. The period of execution of the contract shall be for ninety (90) months subdivided as follows:

Milestone 1	Design a minimum of five branding proposals including logos, colour schemes, fonts, naming, social media templates and presentation templates, and any artwork for web and mobile applications.	45 calendar days from signing of the contract
Milestone 2	Design, build and test iOS and Android applications that can authenticate with the Maltese eID Server with the eID Card's authentication certificate (using NFC	3 months from signing of the contract

	functionality) at LoA High. This will be part of the Wallet Solution (Version 2).	
Milestone 3	Design, build, test and deploy and operate Version 1 through which the User can authenticate with the eID server, store identification data downloaded following authentication with the Maltese eID server, include age verification functionality and at least two (2) use cases, and provide the ability to store, present and share digital information securely. This app is to use approved branding in both Maltese and English, in line with the Accessibility Directive.	6 months from signing of the contract
Milestone 4	Design, build and test the Wallet Provider's ability to issue and revoke its attestations (with the option to use signing certificates not issued by the cryptographic signing component if not completed). Design, build and test the corresponding verification mechanism.	6 months from signing of the contract
Milestone 5	Design, build and test the Signing Certificate Provider component (PKI).	12 months from signing of the contract
Milestone 6	Design, build and test the RP Registrar component.	9 months from signing of the contract
Milestone 7	Design the UX for the Wallet Solution.	9 months from signing of the contract
Milestone 8	Design, build, test and deploy WRPAC Provider component.	15 months from signing of the contract
Milestone 9	Design, build and test the RP Verification component.	15 months from signing of the contract
Milestone 10	Design, build, test and deploy the Digital Signing component (SCA).	15 months from signing of the contract
Milestone 11	Design, build and test the PID Provider components (including PID Issuance).	12 months from signing of the contract
Milestone 12	Design, test and deploy the RWSCD component, integrating it with the necessary components for the successful PID Issuance (including RWSCD registration, PID Secret key registration and RWSCD operation) to the Wallet Solution. It is expected that all the infrastructure and supporting hardware has been installed and configured by this milestone.	15 months from signing of the contract
Milestone 13	Further design, build and test the Wallet applications for Android and iOS, to include the remaining functions which were not implemented in previous milestones.	16 months from signing of the contract
Milestone 14	Further design, build, test and deploy the Wallet Provider components, to include the remaining functions which were not implemented in previous milestones.	16 months from signing of the contract

Milestone 15	Integrate and deploy the EUDIW Solution with the necessary exchanges between the Wallet Provider, Signing Certificate Provider, Wallet Relying Party Access Certificate Authority, PID Provider, Relying Party Registrar and Wallet Solution including the verifier components and SCA attaining a fully compliant EUDIW Solution. Version 2 shall still include the age verification functionality from Version 1, relies on the existing eID Card and the keys it contains and uses a Remote WSCD.	19 months from signing of the contract
Milestone 16	Support the Contracting Authority attain certification of the Solution according to national or EU scheme, whichever is applicable at the time.	21 months from signing of the contract
	Hosting, Operations, SLA, Maintenance, Training, Review of Regulatory and Standards Updates and Support.	90 months (duration of the contract)

The Contracting Authority reserves the right to extend the contract or part thereof by up to six (6) months at no extra cost, such that the extension does not delay the completion of Milestone 16 by more than six (6) months. No extensions are possible for Milestones 1 and 3. If an extension is granted, the hosting, operation, maintenance and support related to Version 1 shall be at the same rates and terms.

Should, at any point, the Contractor become aware of any circumstance outside their control that may significantly delay the performance of this contract and the agreed services, the Contractor shall immediately notify the Contracting Authority in writing of the anticipated delay, and as far as this may be feasible, suggest an alternative approach to performing the services.

Extensions to the contract duration by the Contractor are subject to approval by the Contracting Authority, following approval by the DG Contracts, upon a written submission by the Contractor indicating a reasonable technical justification for such extension. The Contracting Authority will inform the Awarded Bidder during the contractual period if an extension is required.

Further to the provisions of the General Conditions, the period of execution of the contract shall be of ninety (90) months, after which the Contracting Authority with agreement of the Contractor reserves the right to extend the contract by an additional two (2) periods of twenty-four (24) months from the date of contract - in this manner extending the operation, maintenance and support of the Solution.

Unless where otherwise stated, in the event that the period of execution of the project is extended for any reason, the period of execution of the present contract shall be extended accordingly. The contractor shall not be entitled to request any additional payments in this respect in a court or tribunal.

Article 19: Delays in Execution

- 19.2** Daily delays in execution penalties shall be imposed on the Awarded Bidder. The delays in execution shall include the inability of the Awarded Bidder to meet the milestone deadlines as detailed below:

Milestone 1: €1,000 per day of delay;
Milestone 2: €1,000 per day of delay;
Milestone 3: €2,500 per day of delay;
Milestone 4: €1,000 per day of delay;

Milestone 5: €1,000 per day of delay;
Milestone 6: €1,000 per day of delay;
Milestone 7: €1,000 per day of delay;
Milestone 8: €1,000 per day of delay;
Milestone 9: €1,000 per day of delay;
Milestone 10: €1,000 per day of delay;
Milestone 11: €2,000 per day of delay;
Milestone 12: €2,000 per day of delay;
Milestone 13: €2,000 per day of delay;
Milestone 14: €2,000 per day of delay;
Milestone 15: €2,500 per day of delay;
Milestone 16: €2,000 per day of delay;

For penalties during the Operate, Maintain and Support Phase - €1,000 per day of delay.

The imposition of deductions as aforesaid shall not waive the Contractor's duty to perform any of its obligations or to rectify any of the shortcomings giving rise to the deduction. Furthermore, the deductions as aforesaid shall be effected by way of penalty and without prejudice to the Contracting Authority's right to claim damages from the Contractor if the Contractor's default result in such damages.

In the event that the Contracting Authority considers that a deduction is to be made in respect of any of the above listed failures and prior to any monetary deduction being made against the Contractor, the Contracting Authority shall give written notification and provide suitable evidence to substantiate its assertion for entitlement.

The Contractor shall have a period of a maximum of three (3) working days to submit representations on the default. If no representations on the default are presented by the Contractor, the Contracting Authority will proceed with the monetary deduction.

These above penalties shall be applicable up to a maximum of 15% of the contract value.

Upon reaching 15% threshold, the Contracting Authority reserves the right to invoke Article 19.3 of the General Conditions to terminate the contract and seek services of a third party for the completion of the required service. In such an instance, the Awarded Bidder shall be paid only for the services actually rendered. No further payments shall be effected in favour of the Contractor.

- 19.3** If these liquidated damages exceed more than 15% of the contract value, the Contracting Authority may, after giving notice to the Contractor and having obtained prior approval of the Central Government Authority:
- a) terminate the contract; and
 - b) complete the services at the Contractor's own expense.
- 19.6** Further to the General Conditions, within fifteen (15) days of realising that a delay might occur, the Contractor shall notify the Contracting Authority full details in writing of:
- a) The reasons for the delay;
 - b) The consequences of the delay; and any measures that have to be implemented in order to mitigate the delay.
 - c) If the Contractor claims that the delay is due to a Contracting Cause, the reason for making that claim.

Whether the delay is due to a Contracting Authority Cause or not, the Awarded Bidder shall make all reasonable endeavours to eliminate or mitigate the consequences of the delay.

Article 20: Modification of the Contract

- 20.2** Further to the provisions of the General Conditions and in accordance with Article 18.2, the period of execution of the contract shall be of ninety (90) months, after which the Contracting Authority with agreement of the Contractor reserves the right to extend the contract by an additional two (2) periods of twenty-four (24) months from the date of contract.
- 20.5** Further to the General Conditions, the percentage allowed as modification for repetition of service shall not exceed 55% of the total contract value.

The prerogative to order such repetition of services shall vest in the Contracting Authority and if not used the Contractor shall have no claim against Government.

Repetition of Services may be expected to arise under unforeseen circumstances falling within the scope of the services of this Contract, which may include but not limited to the following:

- the need for further design, development, testing and implementation and support services;
- the need for integration with other systems including those not within the control or owned by the Contracting Authority;
- further training requirements
- the need for amendments and enhancements to the Solution emanating from legislation changes.

Further to the above-mentioned circumstances, the CA shall also reserve the right to extend the duration of the contract following agreement with the contract and in line with what is being stated in Article 30.1 of the Special Conditions.

- 20.6** Subject to what is stated in the Public Procurement Regulations, the additional services (i.e. new services not included in the original tender) shall be capped at 20% of the contract value.

Additional Services may be expected to arise under unforeseen circumstances falling within of the scope of the services of this Contract which may include but not limited to:

- i. Enhancements to the Solution and its functionalities that become necessary during the contract term because of changes in legislation, implementing rules or in administrative procedures affecting the business processes.
During the course of the contract, the Awarded Bidder shall make the necessary changes ensuring alignment with relevant standards, EU and national legislation including those stemming from certification requirements to maintain [EUDI Regulation] requirements. The Awarded Bidder shall provide a detailed description of the necessary work and estimate of the effort and cost. The Contracting Authority reserves the right to appoint an independent third party to validate the Awarded Bidder's estimates. Any disputes are to be settled according to Article 38 of the General Conditions.
- ii. New functionalities that become necessary during the contract term to cater for changes in underlying and interconnecting systems within Government Departments / agencies / entities (public or private) that link to the Solution that will require shifting in timelines.

This provision is being made to cater for any unforeseen increase in the requirements during the duration of the contract.

The prerogative to order such additional services shall vest in the Contracting Authority and if not used the Contractor shall have no claim against Government.

Provided that before ordering additional services, the Contracting Authority shall obtain the approval of the Director of Contracts for the rates to be used, unless already provided in the Financial Offer as requested by the Contracting Authority. In such a case, the rates for Additional Services provided by the Contractor in the Financial Offer may apply. These rates may be used at the discretion of the Contracting Authority, if and when necessary, along the duration of the Contract.

- 20.8** Further to the General Conditions, once an additional service is identified, the Contractor will be asked to issue a quotation to indicate the work effort and duration for the additional service to be implemented. Prior to proceeding with the additional service, the Contracting Authority has to approve the quotation issued by the Contractor.
- 20.9** Further to the General Conditions, with specific reference to Enhancements, these shall be incorporated in the Solution and supported under the terms and conditions of this contract. The support and maintenance of enhancements or additional services will be at no extra cost unless otherwise agreed beforehand by the Contracting Authority.

Article 24: Interim and Final Progress Reports

- 24.1** Further to the General Conditions, Progress Reports shall be presented to the Contracting Authority on a regular basis as indicated below and when requested by the Contracting Authority.

a) Month 0 till completion of Milestone 16: Monthly reports to track progress and next steps. Reports to include at least the following (subject to any additional items during implementation):

- KPIs;
- Confirm delivery and approval of each milestone;
- Track and resolve project risks and issues; and
- Plan until the release.

b) Completion of Milestone 16 till end of contract: quarterly reports on the operation, maintenance and support. These reports are to include:

- % uptime, downtime hours, root cause, SLA Compliance;
- Incident volume, resolution time, SLA Breaches;
- Requests by type, fulfilment type, SLA Status;
- Progress of development of any use cases.

A progress report shall also be submitted when a request for payment against a presentation of an invoice is forwarded to the Contracting Authority.

As minimum, during the design, build and development of Version 1 and Version 2, meetings with the Project Manager shall be held on a weekly basis, or as necessary. The progress reports shall be the basis of these meetings.

The Contracting Authority may require an online or in-person meeting with the Awarded Bidder. Online Meetings can be requested within one day's notice whereas in-person meeting will be requested with a minimum of three days' notice.

The project closure report, technical reports, final user manuals and other reports as per Section 3 Article 4.2.3.11.9, shall be submitted in electronic format (excluding source code) to the Contracting

Authority. Reports must be written in the English Language. The Contracting Authority is responsible for approving these reports.

- 24.2. All invoices must be accompanied by the relevant progress report, which has to be certified by the Project Coordinator confirming that the agreed objectives have been met. No payment obligation shall arise before the progress report has been accepted by the Contracting Authority.
- 24.7 The Contractor shall provide to the Contracting Authority, at each milestone and upon request, a cost report disaggregated by system component. The format of such reports is as specified by the Project Manager during the period of execution of the Contract. The report shall distinguish between development costs attributable to each component in the IP ownership schedule, post-delivery maintenance and support costs, and costs attributable to Third-Party Components. The Contractor shall cooperate with the Contracting Authority's auditors in verifying the accuracy of cost reports.

Upon completion of each milestone, the Contractor shall submit a Milestone Completion Certificate identifying:

- a. the components completed and delivered;
- b. confirmation that all mandatory deliverables have been provided; and
- c. the date on which each component was available for use in the manner intended.

The Contracting Authority shall issue written acceptance or raise objections within 14 days. A milestone is not complete, and the corresponding payment shall not fall due, until written acceptance is issued. Accepted certificates constitute the accounting records supporting capitalisation of the relevant components.

Not later than 60 days after acceptance of each component, the Contractor shall deliver an As-Built Asset Register entry containing:

- a. a description and technical specification;
- b. delivery and acceptance date;
- c. total cost consistent with cost reports;
- d. an assessment of expected useful life and basis for that assessment; and
- e. identification of dependencies.

A consolidated register covering all components shall be delivered not later than 60 days after final system acceptance.

The Contractor shall classify all post-acceptance work orders as either Maintenance Work or Enhancement Work and shall invoice them separately with sufficient description for the Contracting Authority to make an independent classification determination. The parties agree to resolve classification disputes in good faith having regard to applicable accounting standards.

The IP assignment under Section 2 Article 14 takes effect at the moment of creation of each Bespoke Deliverable, such that intellectual property rights vest in the Contracting Authority continuously throughout the development process. The Contractor holds any such rights created prior to formal delivery on trust for the Contracting Authority pending delivery.

The Contractor shall, upon reasonable notice, provide the Contracting Authority's auditors, including the National Audit Office and any appointed external auditors, with access to project cost records, time records, invoices, and such other documentation as is reasonably required to verify the recognition and

measurement of intangible assets arising from this Contract. This obligation survives expiry or termination for 7 years.

Article 26: Payments and Interest on Late Payment

26.1 Payments will be made in Euro. This is a Global Price Contract.

Further to the provisions of the General Conditions, no pre-financing is allowed for locally-funded tenders. The Contracting Authority is bound to procure 80% of the awarded Contract Value.

The Contractor shall fulfil the hosting responsibilities detailed in Schedule 3 (Hosting Environment). Provided that the cost of hosting (item 18 of the Financial Bid) shall be borne by the Contracting Authority. Payments for item 18 (following the successful completion of Milestone 3), as confirmed by the awarded bidder and verified by the Contracting Authority) shall be paid directly to the hosting provider by the Contracting Authority on a monthly basis.

Nonetheless, any eventual increases in hosting and infrastructure requirements where it is evinced that the resources do not cater for the corresponding level of usage as specified in the Bidder's response and do not result from any agreed changes to the original requirements, shall be borne solely by the Contractor. Such additional resources shall be provided at no additional cost to the Contracting Authority (or offset from the charges due to the Contractor by credit note).

Narrative	Percentage (%)
Payment 1 shall be released one (1) month after the successful completion of item 1 of the financial bid as confirmed by the awarded bidder and verified by the Contracting Authority.	100% of the total value of item 1
Payment 2 shall be released one (1) month after the successful completion of item 2 of the financial bid as confirmed by the awarded bidder and verified by the Contracting Authority	100% of the total value of item 2
Payment 3 shall be released on a quarterly basis for item 3 of the financial bid as confirmed by the awarded bidder and verified by the Contracting Authority following the successful completion of Milestone 3.	100% of the total value of item 3
Payment 4 shall be released one (1) month after the successful completion of Milestone 2 as confirmed by the awarded bidder and verified by the Contracting Authority.	4.5% of the total value of item 4
Payment 5 shall be released one (1) month after the successful completion of Milestone 4 as confirmed by the awarded bidder and verified by the Contracting Authority.	4.5% of the total value of item 4
Payment 6 shall be released one (1) month after the successful completion of Milestone 13 as confirmed by the awarded bidder and verified by the Contracting Authority.	18% of the total value of item 4
Payment 7 shall be released one (1) month after the successful completion of Milestone 14 (corresponding to item 4 of the financial bid) as confirmed by the awarded bidder and verified by the Contracting Authority.	18% of the total value of item 4
Payment 8 shall be released one (1) month after the successful completion of Milestone 5 (corresponding to	54% of the total value of item 5

item 5 of the financial bid) as confirmed by the awarded bidder and verified by the Contracting Authority.	
Payment 9 shall be released one (1) month after the successful completion of Milestone 7 (corresponding to item 4 of the financial bid) as confirmed by the awarded bidder and verified by the Contracting Authority.	4.5% of the total value of item 4
Payment 10 shall be released one (1) month after the successful completion of Milestone 6 (corresponding to item 6 of the financial bid) as confirmed by the awarded bidder and verified by the Contracting Authority.	72% of the total value of item 6
Payment 11 shall be released one (1) month after the successful completion of Milestone 8 (corresponding to item 7 of the financial bid) as confirmed by the awarded bidder and verified by the Contracting Authority.	63% of the total value of item 7
Payment 12 shall be released one (1) month after the successful completion of Milestone 9 (corresponding to item 8 of the financial bid) as confirmed by the awarded bidder and verified by the Contracting Authority.	90% of the total value of item 8
Payment 13 shall be released one (1) month after the successful completion of Milestone 10 (corresponding to item 9 of the financial bid) as confirmed by the awarded bidder and verified by the Contracting Authority.	63% of the total value of item 9
Payment 14 shall be released one (1) month after the successful completion of Milestone 11 (corresponding to item 10 of the financial bid) as confirmed by the awarded bidder and verified by the Contracting Authority.	54% of the total value of item 10
Payment 15 shall be released one (1) month after the successful integration of PID Issuance (corresponding to Milestone 12) as confirmed by the awarded bidder and verified by the Contracting Authority.	13.5% of the total value of items 4, 7 18% of the total value of item 5 27% of the total value of item 10 30% of the total value of item 11
Payment 16 shall be released one (1) month after the successful integration of all the components within the EUDIW Solution as confirmed by the awarded bidder and verified by the Contracting Authority.	27% of the total value of items 4, 9 18% of the total value of items 5, 6 13.5% of the total value of item 7 9% of the total value of item 10 35% of the total value of item 11
Payment 17 shall be released one (1) month after the successful Certification of the Wallet Solution.	10% of the total value of items 4, 5, 6, 7, 8, 9, 10 35% of the total value of item 11
Payment 18 shall be released on a yearly basis during the operation of the EUDIW Solution (Version 2) for item 12 of the financial bid as confirmed by the awarded bidder through invoices and verified by the Contracting Authority.	100% of the total value of item 12
Payment 19 shall be released on a monthly basis for item 13 of the financial bid as confirmed by the awarded bidder through time sheets and verified by the Contracting Authority.	100% of the total value of item 13
Payment 20 shall be released on a monthly basis for item 14 of the financial bid as confirmed by the awarded	100% of the total value of item 14

bidder and verified by the Contracting Authority.	
Payment 21 shall be released on a quarterly basis for item 15 of the financial bid following the successful integration of all the components within the EDUIW Solution, as confirmed by the awarded bidder and verified by the Contracting Authority. Each quarterly payment needs to be presented in an itemised format, indicating the cost relative to each component in the Solution.	100% of the total value of item 15
Payment 22 shall be released on a monthly basis for item 16 of the financial bid as confirmed by the awarded bidder through time sheets and verified by the Contracting Authority. The payments need to be presented in an itemised format, indicating the cost relative to each component in the Solution.	100% of the total value of item 16
Payment 23 shall be released one (1) month after the successful completion of item 17 of the financial bid as confirmed by the awarded bidder and verified by the Contracting Authority. The payment needs to be presented in an itemised format, indicating the cost relative to each component in the Solution.	100% of the total value of item 17
TOTAL	100%

26.2 As per General Conditions.

Article 27: Financial Guarantee

Article 27 of the general conditions is Not applicable.

Article 30: Revision of Prices

- 30.1** Further to the provisions of the General Conditions, the Contracting Authority (CA) may extend the Contract by two (2) further periods of twenty-four (24) months each, subject to agreement between the Contractor and the CA and following approval by the Central Government Authority. Any extension shall be agreed no later than twelve (12) months prior to the expiry of the initial term or, as applicable, the expiry of any preceding extension period.

Exclusively for these proposed extensions, a revision of price may be considered subject to the mean Retail Price Index (RPI) of the Beneficiary Country over the previous two (2) year period prior to each extension. For the eventual second extension, the previous two years will be the period of the first extension. Any revision of prices is to be included subject to agreement between the Contractor and the CA and following approval by the Central Government Authority.

Items 14, 15 and 16 of the Financial Bid are the eligible for the extension period and shall be utilised according to the requirements of the Contracting Authority.

Article 40: Compliance with local Employment Regulations

- 40.1** The Contractor shall be bound to conform and comply with the Employment and Industrial Relations Act (CAP 452), its Subsidiary Legislations (including the Employment Agencies Regulations S.L. 452.130), and any other subsequent Legal Notices that may come into force, as well as any other national legislations, regulations, standards and codes of practice, in force during the execution of the contract, as applicable to the Contractor's particular operating situation and nature of activities.

Article 41: Protection of Personal Data

- 41.1** For the purpose of this Article “Personal Data”, “Sensitive Personal Data” and “Processing” shall have the same meaning as set out in the Data Protection Act (Cap. 586 of the Laws of Malta) and Regulation (EU) 2016/679 (General Data Protection Regulation).
- 41.2** Further to any applicable provision of these Special Conditions, the Contractor shall comply with the provisions of applicable personal data protection legislation when performing the services under this contract and shall ensure that the Deliverables are created in accordance with such personal data protection legislation. In particular, the Contractor shall ensure to implement the principles of data protection by design and default as set out in Article 25 of the General Data Protection Regulation. The Contractor shall document its compliance with such principles in writing and shall provide such documentation to the Contracting Authority upon request.
- 41.3** The Contractor shall ensure that any solution developed pursuant to this Call for Tenders allows for the Contracting Authority to comply with applicable personal data protection legislation, including but not limited to Article 5 of the General Data Protection Regulation.
- 41.4** When performing the services, the Contractor may be required to process personal data on behalf of the Contracting Authority, particularly when testing, integrating and configuring the Deliverables with the Contracting Authority’s own systems and that of its sub-licensees. When doing so, the Contractor shall act as a data processor, acting on behalf of the Contracting Authority (the data controller) and shall only process such personal data in accordance with this Article 41.4. The Contractor shall:
- a. Act only upon the written instructions of the Contracting Authority, including with regard to transfers of personal data to a third country or an international organisation, unless required to do so by EU or Maltese law. In such a case, the Contractor shall inform the Contracting Authority of that legal requirement before processing, unless that law prohibits such information on important grounds of public interest;
 - b. Ensure that persons authorised to process the personal data (including, but not limited to, the Contractor’s employees and resources) have committed themselves to confidentiality or are under an appropriate statutory obligation of confidentiality;
 - c. Implement appropriate technical and organisational measures to protect any personal data that may be processed on behalf of the Contracting Authority against accidental destruction or loss or unlawful forms of processing thereby providing the best possible level of security appropriate to the particular risks in question and take any other such measures as required by Contractor’s obligations as a processor in terms of Article 32 of the General Data Protection Regulation;
 - d. Not engage any other sub-processor without first obtaining the Contracting Authority’s prior consent in writing which may not be unreasonably withheld or delayed. Where the Contractor engages another processor to carry out specific processing activities on behalf of the Contracting Authority, the Contractor shall ensure that the same data protection obligations as set out in this contract shall be imposed on that other processor or sub-processor by way of a written contract, in particular providing sufficient guarantees to implement appropriate technical and organisational measures in such a manner that the processing will meet the requirements of the General Data Protection Regulation. Where that other processor or sub-processor fails to fulfil its data protection obligations, the Contractor shall remain fully liable to the Contracting Authority for the performance of that other processor or sub-processor’s obligations;
 - e. Taking into account the nature of the processing, assist the Contracting Authority by appropriate technical and organisational measures, insofar as this is possible, for the fulfilment of the

Contracting Authority's obligation to respond to requests for exercising the data subject's rights laid down in Chapter III of the General Data Protection Regulation;

- f. Assist the Contracting Authority in ensuring compliance with the obligations pursuant to Articles 32 to 36 of the General Data Protection Regulation taking into account the nature of processing and the information available to the Contractor;
- g. In any case, immediately inform the Contracting Authority of any personal data breach, as defined by the General Data Protection Regulation, and this whether or not the breach was caused by the Contractor;
- h. At the choice of the Contracting Authority, delete or return all the personal data to the Contracting Authority after the end of the provision of services relating to processing, and delete existing copies unless EU or Maltese law requires storage of the personal data; and
- i. Make available to the Contracting Authority all information necessary to demonstrate compliance with the obligations laid down in this article and allow for and contribute to audits, including inspections, conducted by the Contracting Authority or another auditor mandated by the Contracting Authority. In this regard, the Contractor shall immediately inform the Contracting Authority if, in its opinion, an instruction infringes the General Data Protection Regulation or other EU or Maltese data protection provisions.

41.5 The Contractor shall, in terms of Article 28 (3) of the General Data Protection Regulation 2016/679 (GDPR), sign a Data Processing Agreement to regulate the processing of personal data, ensuring compliance with European Union or Member State Law.

Article 42: Confidentiality of Data

- 42.1** The Contractor will not (and will ensure that its subcontractors and employees do not) store, copy or use data which is not in the public domain (other than as a result of a breach by the Contractor of its other obligations under the Contract) or was properly in the possession of the Contractor prior to receiving the data from the Contracting Authority for any purpose other than to the extent necessary to perform its obligations under the Contract.
- 42.2** The Contractor shall keep strictly confidential all information received in connection with the Contract and will disclose the same only to those of its staff who require information for the purpose of carrying out the Contractor's obligations under the Contract. The Contractor shall not disclose such information (howsoever obtained and in whatsoever form) to any third party unless such disclosure is compelled by law.
- 42.3** The Contractor shall not use any data to solicit any business for any of the Contractor's products or services, without the prior written consent of the Contracting Authority.
- 42.4** The Contractor undertakes to:
 - a) Keep all documentation and other papers and all discs, tapes and other media recording and will store the information entrusted within the Contractor's possession, custody or control in connection with the Contract, secure and in such a way so as to prevent unauthorized access to such information;
 - b) Immediately notify the Contracting Authority if it becomes aware that the information entrusted within the Contractor's possession, custody or control in connection with the Contract has been communicated or disclosed to any unauthorized Third Party;

- c) Return, delete or destroy upon the Contracting Authority's demand all information provided to the Contractor without keeping any copies and if requested by the Contracting Authority, provide a certificate confirming that the requirements of this Article have been complied with in full, at their expense within five (5) Working Days following the Contracting Authority's demand.

42.5 The Contractor shall:

- a) Make available to the Contracting Authority upon request all information relating to the processing of such data carried out in terms of this Contract; and
- b) Hand over such data to the Contracting Authority upon request, or termination or expiry of this Contract, unless such Contract is renewed.

42.6 The Contractor accepts that the provisions of the Official Secrets Act (Chapter 50 of the Laws of Malta) as amended by Act XVIII of 1996 may apply to the Contractor.

42.7 It shall be the responsibility of the Contractor to procure that its officers, employees or agents abide by the obligations set out in this Article by, inter alia, obtaining from such officers, employees or agents to whom any information is to be disclosed or who may in any way obtain access to such information, enforceable undertakings in terms at least as binding upon the said officers, employees or agents as the Contractor is bound to the Contracting Authority by virtue of this Contract.

42.8 This Article shall survive the termination of the Contract and shall continue to apply unless or until any of the following circumstances arise:

- a) The information is already known to the Contractor or in its possession before undertaking the obligation to keep it confidential;
- b) The information is or becomes publicly known other than through the unauthorized disclosure by the Contractor;
- c) The information is received from a Third Party without similar obligations of confidence and without breach of this Article;
- d) Is already possessed or independently developed by the Contractor;
- e) Is required to be disclosed by a court of competent jurisdiction or by any other statutory, fiscal or other authority; or
- f) Is approved for release by written authorisation of the Contracting Authority.

Article 43: Representations and Warranties

43.1 The Contractor warrants and represents that as at the date of execution of this contract and for the duration of the term:

- a) it has full capacity and authority to enter into and to perform this contract;
- b) this contract is executed by a duly authorized representative of the Contractor;
- c) once duly executed, this contract will constitute its legal, valid and binding obligations;
- d) it shall comply with its obligations in terms of this contract and at law; and
- e) it is not a party to any contract or agreement preventing it from entering into this contract and carrying out its obligations herein.

- 43.2** In addition to the warranties and representations set out in Article 43.1 above, the Contractor further warrants and represents to the Contracting Authority that:
- a) it is the valid owner or licensor of any intellectual property and intellectual property rights which shall be incorporated into the software to be created for the Contracting Authority as part of the services;
 - b) the software and the intellectual property rights pertaining to it are free from any right in rem or other encumbrance which would hinder or prohibit the Contracting Authority's right to use them as contemplated within this contract
 - c) all the intellectual property rights pertaining to the software are valid and subsisting and the Contractor is not aware of, nor are there or have been any claims, challenges, disputes or proceedings, pending or threatened, filed against the Contractor or its group in relation to the ownership, validity or use of any such intellectual property rights;
 - d) Exploitation, possession and use of the intellectual property rights pertaining to the software by the Contracting Authority in accordance with the terms and conditions of this contract will not infringe the rights of any third party; and
 - e) The Contractor has the approvals, consents, permissions, permits and right to use and assign the intellectual property rights relating to the software to the Contracting Authority in accordance with the terms of this contract;
 - f) The services will be performed:
 - i. in such a way as not to cause any fault or malfunction in the software or any related software or network and information systems of the Contracting Authority.
 - ii. in such a way as not to cause any interruption to the business processes of the Contracting Authority (other than any agreed and unavoidable interruption which is required in order to perform the services in a proper and efficient manner);
 - iii. in accordance with all applicable laws and regulations;
 - iv. In accordance with the SLA; and
 - v. with all reasonable skill and care;
 - g) it shall not introduce any viruses or vulnerabilities onto the Contracting Authority's network and information systems while performing the services;
 - h) the software provided under this contract will be of satisfactory quality and conform substantially to the Technical Specifications; and
 - i) it has adequate resources to meet its obligations under this contract in a timely and reliable manner.
- 43.3** The said warranties and remedies provided in this Article 43 are in addition to any other condition, warranty, or remedy given, whether express or implied, in contract or at law in particular including as to the fitness for the purpose and merchantability of the software.
- 43.4** In the event that the Contracting Authority discovers or is informed of an inherent or material error which substantially affects the use of the Deliverables (which use must always be in accordance with the intended use of the said Deliverables as set out in this contract) and notifies the Contractor of the error, the Contractor shall correct such error by patch or new release (at its option) that part of the Deliverable which contains the error at the Contractor's sole cost and expense.

- 43.5** The Contracting Authority shall endeavour to provide the Contractor with sufficient detail to enable the Contractor to replicate any problems or errors identified within the software.
- 43.6** The Contractor warrants that the Solution shall at all times during the Contract period:
- a) perform in accordance with the technical specifications in Section 3;
 - b) enable the Contracting Authority to discharge its obligations under the [EUDI Regulation], including but not limited to obligations relating to wallet security, credential integrity, verification mechanisms, revocation propagation, and wallet instance attestation; and
 - c) conform with all applicable technical standards and Implementing Acts under the [EUDI Regulation].

A breach of this warranty causing or contributing to a third-party claim against the Contracting Authority constitutes a material breach of this Contract.

- 43.7** The Contractor warrants that revocation signals issued by credential issuers shall be propagated to affected wallet instances and made available to relying parties within a timeframe to be decided during initial meetings and/or in alignment with any relevant technical specification, and in any event within the maximum latency permitted under applicable implementing acts. The Contractor shall monitor revocation propagation continuously and report failures to the Contracting Authority within a timeframe to be decided during initial meetings and/or in alignment with any relevant technical specification. Any failure resulting in a relying party accepting a credential that had been revoked prior to presentation shall be reported immediately and constitutes a notifiable Security Incident.

Article 44: Acceptance and Testing

- 44.1** The Contractor shall provide the Deliverables in accordance with best industry practices and this contract. The Contractor shall implement all necessary technical and organisational security measures, as applicable under the Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (hereinafter referred to as the General Data Protection Regulation), the Data Protection Act (Cap. 586 of the Laws of Malta) and the subsidiary legislation thereunder and any other applicable law in Malta which may be in force from time to time, to ensure that errors in Deliverables and data breaches are minimised.
- 44.2** Prior to providing the Contracting Authority with the Deliverables for the Contracting Authority's testing and use, the Contractor shall ensure that the Deliverables are thoroughly tested and are free from defects. The Contractor shall provide the Contracting Authority with its test sheets and test certificates as the Contracting Authority may require. The Contracting Authority shall be entitled to inspect or test the Deliverables at any time.
- 44.3** Without prejudice to Article 14, upon completion of the development of the Deliverables, the Contractor shall submit a complete copy to the Contracting Authority and demonstrate its functionality to the Contracting Authority.
- 44.4** The Contracting Authority reserves the right to review and test the Deliverables in accordance with this contract, relevant legislation and the technical specifications pursuant to any acceptance criteria or test plans mutually agreed upon in writing by the parties for such Deliverables.
- 44.5** The Contracting Authority will provide the Contractor with written notification of acceptance for each Deliverable promptly upon acceptance; however, failure to reject a Deliverable, as set forth below, will be deemed acceptance.

- 44.6 If the Contracting Authority, in its reasonable and good faith judgment, determines that any submitted or performed Deliverable does not satisfy the mutually agreed upon acceptance criteria or does not meet best industry standards, the Contracting Authority must so notify the Contractor in writing within a time period agreed between the parties in writing for each Deliverable after the Contractor's submission or completion of the Deliverable and shall specify the deficiencies in detail. The Contractor will use its best efforts to correct such deficiencies and resubmit or reperform the Deliverable to the Contracting Authority within seven (7) calendar days at no cost to the Contracting Authority. The Contracting Authority will again review and test the Deliverable against the agreed-upon acceptance criteria and detail any deficiencies to the Contractor in writing within a time period agreed between the parties in writing for each Deliverable after resubmission or reperformance of the Deliverable. If a Deliverable fails to meet the functional requirements mutually agreed upon in writing by the parties for such Deliverable after its second resubmission to the Contracting Authority, the Contracting Authority may at its sole discretion either:
- a) again reject the Deliverable and return it to the Contractor for further correction and resubmission in accordance with the process described above; or
 - b) again reject the Deliverable and return it to the Contractor for further correction and resubmission in accordance with the process described above and impose penalties in accordance with Article 19.2; or
 - c) terminate the contract immediately upon written notice and recover all fees paid for such deficient Deliverable.
- 44.7 Acceptance of the Deliverables will not affect the Contracting Authority's rights or remedies.
- 44.8 Each Deliverable shall be accompanied by relevant technical information.

Article 45: Operational Continuity

- 45.1 Unless full ownership of the Escrow Materials is granted to the Contracting Authority, the Contractor shall deposit the Escrow Materials with an approved escrow agent within 14 days of this Contract and after each major release or milestone. The escrow agent shall verify within 30 days of each deposit that the Escrow Materials are complete and that the source code compiles and deploys. The Contracting Authority may appoint an independent technical auditor for periodic verification. The Escrow Materials shall be released automatically on any Trigger Event, being:
- a) the Contractor's insolvency, administration, or winding-up;
 - b) abandonment of material obligations for more than 30 consecutive days following written notice;
 - c) material unremedied breach; or
 - d) failure to maintain required [EUDI Regulation] certifications.
- 45.2 In the event of any Trigger Event, the Contracting Authority may by written notice exercise step-in rights to take temporary operational control of service delivery. During any step-in period, the Contractor shall:
- a) grant the Contracting Authority and any nominated third-party full access to all systems, infrastructure, credentials, data, and personnel required to maintain service continuity;
 - b) take no action that impedes such access;
 - c) cooperate with the Contracting Authority's operational decisions; and
 - d) ensure that all hosting providers, infrastructure providers, and subcontractors cooperate with the Contracting Authority in the exercise of step-in rights, including by facilitating direct access to infrastructure accounts and services.

The Contractor shall include in all agreements with hosting providers and subcontractors an obligation to cooperate with any step-in exercise notified by the Contracting Authority. Step-in does not constitute termination unless the Contracting Authority expressly elects to terminate.

- 45.3 The Contractor shall, for not less than 12 months following expiry or termination for any reason, provide transition assistance comprising:
- a) availability of key technical personnel nominated at contract commencement or as updated during the execution of the contract;
 - b) all operational data in open, machine-readable formats;
 - c) full documentation of operational procedures, system administration tasks, and escalation protocols;
 - d) incident response playbooks covering all major incident categories;
 - e) operational runbooks for all routine and non-routine system operations;
 - f) monitoring configuration documentation including alert thresholds, dashboards, and on-call protocols; and
 - g) active cooperation with the successor contractor's onboarding programme.

The Contracting Authority shall reimburse the Contractor's reasonable costs at market rates.

Article 46: Wallet Orchestration Control and Runtime Independence

- 46.1 The Contractor shall ensure that the Solution does not create any dependency on vendor-operated orchestration services, proprietary runtime control platforms, or external infrastructure that cannot be independently deployed and operated by the Contracting Authority or a successor contractor.
- a) Orchestration Independence. The Orchestration Layer in its entirety shall be fully deployable and operable by the Contracting Authority or a successor contractor without reliance on vendor-operated infrastructure. All components of the Orchestration Layer shall be delivered as Bespoke Deliverables under Section 2 Clause 14.5.
 - b) Open Interfaces. All orchestration services shall expose their interfaces through documented open APIs using standard protocols. No component of the Orchestration Layer shall communicate using proprietary or undocumented protocols.
 - c) Architectural Compliance. The Contractor shall, at the commencement of the design phase and again before system acceptance, provide a written attestation that the architecture complies with (a) and (b) above. The Contracting Authority may engage an independent technical reviewer to verify this. Acceptance of the system design and final system is conditional on compliance with this clause.

Article 47: Incident Reporting

- 47.1 The Contractor shall notify the Contracting Authority immediately, and in any event within two (2) hours, of any actual or suspected Security Incident, including a description of the incident, its known or suspected cause, and remediation steps. The Contractor shall provide all information and cooperation required by the Contracting Authority to comply with its obligations under applicable EU and National legislation and shall cooperate with any supervisory investigation arising from a Security Incident. This clause survives expiry or termination.

Article 48: Delivery of Equipment

- 48.1 The Contractor shall deliver the equipment in accordance with the conditions of the contract. The equipment shall be packaged so as to prevent their damage or deterioration in transit to their destination.
- 48.2 The Contractor shall provide such packaging of equipment as is required to prevent their damage or deterioration in transit to their destination as indicated in the contract. The packaging shall be sufficient to withstand, without limitation, rough handling, exposure to extreme temperatures, salt and precipitation during transit and open storage. Package size and weight shall take into consideration, where appropriate, the remoteness of the final destination of the equipment, and the possible absence of heavy handling facilities at all points in transit.
- All equipment shall be packed in sturdy packages to eliminate damage due to logistical arrangements up to the destination and accordingly marked and labelled with regard to the handling procedures during transit.
- 48.3 The packaging, marking and documentation inside and outside the packages shall remain the property of the Contractor, subject to any modifications subsequently ordered by the Project Manager, and subject to respect for the environment.
- 48.4 No equipment shall be shipped or delivered to the place of acceptance unless the Contractor has advised the Contracting Authority as least twenty-one (21) calendar days in advance. The Contractor shall be responsible for the delivery at the place of acceptance of all supplies and supplier's equipment required for the purpose of the contract.
- 48.5 Each delivery must be accompanied by a statement drawn up by the Contractor, comprising of a packing list and other delivery documents which are to clearly indicate the Contract Number.
- 48.6 Each package shall be clearly marked, as agreed upon with the Contracting Authority.

Article 49: Verification and Handing Over of Equipment

- 49.1 Upon successful completion of Milestone 16, the Contracting Authority shall accept and take ownership of all the equipment by issuing a certificate of acceptance.
- 49.2 The Contracting Authority shall, during the progress of the delivery of the equipment and before the equipment is taken over, have the power to order or decide:
- a) the removal from the place of acceptance, within such time or times as may be specified in the order, of any equipment which, in the opinion of the Contracting Authority, is not in accordance with the contract;
 - b) their replacement with proper and suitable equipment;

c) the removal and proper re-installation, notwithstanding any previous test thereof or payment thereof, of any installation which in respect of materials, workmanship or design for which the Contractor is responsible, is not, in the opinion of the Contracting Authority, in accordance with the contract;

d) that any work done or equipment supplied or materials used by the Contractor is or are not in accordance with the contract, or that the equipment or any portion thereof do not fulfil the requirements of the contract.

49.3 The Contractor shall, with all speed and at his own expense, make good the defects so specified. If the Contractor does not comply with such order, the Contracting Authority shall be entitled to employ other persons to carry out the orders and all expenses consequent thereon or incidental thereto shall be deducted by the Contracting Authority from any monies due or which may become due to the Contractor.

49.4 Equipment which is not of the required quality shall be rejected. A special mark may be applied to the rejected equipment. This shall not be such as to alter them or affect their commercial value. Rejected equipment shall be removed by the Contractor from the place of acceptance, if the Project Manager so requires, within a period which the Project Manager shall specify, failing which they shall be removed as of right, at the expense and risk of the Contractor. Any deliveries incorporating rejected materials shall be rejected.

Article 50: Equipment Warranty Obligations

50.1 The Contractor shall warrant that the equipment is new, unused, of the most recent models and incorporate all recent improvements in design and materials, unless otherwise provided in the contract. The Contractor shall further warrant that all equipment shall have no defect arising from design, materials or workmanship, except insofar as the design or materials are required by the specifications, or from any act or omission, that may develop under use of the equipment in the conditions obtaining in the country of the Contracting Authority.

The equipment is to be warranted during the entire duration of the contract, or covered with a support agreement where that is not possible for the entire contract duration, for full parts and labour, onsite service, software updates; such period is defined as the warranty period. If any equipment, including but not limited to HSMs, appliances, modules, firmware, software, or related components, reaches End-of-Life, End-of-Sale, or End-of-Support during the duration of the contract, the Contractor shall, at its own cost and without degradation of service, replace the affected equipment with an equivalent or superior supported model subject to approval by the Contracting Authority. The replacement shall maintain compatibility with the existing Solution. The Contractor shall provide prior written notice of any End-of-Life or End-of-Support event and shall complete the replacement or upgrade before support expires, ensuring continuity of warranty, maintenance, firmware updates, security patches, and vendor support.

The Contractor shall be fully responsible for the manufacturer's warranty in respect of proper design, quality and workmanship of all equipment and accessories covered by the tender for the above period.

50.2 The Contractor shall be responsible for making good any defect in, or damage to, any part of the equipment which may appear or occur during the warranty period and which:

a) results from the use of defective materials, faulty workmanship or design of the Contractor; or

- b) results from any act or omission of the Contractor during the warranty period; or
- c) appears in the course of an inspection made by, or on behalf of, the Contracting Authority.

50.3 The Contractor shall at his own cost make good the defect or damage as soon as practicable. The warranty period for any items replaced or repaired shall recommence from the date on which the replacement or repair was made to the satisfaction of the Contracting Authority.

50.4 If any such defect appears or such damage occurs during the warranty period, the Contracting Authority shall notify the Contractor. If the Contractor fails to remedy a defect or damage within the time limit stipulated in the notification, the Contracting Authority may, with the approval of the Central Government Authority:

a) remedy the defect or the damage itself, or employ someone else to carry out the work at the Contractor's risk and cost, in which case the costs incurred by the Contracting Authority shall be deducted from monies due to or guarantees held against the Contractor or from both; or

b) terminate the contract.



SECTION 3 - SPECIFICATIONS / TERMS OF REFERENCE (Note 3)

1. Background Information

1.1 - Beneficiary Country

Malta.

1.2 - Central Government Authority

Department of Contracts.

1.3 - Contracting Authority

Malta Digital Innovation Authority.

1.4 - Relevant Country Background

The Maltese Islands are geographically located in the centre of the Mediterranean Sea, south of Sicily. The Islands have a total land area of 316 km² and comprise 3 main islands - Malta (246 km²), Gozo (67 km²) and Comino (2.7 km²). According to the National Statistics Office, the estimated total population of Malta and Gozo at the end of 2024 stood at 574,250, up by 1.9 per cent when compared to the previous year. This makes it one of the most densely populated countries in Europe.

1.5 - Current State of Affairs in the Relevant Sector

The European Digital Identity Wallet (EUDIW) is being developed under the updated eIDAS 2.0 Regulation (EU 2024/1183), which entered into force in May 2024. All EU Member States must provide at least one compliant wallet by December 2026. The Malta Digital Innovation Authority (MDIA) has been entrusted with the role of business owner for the European Digital Identity (EUDI) Wallet initiative. This project represents a significant step forward in secure digital identity management across the EU.

Member States' digital identity infrastructures are therefore undergoing rapid alignment with the EU's common Architecture and Reference Framework (ARF) and Implementing Acts, which define technical, security and interoperability requirements. Organisational structures in this sector originate from earlier national eID schemes, which were often not easily reusable cross-border. The European Digital Identity Wallet aims to address this by introducing shared legal, governance, and technical foundations across all Member States. Large-Scale Pilot projects (e.g., POTENTIAL, EWC, NOBID, DC4EU) have validated interoperability, cross-border use cases (e-government, banking, mobile driving licence, e-prescription, payments), and key governance lessons between 2024-2025.

Member States must issue wallets, onboard users, certify wallet providers, issue high-assurance attributes, and ensure their public-sector online services accept any EUDIW. Infrastructure development is progressing, supported by the ARF, reference implementations, shared testing infrastructures, and cross-border pilot networks. Information flows are becoming more structured through EU guidance, common standards, and coordinated conformance testing.

While industry readiness is increasing—particularly in sectors that will face legal obligations—adoption remains the largest challenge. Public trust, digital literacy, and visible user benefits strongly influence uptake.

1.6 - Related Programmes and Donor Activities

The MDIA is an Authority operating at the intersection of innovation and technology. The MDIA is tasked to foster the uptake of innovative technology in a secure manner, which interalia include Artificial Intelligence (AI), Distributed Ledger Technology (DLT), Big Data, Internet of Things (IoT), and innovative Digital Identity Solutions. It aims to do this by imbuing the right Laws and Regulation to stimulate the industry, protect the users and promote innovation in Malta.

The Maltese implementation of the European Digital Identity Wallet (EUDIW) will leverage existing solutions such as the existing national electronic identity (eID) system which has been notified at a level of assurance high. The current eID infrastructure will serve a key role in the authentication layer, enabling secure identity verification and ensuring continuity with established national identity services. This will allow Malta to then pivot into a new solution ensuring that citizens and residents alike benefit from an easy-to-use, secure-by-design and privacy-preserving solution.

2. Contract Objectives and Expected Results

2.1 - Overall Objectives

The overall objectives of the project of which this contract will be a part are as follows:

Implementation and roll out of a Maltese European Digital Identity Wallet ecosystem that complies with the [EUDI Regulation] and all applicable Implementing Acts.

The overall objectives will be achieved in different phases:

- Design, develop, test, deploy and operate Malta's first national mobile application to store digital documents. Via this mobile application the users can authenticate with the Maltese eID server, store identification data downloaded following the authentication with the Maltese eID server, include age verification functionality, at least two (2) use cases, and the ability to store, present and share digital information securely. This app is to use approved branding in both Maltese and English and in line with accessibility directive - Version 1.
- Design, develop, test, deploy and operate Malta's Wallet Solution building, where technically possible, on the work done in Version 1. This Wallet Solution will use the existing Maltese eID Cards (for citizens and residents) and the keys they contain (i.e. the authentication key and the signing key). It includes the design, development, testing, deployment and operation of a Solution incorporating a Signing Certificate Provider, Wallet Relying Party Access Certificate Authority, PID Provider, Relying Party Registrar, Signature Creation Application and Wallet Provider using Remote HSMs as the Wallet Secure Cryptographic Device - Version 2.
- The Contracting Authority aims to have a fully compliant and certifiable EUDIW at the end of Version 2 of the project.
- In the future, the solution may be upgraded to include the migration to a remote QSCD for qualified electronic signatures created by the EUDIW, and the use of certified Secure Elements as they become generally available on mobile devices. This third phase is not in scope of this contract, but as far as possible the investments in this contract will be re-used in the future.

2.2 - Specific Objectives

The objectives of this contract (which are not necessarily those of the project) are as follows:

- Design a mobile application for storing digital documents and enable new digital services.
 - This mobile application may not necessarily be compliant with the [EUDI Regulation] but will leverage existing infrastructure where possible providing citizens and residents access to a secure mobile app in the shortest timeframe possible.

- Design, testing and deployment of this mobile application.
- Test the system thoroughly and assist with integration into the national setup, including the eID server and as necessary for the use cases.
- Operate, maintain and support to ensure that the users have uninterrupted access to a secure and privacy-preserving application.
- Design a solution based on the high-level technical architectures provided and compatible with the systems currently in place.
 - Implement the necessary components for an EUDIW ecosystem compliant with the [EUDI Regulation] and all applicable Implementing Acts.
 - Test the system thoroughly and assist with integration into the national setup.
 - Support the contracting authority with the certification of the solution.
 - Design, testing and deployment of this Version 2.
 - Roll out use cases based on regulatory obligations and national priorities.
 - Operate, maintain and support to ensure that the Maltese EUDIW users have uninterrupted access to a secure and privacy-preserving Solution.
- Support in the transition from Version 1 to Version 2, providing a user-friendly experience when migrating to Version 2.

2.3 - Results to be achieved by the Awarded Bidder

1. Design, develop and deploy a mobile application (Version 1) through which users can authenticate with the Maltese eID server, offer age verification functionality, at least two (2) use cases and allow the users to store, present and share digital information if their device allows it.
2. Go live of the mobile application (Version 1) should not exceed six (6) months from commencement date.
3. Design, develop and deploy a Wallet Solution (Version 2) that integrates successfully a number of different components developed according to the [EUDI Regulation] and relevant Implementing Acts. These components include the Wallet Provider's Backend, Wallet apps, Remote HSMs, PID Provider's Component, Relying Party Registrar, Signature Creation Application Signing Certificate Provider's components, Signature Creation Application and Wallet Relying Party Access Certificate Authority's component. This solution relies on the existing eID Card and the keys it contains and uses Remote HSMs as one of the Wallet Secure Cryptographic Devices.
4. The solution should ensure unlinkability, cross-border interoperability and the use of pseudonyms.
5. The provision of support to certify the various components in line with national and EU certification schemes. This is to be achieved within twenty-one (21) months from commencement date.
6. The provision of operation and maintenance support of the solution in production stage at any particular instance.
7. Age verification, authenticating online and in person and signing of documents.
8. The provision of technical documents for each component developed.
9. The provision of additional use cases to be added as needed by the Contracting Authority based on national priorities and obligations arising from EU legislation.

These may be presented either in order of importance or in chronological order, as appropriate.

3. Assumptions and Risks

3.1 - Assumptions Underlying the Project Intervention

It is assumed by the Contracting Authority that the Awarded Bidder and Key Experts and any supporting staff:

- i. can communicate verbally, orally and that they have good writing skills in English and/or Maltese;
- ii. are flexible and capable of respecting specific targets and adherence to the proposed deadlines without jeopardising the quality of work;

- iii. will develop a schedule and schedule management plan, a quality management plan, a resource management plan and a project management plan;
- iv. any travel undertaken by the Awarded Bidder and the Awarded Bidder's experts is at the cost of the Awarded Bidder.

The Awarded Bidder is expected to:

- i. be capable of overcoming hurdles that may arise during the course of development and implementation, to ensure timely and cost-effective delivery as per milestones stipulated and by the end of the contract period as applicable;
- ii. keep up to date with policy developments underway at national and EU level throughout the execution of the contract;
- iii. keep up to date with the development of new and applicable standards and any revisions to existing relevant standards;
- iv. keep up to date with changes to the ARF and discuss such changes with the Contracting Authority;
- v. conduct information collection practices and methodologies which adhere with the relevant data protection regulations;
- vi. the Awarded Bidder shall treat all documents and information received in connection with the contract as private and confidential, and shall not, save in so far as may be necessary for the purposes of the performance therefor, publish or disclose any information;
- vii. adhere to applicable legislation and best practice concerning the services in accordance with applicable Maltese and European legislation;
- viii. thoroughly read and familiarise itself with all pertinent regulations, legislation and standards, understand the content and context and adhere to the conditions in these documents. In the event of any difficulties the Contracting Authority assumes that the Awarded Bidder shall bring these to the attention of the Contracting Authority prior to the commencement of the project;
- ix. provide the necessary resources and adequate number of personnel to satisfy the services required by the Contracting Authority within the time-frame provided;
- x. respect time-frames as indicated by the Contracting Authority;
- xi. be available until completion of the contract and shall furthermore provide post-consultancy feedback/clarifications to the Contracting Authority;
- xii. the Awarded Bidder shall perform the services under the contract with due care, efficiency and diligence, in accordance with the best professional practice.
- xiii. the Awarded Bidder shall deliver work of high quality;
- xiv. conduct the work in an ethical manner throughout, particularly when in direct contact with the Contracting Authority and other Public Bodies; and
- xv. obtain a licence for the Contracting Authority and users of the Software solution to use the solution, to the extent that such Software solution uses third party software.
- xvi. the Awarded Bidder shall refrain from making any public statements without the prior approval of the Contracting Authority, and from engaging in any activity which conflicts with the obligations towards the Contracting Authority under the contract.
- xvii. the payments to the Awarded Bidder under the contract shall constitute the only income or benefit it may derive in connection with the contract and neither it nor its personnel shall accept any commission, discount, allowance, direct payment or other consideration in connection with or relation to, or in discharge of, its obligations under the contract.

The Awarded Bidder must ensure the availability of the required expertise including the adequate skills and the necessary resources for the duration of the contract.

3.2 – Risks

1. Time limits may not be used as a justification for sub-standard work or unachieved deliverables. It is expected that the Awarded Bidder has sufficient organisational capacity to handle pressure, maintain high quality research standards and deliver on time.

2. Stakeholders may not be prompt in their provision of responses and/or information.
3. Not all information may be available or easily accessible.
4. There may be situations where a host system does not exist or where interfacing platforms to the existing systems are not in place yet.

4. Scope of the Work

4.1 – General

4.1.1 Project Description

As per Article 5a (1 to 3) of [EUDI Regulation], Malta will provide a EUDIW to its citizens and residents. EUDIW can be provided directly by a MS, under a mandate from a MS, or independently of the MS but recognised by that MS. The EUDIW is planned to ensure privacy and security by design, with a focus on user-centricity and interoperability. While the use of the Wallet is not mandatory for the citizens and residents, it will be available free of charge and be accessible to people with disabilities.

In Malta, the provision of the EUDIW will follow the following phases:

1. Design, develop, build and deploy Version 1 through which the User can authenticate with the eID server, store identification data downloaded following the authentication with the eID server, include age verification functionality, at least two (2) use cases, and store, present and share digital information securely. This application is to use approved branding in both Maltese and English, in line with the Accessibility directive within six (6) months from the signing of the contract.
2. Within twenty-one (21) months from signing of the contract design, develop, build, assist with certification and deploy Version 2 of the Solution with the necessary integration and exchanges between the Wallet Provider, Signing Certificate Provider, Wallet Relying Party Access Certificate Authority, PID Provider, Relying Party Registrar and Wallet Solution including the verifier components and SCA. Version 2 shall still include the functionality from Version 1 (age verification and at least two (2) use cases), relies on the existing eID Card and the keys it contains and uses a Remote WSCD.

For both phases, the Contracting Authority is seeking to introduce additional digital services, with these new use cases being added as needed based on national priorities and obligations arising from EU legislation. These use cases are additional to the functionalities incorporated in Version 1 and Version 2. Re-usability of any developed software should be prioritised to reduce repetition of work.

4.1.2 Geographical Area to be covered

Malta, with cross-border compatibility with the EU.

4.1.3 Target Groups

The mobile application (Version 1) and the EUDIW (Version 2) is intended for Maltese citizens and residents, enabling secure access to digital services within Malta and across the EU. Interoperability is essential - not only for seamless use within Malta, but also to support cross-border functionality.

Through the wallet, users will be able to authenticate themselves when interacting with public and private services in other EU Member States, present verified identity credentials and attributes, and validate digital identity documents issued by other Member States. This is made possible through the common standards defined in the EU's Architecture and Reference Framework (ARF).

All Maltese citizens and residents in possession of an e-ID card or residence document.

4.1.4

Definitions

1. 'eID Card' means the electronic Identity Card issued to citizens of Malta also generally referring to the eResidence Permit Card and Document respectively issued to third country nationals and European citizens who reside in Malta;
2. 'Wallet Secure Cryptographic Application' (WSCA) means an application that manages critical assets by being linked to and using the cryptographic and non-cryptographic functions provided by the WSCD;
3. 'Wallet Unit' means a unique configuration of a Wallet Solution that includes the Wallet Instance, WSCA and WSCD provided by the Wallet Provider to a Wallet User;
4. 'Critical assets' means assets within or in relation to a Wallet Unit of such extraordinary importance that where their availability, confidentiality or integrity are compromised, this would have a very serious, debilitating effect on the ability to rely on the Wallet Unit;
5. 'PID Provider' means the architectural component responsible for issuing and revoking the person identification data and ensuring that the person identification data of a user is cryptographically bound to a Wallet Unit;
6. 'User' means a user who is in control of the mobile application developed in Version 1;
7. 'Wallet User' means a user who is in control of the Wallet Unit developed in Version 2;
8. 'Relying Party' means a party that intends to rely upon Wallet Units for the provision of public or private services by means of digital interaction;
9. 'Secure Element' (SE) means a tamper-resistant hardware component used to securely store and process sensitive data, such as cryptographic keys, personal identification numbers (PINs), and payment credentials.
10. 'Solution' means the complete and integrated set of components, systems, services, and deliverables proposed and provided by the awarded bidder to fully meet the functional, technical, operational, and compliance requirements as specified in this document. NOTE: Solution is broader than Wallet Solution and covers all elements depicted in the present document, including, e.g., the PKI, the hosting facilities, etc., that are necessary for the Wallet ecosystem but not necessarily part of, or dedicated to, the Wallet Solution.
11. 'Trusted Execution Environment' (TEE) means a secure area within a main processor that ensures sensitive data is stored, processed, and protected in an isolated and trusted environment;
12. 'Wallet Provider' means the component which provides the Wallet Solution;
13. 'Wallet Unit Attestation' (WUA) means a data object that describes the components of the Wallet Unit or allows authentication and validation of those components;
14. 'Wallet Instance' means the application installed and configured on a Wallet User's device or environment, which is part of a Wallet Unit, and that the Wallet User uses to interact with the Wallet Unit;
15. 'Wallet Instance Attestation' (WIA) means a data object that attests to the authenticity and integrity of a Wallet Instance running on a device;
16. 'Wallet Solution' means a combination of software, hardware, services, settings, and configurations, including the Wallet Instance, one or more WSCA and one or more WSCD;
17. 'Wallet Secure Cryptographic Device' (WSCD) means a tamper-resistant device that provides an environment that is linked to and used by the WSCA to protect critical assets and provide cryptographic functions for the secure execution of critical operations;
18. 'Wallet cryptographic operation' means a cryptographic mechanism necessary in the context of authentication of the wallet user and the issuance or presentation of person identification data or electronic attestations of attributes;

19. 'Wallet Relying Party Access Certificate' (WRPAC) means a certificate for electronic seals or signatures authenticating and validating the Relying Party issued by a provider of such certificates;
20. 'Wallet Relying Party Access Certificate Provider' (WRPAC Provider) means a component that issues WRPAC to Relying Parties registered in that Member State.

4.2 Specific Activities

4.2.1 Details on the different project versions

4.2.1.1 Version 1 - Malta's national mobile application for storing digital documents

Version 1 will be an initial standalone mobile application intended to provide baseline functionality. In particular, it will provide age verification functionality which is to preferably follow the Age Verification Application user journey, as outlined in the European Age Verification Solution blueprint.

Users log in using the existing Malta's national eID infrastructure, which at minimum uses LoA Substantial with the option to use LoA High. Having Version 1 use LoA High authentication on launch will make the transition to Version 2 smoother for the end users, hence it is preferred that the awarded bidder integrates LoA High authentication in Version 1.

The app will offer age verification functionality, whereby a user would be able to retrieve, and then present proof related to one's age, without providing any other details or the actual age itself. This mobile application may not necessarily be compliant with the [EUDI Regulation] but will leverage existing infrastructure where possible, to provide citizens and residents access to a secure mobile app in the shortest timeframe possible.

The user begins by installing the mobile application and authenticating using the national eID system. Once authenticated, the user then goes through an activation process in which a Proof of Age attestation is issued. The app retrieves verified age information from an authentic source and stores a cryptographically secured Proof of Age attestation on the device. The process is designed to be privacy preserving: the proof asserts only whether the user meets a specific age threshold (e.g. "over 18") without exposing the actual age or any other personal attributes. The application can then be used to verify one's age using the proofs obtained when accessing an online service requiring age verification. Presentation is optimised for secure online flows, enabling fast, minimal-data sharing interactions between the user and the relying party.

In addition to the age verification functionality, the Awarded Bidder shall also prioritise the integration of at least two (2) high-frequency usage, low-complexity use cases (daily-life use cases), as determined by the Contracting Authority, that demonstrate immediate utility to the end user. The Solution must support 'out-of-the-box' templates for common data attributes to minimise integration time for service providers who will make use of the app.

The application must be created for both the Android and iOS platforms and be published on the Google Play Store and Apple App Store respectively. It must also support gathering anonymised analytics to benchmark the KPIs using privacy by design principles, and backend functionality must be hosted within the MITA's Off-Premise Hybrid Cloud Platform (Microsoft Azure).

The application must also incorporate Maltese-specific branding, in line with the Accessibility directive, across all user-facing elements, including the app name, store descriptions, icons, splash screens, and visual themes.

The awarded bidder will be expected to design, test, and deploy the mobile application. They will be required to test the system thoroughly and assist with integration into the national setup, including the eID server and as necessary for the use cases. The awarded

bidder will also be expected to operate, maintain and support the application to ensure uninterrupted access to the application by the users.

4.2.1.2 *Version 2 - Wallet Solution functionalities*

The Version 2 Wallet Solution shall be conformant to the applicable requirements in the [EUDI Regulation]. In particular, the basic functionalities of the EUDIW are legally defined. According to Article 5a of [EUDI Regulation], the Wallet Solution provided by the awarded bidder shall be an EUDIW such that:

- 1) Under their sole control, Wallet Users shall be able to securely **request, obtain, select, combine, store, delete, share** and **present** PIDs and EAAs (including EAAs with embedded disclosure policies), to **authenticate** to Relying Parties (RPs) online and, where appropriate, offline, all while ensuring that selective disclosure is possible (item 4(a));
- 2) RPs shall be **authenticated** and **identified** in accordance with Article 5b of [EUDI Regulation] (item 5(a)(viii));
- 3) RPs shall be able to **request** and **validate** the PIDs/EAs belonging to Wallet Users, and to **verify** the authenticity and validity of EUDIWs they request them from (items 5(a)(ii) and 5(a)(viii));
- 4) Wallet Users shall be able to **generate pseudonyms** and **store** them encrypted and locally within the EUDIW (item 4(b));
- 5) Wallet Users shall be able to **authenticate** another user's EUDIW, and **receive** and **share** PID and EAAs in a secure way **between two EUDIWs**, as well as **validate** them (item 4(c));
- 6) Wallet Users shall be able to **access a log** of all transactions carried out through their EUDIW via a common Dashboard, enabling users to:
 - a) **view** an up-to-date list of RPs with which they connected and, where applicable, all data exchanged (item 4(d)(i));
 - b) easily **request erasure** by a RP of personal data pursuant to Article 17 of [GDPR] (item 4(d)(ii));
 - c) easily **report** a RP to the competent national data protection authority, where an allegedly unlawful or suspicious request for data is received (item 4(d)(iii));
- 7) Wallet Users shall be able to **sign** by means of qualified electronic signatures, free of charge (item 4(e)). This functionality may be limited by the MS to signatures for non-professional purposes;
- 8) Wallet Users shall be able to **download** their data, EAAs, and configurations, where technically feasible (item 4(f));
- 9) Wallet Users shall be able to **exercise their rights** to data portability (item 4(g));
- 10) Wallet Users shall be able to **display** an EUDIW Trust Mark (item 5(a)(iv));
- 11) Wallet Users shall be **uniquely represented** by the PID available from the eID scheme under which the EUDIW is provided (item 5(f));
- 12) Wallet Users shall be able to **revoke** their EUDIW upon explicit request. The EUDIW can also be revoked by the Wallet Provider in case the security has been compromised or in case of death of the user (item 9);
- 13) Wallet Users shall be able to easily **request technical support** and **report technical problems** and other incidents (item 10);
- 14) The EUDIW is **secure by-design** (item 12).

The EUDIW shall be **provided under an eID scheme** with LoA high, and users shall be able to **securely onboard** by using an eID means in accordance with Article 5a(24) of [EUDI Regulation] (items 5(a)(v) and 11). The use of the eID means shall meet the requirements set out in Article 8 of [EUDI Regulation] with regards to **LoA high** (item 5(d)). In Malta, the EUDIW shall be based on the national eID card scheme as described hereunder, which is notified at

a High Level of Assurance in accordance with Opinion No. 1/2021¹ of the Cooperation Network under the [EUDI Regulation].

In addition to these functionalities, it is appropriate to provide additional functionalities to the EUDIW, including interoperability with **existing eID** means, as long as those functionalities comply with Article 5a of [EUDI Regulation]. In the case of Malta, interoperability with the eID Card is mandatory, as it will be used to onboard users at all stages of the EUDIW.

EUDIWs shall support common protocols and interfaces that allow all the functionalities mentioned above, as per Article 5a(5) of [EUDI Regulation]. The common protocols and interfaces are further specified in [CIR 2024/2982].

In accordance with Article 5a(8) of the [EUDI Regulation], Member States are required to provide free validation mechanisms to verify the authenticity and validity of EUDIWs, as well as to enable users to confirm the authenticity and validity of the identities of registered RPs. The development of such a validation tool falls within the scope of this project.

Some general principles are to be kept in mind when designing the EUDIW. One of the main focuses is to ensure security by design and by default, and to ensure no information on users is collected without their permission (see Article 5a(12-14-16-17) of [EUDI Regulation]).

Another requirement is that the EUDIW is available free of charge (by Article 5a(13) of [EUDI Regulation]) and is accessible for people with disabilities (by Article 5a(21) of [EUDI Regulation]).

The solution needs to be compliant with the [EUDI Regulation], and all relevant Commission Implementing Regulations including but not limited to [CIR 2015/1502], [GDPR] and other relevant EU and national legislations. The awarded bidder is expected to allocate a minimum of seven thousand (7,000) Person Hours in consultancy services to the Contracting Authority on changes stemming from new Legislation, Implementing Acts and Standards, empowering the Contracting Authority to take decisions in relation to the Solution. Usage of these hours or part thereof will be agreed upon between the Contracting Authority and the Contractor on a case-by-case basis, including delivery deadlines.

4.2.1.3 Requirements common to Version 1 and Version 2

4.2.1.3.1 *Separation of Environments*

The awarded bidder shall provision, configure, and maintain a dedicated staging environment that is logically and physically separate from both the development and production environments. This staging environment shall be used for pre-production testing, quality assurance, and validation purposes, and must closely mirror the production environment in terms of configuration, performance, and security controls.

4.2.1.3.2 *User Experience Commitment*

The awarded bidder shall ensure that the design of the mobile application (Version 1) and the EUDIW Solution (Version 2) is user-centric, visually appealing, and aligned with the latest trends in digital product design and user experience (UX). The UX shall support both English and Maltese language options. To this end, the awarded bidder commits to:

- Applying contemporary design principles, including accessibility, responsiveness, and intuitive navigation. The Wallet Unit shall comply with applicable requirements and standards in the Directive 2016/2102 on the accessibility of website and mobile applications of public sector bodies, including compliance with European Standard ETSI

¹ [Opinion No. 1/2021 - eID User Community -](#)

EN 301 549 v1.1.2. The Wallet Unit shall comply with accessibility requirements for products and services established under Directive 2019/882;

- Conducting user research and usability testing to validate design decisions;
- Incorporating feedback from diverse user groups to ensure inclusivity and appeal;
- Staying abreast of evolving design standards and best practices within the EU digital identity ecosystem and beyond;
- Collaborating with relevant stakeholders to ensure the visual and functional design reflects the values of trust, security, and innovation.

Throughout the contract duration, the awarded bidder shall perform a design refresh at three (3)-year intervals. The final design(s) of the public-facing components of the solution and any subsequent design refresh shall be subject to review and approval by the Contracting Authority. The Contracting Authority shall be actively engaged during the UX's design stage.

The above is applicable to any public facing interface of the Solution.

4.2.1.3.3 *Age Verification*

The mobile application (Version 1), and the EUDIW (Version 2) (which for Version 2 is without prejudice to the complete implementation of Section 3 Clause 4.2.3.5) shall provide a privacy-preserving Age Verification use case to relying parties that require confirmation of a user's age, such as verifying that a user is 18 years or older, without disclosing the user's full date of birth or other personal details. This service shall utilise the verified date of birth and apply selective disclosure techniques to generate cryptographic proofs of age eligibility. Relying parties will be able to request and receive a simple "Yes/No" confirmation that the user meets the required age threshold, ensuring compliance with legal or service-specific age restrictions while fully respecting the principles of data minimisation and user consent.

4.2.1.3.4 *Branding*

The awarded bidder is responsible of the design, development and update along the years of the Solution's branding. This includes, but is not limited to, logos, colour schemes, fonts, naming, dark and light themes for the mobile applications, social media templates and presentation templates, and any artwork. The awarded bidder is to consult continuously with the Contracting Authority, providing a minimum of five proposals. The Contracting Authority has final say on the branding chosen. The IP of the branding is to be owned by the Contracting Authority.

4.2.1.3.5 *Mobile Application and Wallet Instance Installation*

The awarded bidder shall make the mobile application (Version 1), and the Wallet Solution (Version 2) available for installation only via the official app store of the relevant operating system (e.g., Android, iOS).

4.2.1.3.6 *Support for uptake*

The Contracting Authority is committed to rapidly promoting the uptake of Version 1 and Version 2 and expects the awarded bidder to actively support this strategic objective.

The Contractor shall support and contribute to the adoption of key additional digital services that will act as flagship use cases for Version 1 and Version 2, demonstrating added value and functionality to citizens, residents and service providers. These services will serve as the primary drivers of adoption and visibility, and their successful integration will be critical to

the overall rollout strategy. The Contracting Authority will inform the Awarded Bidder of which use cases will be implemented and their respective timelines. The Awarded Bidder is expected to allocate a minimum of twenty thousand (20,000) Person Hours in development services for implementing these use cases. Usage of these hours or part thereof will be agreed upon between the Contracting Authority and the Contractor on a case-by-case basis, including delivery deadlines, except for where otherwise stated in the Section 2, Article 18.2.

In the case of Version 2, the EUDIW Solution provided must be fully capable of supporting the use case scenarios as outlined in the Architecture Reference Framework. To facilitate an accelerated integration process, the awarded bidder shall, at the earliest opportunity following the deployment of the Solution on the staging environment, provide a comprehensive Technical Integration Document. This document must detail the APIs necessary for seamless integration by Relying Parties to the EUDIW. In addition, the awarded bidder shall offer dedicated technical support and guidance to the Contracting Authority and its partners throughout the onboarding process.

Furthermore, to ensure interoperability and trust across Member States, the awarded bidder is required to deliver a Verification Engine, including its complete source code, which will be made available to Relying Parties that are Public Bodies. This engine must enable the validation of credentials presented to Relying Parties by both Maltese and other Member State Wallets, thereby supporting cross-border recognition and compliance with EU standards.

4.2.1.3.7

Secure Development Practices

Software Development Lifecycle

The awarded bidder shall ensure that the Solution is developed using a secure Software Development Lifecycle (SDLC) framework that integrates security considerations at every stage and follows industry standard best-practices from design to deployment and maintenance. It is recommended that this phase follows the ISO/IEC 27034 standard related to application security. Secure configuration and controlled release processes shall be implemented to protect the production environment and data from compromise by development and test activities.

Basic Controls:

- Mandatory threat modelling (e.g. STRIDE) and risk assessments (e.g., DREAD) shall be carried out at each major phase of the SDLC, at a minimum covering the Analysis, Design, Implementation, Testing, Deployment and Operation phases of the EUDIW.
- Use of secure coding guidelines and standards (e.g., OWASP Secure Coding Practices), and framework or language specific best practices.
- Maintained documentation detailing security controls and their assurance levels, mapping of controls to architecture components, and justification of risk coverage.
- Security updates shall be provided and, where applicable, through automatic security updates that are installed within an appropriate timeframe enabled as a default setting, with clear and easy to use opt out mechanisms through the notification of available updates to users.
- Where technically feasible, new security updates shall be provided separately from functionality updates. Where technically feasible, new security updates shall be provided separately from functionality updates.
- A vulnerability management policy meeting the requirements set out in Annex I to the CRA shall be established, maintained, and operated. This policy shall inter alia define

the vulnerability disclosure policy for the Solution and a mechanism for responsible disclosure, including a clear and accessible contact address for reporting vulnerabilities identified in the EUDIW.

- The winning bidder shall ensure that information about fixed vulnerabilities shall be shared and publicly disclosed and registered in accordance with the requirements set out in the CRA. In duly justified cases, where the Wallet Provider considers the security risks of publication to outweigh the security benefits, public disclosure regarding a fixed vulnerability may be delayed until after users have been given the possibility to apply the relevant patch.
- Strict and well documented change management processes with segregation of duties for code deployment, applicable to all planned and emergency changes.
- Logical or physical separation of environments for development, testing, and production shall be maintained. The level of separation necessary should be identified and implemented to prevent inappropriate developer access and ensure a stable testing environment.
- Post-implementation testing shall occur subsequent to system changes, to validate that existing applications and security controls were not compromised. This testing shall include regression checks of affected functionality and verification of any applicable security controls, and may include smoke tests, automated tests, and User Acceptance Testing (UAT).

Test Data

Test information shall be appropriately selected, protected, and managed to ensure the reliability of test results and the confidentiality of operational information. Sensitive information (including personally identifiable information) shall not be copied into the development and testing environments unless absolutely necessary, with documented justification. Sensitive information must only be accessible to personnel with a demonstrated need to know and strictly for the period in which access is required. When operational information is used for testing, the same access control procedures applied to operational environments shall be applied to test environments. A separate authorisation shall be required each time operational information is copied to a test environment. The copying and use of operational information shall be logged to provide an audit trail. Sensitive information shall be protected by removal or masking if used for testing. Operational information shall be properly deleted from a test environment immediately after testing is complete to prevent unauthorised use of test information. Test information shall be securely stored to prevent tampering, which can otherwise lead to invalid results, and only used for testing purposes.

Application Sandboxing and Least Privilege

The EUDIW mobile apps shall operate within a secure sandbox environment provided by the mobile operating system, with minimal permissions. Basic controls:

- Adherence to mobile OS security best practices (e.g., Android Keystore, iOS Keychain for sensitive data).
- The application shall not use techniques that bypass or weaken the native OS sandbox constraints, and shall restrict inter-process communication (e.g., intents, deep links) to trusted components only.
- Strict enforcement of the principle of least privilege for all application permissions, with permissions requested dynamically at runtime where possible and reviewed periodically to remove any that are no longer required.
- Sensitive data shall not be stored or transmitted via insecure shared mechanisms (e.g., clipboard, shared storage) or written to system logs or debug output.

Data Storage Isolation

Sensitive data stored on the mobile device shall be strongly encrypted and isolated from other applications. Basic controls:

- Application-level encryption for all stored sensitive data, regardless of OS-level encryption.
- Sensitive data stored locally shall have defined retention policies and shall be securely erased when no longer required (e.g. on logout or revocation).
- Sensitive data shall not be included in device backups.

Integrity and Anti-Tampering Controls (Mobile Specific)

The mobile applications shall implement measures to detect and prevent tampering and rooting/jailbreaking. Underlying hardware, and all configurations shall be protected against unauthorised modification, in line with the Cyber Resilience Act's requirement to protect the integrity of data, commands, programs and configuration. Basic controls:

- Root/jailbreak detection and appropriate responses (e.g., aborting, disabling sensitive functionality, alerting the user).
- The application shall verify its own code signature at runtime to ensure that it has not been modified or repackaged.
- The application shall implement mechanisms to block screenshots and screen recordings of sensitive information within the app.
- The application shall implement certificate pinning to ensure that communication with backend services cannot be intercepted via forged or untrusted certificates.
- The application shall verify the integrity and authenticity of updates prior to installation, and mechanisms shall be in place to prevent rollback to vulnerable versions.
- The application shall detect execution in emulated or virtualised environments and apply appropriate mitigations (e.g., restricting sensitive functionality).
- Upon detection of tampering or suspicious behaviour, the application shall implement safe response mechanisms, such as shutting down sensitive functions, wiping session data, or logging security events for later analysis.
- Cryptographic hashing and digital signatures for all software components (application, firmware, operating system).
- Secure boot mechanisms for underlying devices.
- Regular integrity checks of critical files and configurations and stored data.

Authentication and Access Control Models

Robust authentication and access control mechanisms are critical for protecting the EUDIW and the sensitive data it contains. Basic controls:

- Protection against brute-force attacks, credential stuffing, and replay attacks and timing.
- Secure PIN policies (complexity, lockout, expiry).
- The log-on procedure shall not display system or application identifiers until the log-on process has been successfully completed.
- A general notice warning that the device should only be accessed by authorised users shall be displayed.
- Help messages during the log-on procedure that would aid an unauthorised user shall not be provided.

- The system shall validate log-on information only on completion of all input data. If an error condition arises, the system shall not indicate which part of the data is correct or incorrect.
- Unsuccessful and successful log-on attempts shall be logged.
- A security event shall be raised if a potential attempted or successful breach of log-on controls is detected.
- Upon successful log-on, the date and time of the previous successful log-on and details of any unsuccessful log-on attempts since the last successful log-on shall be displayed.
- PINs being entered shall not be displayed by default.

Encryption of Data at Rest and in Transit

All sensitive data, both at rest and in transit, shall be encrypted using strong, industry-standard cryptographic algorithms. Basic controls:

- Data at rest (on device, backend servers, storage) shall be encrypted, thereby protecting the confidentiality of stored data as required by the CRA.
- Data in transit shall be protected using strong cipher suites, thereby protecting the confidentiality of stored data as required by the CRA.
- Any encryption algorithms must be reviewed on a biannual basis and updated in line with evolving best practices, emerging threats (such as quantum computing risks), and applicable regulations such as the CRA. The awarded bidder is expected to discuss the outcomes of this review with the Contracting Authority and changes are subject to the Contracting Authority's sign-off.

Security Monitoring Requirements

Continuous security monitoring is essential for detecting, analysing, and responding to security incidents in a timely manner. Comprehensive logging and audit trails shall be maintained for all security-relevant events within the EUDIW ecosystem. A robust incident detection and response capability aligned with ISO 22301 (Business Continuity and Disaster Recovery), shall be in place to handle security incidents effectively. The EUDIW security operations shall leverage threat intelligence to proactively identify and mitigate emerging threats. The winning bidder shall maintain current independent verification of the effectiveness of its technical and organisational security measures. Basic Controls:

- Logging of authentication attempts (success/failure), data access, data modification, key management operations, and administrative actions.
- The system shall report on corruptions to the integrity of stored, transmitted or otherwise processed data, commands, programs and configuration
- Centralised log management with secure aggregation and retention policies to ensure that in the event that the EUDIW is not operational, logs are correlated for investigation purposes and to prevent tampering for integrity purposes.
- Logged information shall at least contain: the time and date of the transaction; the name, contact details, and the unique identifier of the corresponding wallet-relying party and the Member State in which that wallet-relying party is established, or in case of other wallet units, relevant information from the wallet unit attestation; the type or types of data requested and presented in the transaction; in the case of non-completed transactions, the reason for such non-completion.
- Wallet instances shall log reports sent by the wallet user to the data protection authorities via their wallet unit.
- Logs shall be accessible to the Awarded Bidder and the Contracting Authority, where it is necessary for the provision of wallet services, on the basis of explicit prior consent by the wallet user.
- Real-time security monitoring tools (e.g., Security Information and Event Management System (SIEM) with predefined alerts for suspicious activities.
- Defined incident response plan, including roles, responsibilities, and communication protocols.

- Wallet units shall allow wallet users to substantiate reports, including by attaching relevant information to identify wallet-relying parties and claims in machine-readable format.
- Mechanisms to identify and monitor for exfiltration tools.
- Implement tools that enable anomaly and behavioural analytics to detect suspicious activities (e.g., login from an unusual location or device).

4.2.1.3.7.1 *Security Architecture Reviews*

Security architecture reviews shall take place:

- at key SDLC phases (Analysis, Design and prior to Deployment),
- whenever architectural changes occur (e.g. introduction of new components, major upgrades of library dependencies, or changes to cryptographic or privacy mechanisms), and
- regularly during the operational phase.

4.2.1.3.7.2 *Security Testing*

Static Application Security Testing (SAST) and Dynamic Application Security Testing (DAST) shall be executed prior to major releases or deployments.

4.2.1.3.7.3 *Penetration Testing*

Regular penetration testing for systems and applications that store or allow access to data processed (including personal data), covering all components and interfaces, is performed regularly and when significant changes that impact the risk-assessment are made.

4.2.1.3.7.4 *Software Bill of Materials*

Maintained software bill of materials and vulnerability scanning of all dependencies and third-party libraries.

4.2.1.3.7.5 *Security Training*

Industry-recognised and role-appropriate security training for key developers is a requirement. At least one developer on each team must have completed such training prior to commencing work on the project. All developers are expected to undertake such training on a regular basis from that point onwards.

4.2.1.3.7.6 *Configuration Baselines*

Automated secure configuration baselines for all environments (development, testing, production), following hardening guides and industry standards such as CIS (Center for Internet Security) Benchmarks, OWASP Security Best Practices as well as vendor-specific guidelines.

4.2.1.3.7.7 *Version Control*

Version control with an appropriate branching strategy (e.g. GitFlow) for all source code, configurations, and scripts to ensure traceability, integrity and controlled releases.

4.2.1.3.7.8 *Acceptance testing*

User Stories shall contain detailed User Acceptance Criteria following the GHERKIN format or similar. Any system and application changes shall undergo regression testing to meet the defined criteria. Relevant security controls must be included in the User Acceptance Criteria or as their own User Stories where and when applicable.

4.2.1.3.7.9 Dependencies

Minimise external dependencies and third-party SDKs, with thorough security vetting of any that are used and ensuring SDKs are granted only the permissions strictly necessary.

4.2.1.3.7.10 Protected Data Access

Sensitive data stored on the mobile device shall be strongly encrypted and isolated from other applications. Mechanisms may be in place to detect tampering with the secure storage areas or attempts to access protected data outside authorised channels.

4.2.1.3.7.11 Runtime Application Self-Protection

Runtime Application Self-Protection (RASP) capabilities may be in place to detect and react to suspicious activity.

4.2.1.3.7.12 Log Protection

Within all the components, logs shall be protected from unauthorised access, preserving their integrity and availability.

4.2.1.3.7.13 Incident Response Drills

Regular incident response drills and simulations.

4.2.1.3.7.14 Threat Intelligence

Subscription to, and use of, relevant commercial cybersecurity threat intelligence feeds and any other vulnerability databases as stipulated in any relevant EU and national legislation. The bidder is to use at least one sector-relevant commercial feed.

4.2.1.3.7.15 Cybersecurity Audits

Regular audits and assessments of security controls at least annually, using recognised frameworks where applicable in agreement with the Contracting Authority.

4.2.1.3.7.16 Advanced Anomaly Detection

Implement advanced anomaly detection in order to detect any fraudulent behaviour.

4.2.2 Version 2 - Integration with the Maltese Ecosystem

On top of the legal requirements, the Maltese EUDIW shall conform to a specific architecture and shall be able to fit into the Maltese ecosystem. The Maltese EUDIW ecosystem is presented in the High Level Diagram below, and further explanation for each module will be provided in Clause 4.2.3. (in terms of functionalities, interfaces, protocols, etc.). The Contracting Authority wants to store the PID secret key in a centralised and secure Remote Wallet Secure Cryptographic Device ('RWSCD').

The awarded bidder's proposal shall meet the following requirements:

- Secure generation and storage of the PID secret key on the RWSCD.
- PID secret key under the sole control of the user for signing Verifiable Presentations.
- Preservation of user privacy and prevention of replay or denial-of-service attacks.
- Allow for future extensibility of services.

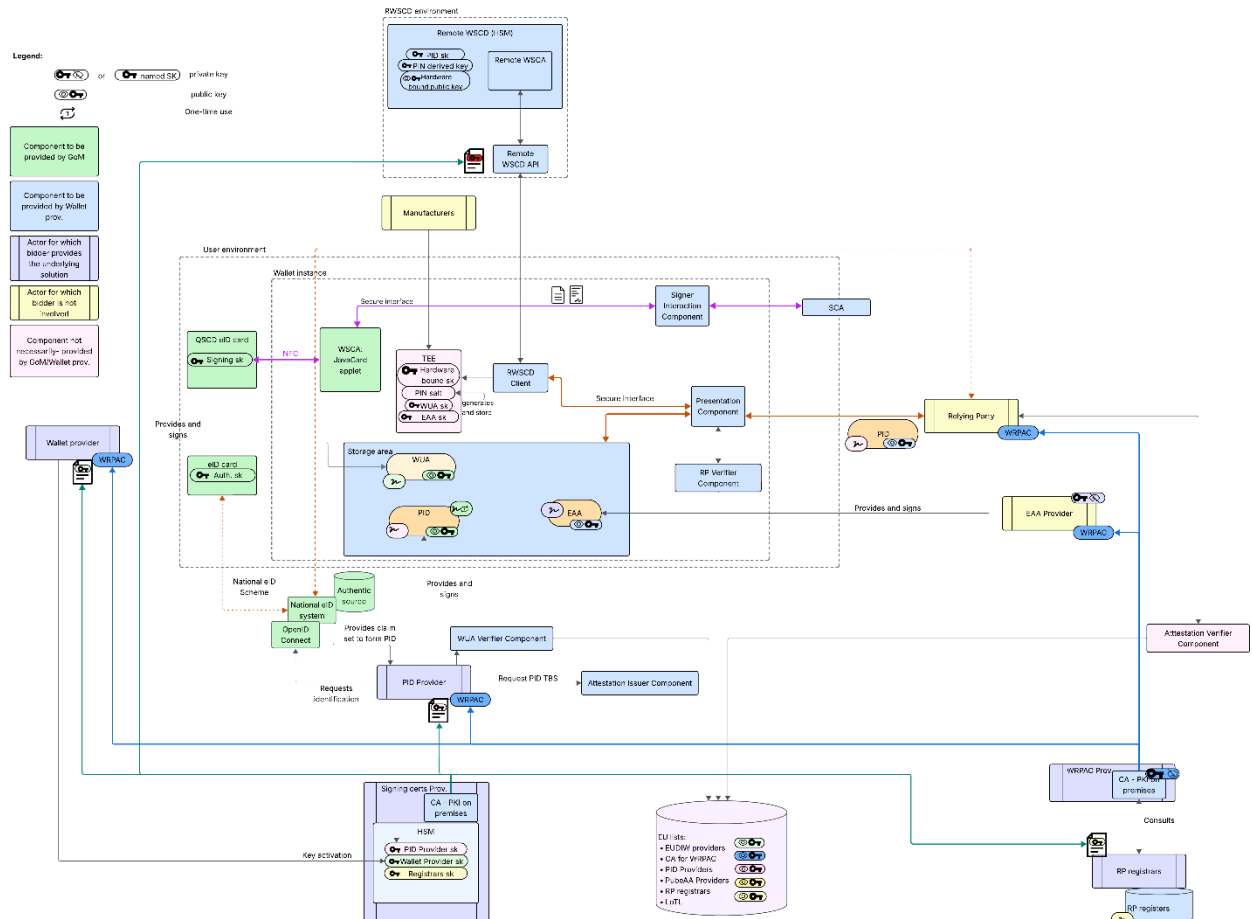


Figure 1: High Level Diagram

The Contracting Authority may permit minor deviations from the proposed technical specifications, provided these are clearly justified by the awarded bidder, do not compromise the overall objectives or integrity of the solution and most importantly guarantee legal compliance with the [EUDI Regulation] and all relevant Implementing Acts. However, the Contracting Authority reserves the right to reject any such deviations at its sole discretion.

The Contracting Authority shall have the flexibility to determine and assign the ownership of individual architectural components to other entities. Accordingly, the Awarded Bidder shall ensure that each component is segregated, at least in logical terms, allowing them to be owned by different entities. The components related to PKI shall be physically segregated from the other components. Therefore, the solution should be designed such that different entities may have access only to the relevant administrative accounts, code repositories, audit logs, backups and access rights configurations. Transfer of ownership of a particular component will imply transfer of rights and obligations.

The RWSCD shall utilise one or more Hardware Security Modules (HSM) to securely manage and protect cryptographic keys, including the PID secret key. The HSMs used must support

[EUDI Regulation] requirements. The RWSCD must provide Service Level Agreements, Recovery Point Objectives, and Recovery Time Objectives as defined in Appendix III.

Furthermore, the HSMS shall support a robust disaster recovery capability, enabling full recovery of all PID secret keys in the event of system failure or data loss. This requirement is critical given the sensitive nature and operational importance of the RWSCD in the context of identity assurance and verifiable credential signing.

The PKI used to issue the necessary certificates, together with the necessary HSMS, will be hosted within the GoM secure hosting environment (Colocation within MITA data centres). This PKI will issue:

- Signing certificates for the signing of the PIDs by the PID Provider;
- Signing certificates for the signing of Wallet Provider's attestation by the Wallet Provider;
- Signing certificates for the signing of the registers by the Registrar;
- WRPACs;
- Any other certificates as per Implementing Acts that are in the public domain on the date of the publication of this tender.

The PKI in charge of issuing the signing certificates listed above will also be in charge of managing the signing key on a HSM, on behalf of their owner (i.e. the PID Provider, the Wallet Provider and the Registrar).

The existing PKI for the issuance of the eID Card authentication and signature certificates, as well as the issuance of document signer certificate to let the national eID System sign the identity data stored in the card, is out of the scope of the present project.

4.2.2.1

RWSCD Registration Requirements

The Solution shall support a secure RWSCD registration process, initiated by a Wallet Instance operating on a mobile device.

The mechanism described below is provided as an example. Bidders may propose an alternative RWSCD registration mechanism, provided it guarantees the level of security required by [CIR 2024/2979] and [CIR 2024/2981] where they refer to critical assets, WSCA and WSCD and [CIR 2015/1502] referred by the two other CIRs.

The Solution is to function in such a way to be seamlessly aligned and fully compliant with the [EUDI Regulation], Implementing Acts and applicable standards.

The registration mechanism must implement multi-factor authentication, comprising:

1. Possession factor: A hardware-bound cryptographic key pair generated on the mobile device.
2. Knowledge factor: A user-defined PIN.

The registration process shall begin following the successful authentication of the user by the PID Provider, and receipt of claims from the national eID service. This is described in more detail in Section 4.2.2.2. The PID Provider then requests the Wallet Instance to provide a public key for the PID.

The Wallet Instance starts by requesting a cryptographic challenge from the RWSCD. This challenge must be designed to prevent replay attacks and shall be cryptographically signed and self-contained, eliminating the need for the RWSCD to maintain session state or data.

The Wallet Instance shall generate the hardware-bound key-pair locally. The private key must remain securely stored on the mobile and must not be exposed or transmitted. The Wallet Instance shall use the Trusted Execution Environment of the mobile device for storing the hardware-bound private key, with the option of using the Secure Element where available.

The Wallet Instance shall ask the user for a PIN and generate a PIN-derived key pair based on a random salt. The salt shall be stored locally on the mobile, to ensure that the same key pair can be generated again for later RWSCD operations. The Wallet Instance shall use the TEE of the mobile device for storing the salt, with the option of using the SE where available.

The Wallet Instance shall send the signed challenge, the generated hardware-bound public key, and the PIN-derived public key to the RWSCD. The signature of the challenge shall prove possession of both the hardware-bound private key and the PIN-derived public key. The RWSCD shall create an account identifier and store the corresponding hardware-bound public key and PIN-derived public key.

For PIN management, the following requirements apply:

1. The PIN retry counter shall be managed by the RWSCD, due to the inability of most mobile platforms to guarantee a high Level of Assurance for local PIN handling. This counter shall be linked to the corresponding account identifier.
2. The RWSCD must not store or have access to neither the plaintext PIN nor the PIN-derived private key. Instead, it shall store the PIN-derived public key for authentication purposes.
3. The RWSCD must not store or have access to the hardware-bound private key. Instead, it shall only store the hardware-bound public key for authentication purposes.
4. Neither the PIN nor the PIN-derived private key shall be persistently stored on the Wallet Instance. Only the salt shall be stored, for later re-generation of the PIN-derived key pair.

The Wallet Instance and the RWSCD shall support the requirement for change and/or reset of the RWSCD PIN by the user.

All cryptographic operations and key management practices must comply with the requirements of the [EUDI Regulation] and relevant Implementing Acts, in particular [CIR 2024/2979] and [CIR 2024/2981].

4.2.2.2 Integration with the Maltese eID infrastructure

A critical aspect of the Maltese Wallet ecosystem is the use it makes of the eID Card. The eID Card possesses two keys and related certificates: one authentication key, and one signature key certified by a qualified certificate. This will act as a QSCD using the signature key it contains. The awarded bidder shall ensure that Wallet Instance shall be able to communicate with the JavaCard applet on the eID Card in a secure manner through a cryptographic secure interface.

The eID Card is engineered to enable secure communication using the PACE protocol over NFC on both Android and iOS devices. The JavaCard applet shall manage the full lifecycle of a card session, including establishing a connection, authenticating with the user's Card

Access Number (CAN), and setting up a secure messaging channel. This secure channel is crucial for protecting all subsequent operations, such as PIN verification and cryptographic commands, from interception or tampering.

Once the secure session is established, the card can be used to read digital certificates and perform digital signature operations. Reading a certificate involves selecting the appropriate file on the card, extracting the binary data, and parsing it into a standard X.509 certificate. Appendix II contains detailed integration documentation including sample code. The code is provided solely for illustrative purposes and reference. The awarded bidder is to create the interface between the Wallet Instance and the eID Card.

The PID Provider shall leverage Malta's national eID infrastructure to issue a PID credential to the user's Wallet Unit. This process relies on the authentication key embedded in the user's eID Card and is facilitated through the OpenID Connect protocol, which ensures secure and standardised integration between the PID Provider and the national eID system.

When the user initialises their Wallet, they are redirected to the PID Provider, which then connects to the national authentication service at eid.gov.mt using the OpenID Connect protocol, as described in Appendix I, requesting the user to be authenticated at a High Level of Assurance (LoA). The user shall tap their eID Card via NFC and use the authentication certificate stored on the card to log in to the eid.gov.mt service.

Following successful authentication, eid.gov.mt returns the necessary user attributes to the PID Provider in the form of claims. These attributes are then used to construct the PID. Once the PID is constructed and digitally signed, it is transmitted to the user's Wallet Unit using secure transport protocols as allowed by [OpenID4VCI].

It is important to note that users may be using their eID Card electronically for the first time when enrolling in the Wallet. Therefore, the Wallet Solution must support first-time eID Card usage, including the mandatory initial PIN change process.

To ensure a smooth and accessible user experience, the Wallet is also expected to provide clear, friendly, and context-aware messages throughout the enrolment journey. These messages should guide users step-by-step, helping them understand each action required and reassuring them in case of any issues. In particular, the Wallet must include supportive guidance in scenarios such as PIN locking, offering instructions on how to unlock or reset the PIN, and directing users to relevant help channels or self-service options where applicable.

Additionally, the Wallet should be designed to anticipate and address common user challenges during enrolment, such as NFC connectivity issues, incorrect PIN entries, or connectivity problems, by offering real-time feedback and troubleshooting tips. This approach will help reduce user frustration, increase successful enrolments, and foster trust in the digital identity ecosystem.

4.2.2.3 *PID Secret Key Generation and PID Issuance Requirements*

Following successful completion of the RWSCD registration process, the Solution shall support the secure generation of a PID secret key and public key on the RWSCD. This key pair is used to enable privacy-preserving identity operations and must be handled in accordance with the following requirements:

Trigger and Context

- The PID secret key shall be generated only after the Wallet Instance has completed the RWSCD registration (and has been authenticated using two-factor authentication).

- The generation process shall be initiated by the RWSCD without requiring additional input from the Wallet Instance.

Key Generation and Storage

- The PID secret key shall be generated using a cryptographically secure random number generator compliant with industry standards.
- The PID secret key shall be unique across all RWSCD accounts and must be bound to the account identifier established during registration.
- The PID secret key shall be stored securely within the RWSCD's protected key storage infrastructure, ensuring confidentiality and integrity.
- The PID secret key must not be accessible to external systems or transmitted outside the RWSCD environment.
- The Solution shall support revocation or rotation of the PID secret key in accordance with key lifecycle management policies.

Operational Usage and Access Control

- The PID secret key shall be used exclusively for identity-related operations as defined in the system's functional specification.
- Access to the PID secret key shall be strictly controlled and limited to authorised internal components of the RWSCD.
- All operations involving the PID secret key shall be logged for auditability, including timestamps, operation type, and outcome.

Compliance and Cryptographic Standards

- The PID secret key generation and management process shall comply with the requirements set forth in the [EUDI Regulation] and the applicable Implementing Acts, e.g. [CIR 2024/2979].
- The Solution shall ensure that no copies of the PID secret key are stored outside the RWSCD's secure environment. If, for the sake of business continuity / disaster recovery, copies of PID secret keys are stored, they shall be subject to the same or greater level of security controls as keys in use.

PID Issuance

- At the end of the PID secret key generation process, the RWSCD sends the account identifier and the corresponding PID public key to the Wallet Instance.
- The Wallet Instance transmits the PID public key to the PID Provider, who combines it with other claims and generates a signed PID. This signed PID is then returned to the Wallet Instance for storage. It is transmitted to the user's Wallet Unit using secure transport protocols as allowed by [OpenID4VCI].

PID Re-issuance

The Solution must also support requests for PID re-issuance, ensuring that a new signed PID can be generated and delivered to the Wallet Instance when needed using secure transport protocols as allowed by [OpenID4VCI].

4.2.2.4 RWSCD Operation Requirements

The proposed Solution shall support secure execution of RWSCD operations initiated by a Wallet Instance, leveraging the multi-factor authentication mechanism established during the registration phase.

Authentication and Request Handling

For example, in the scenario outlined above:

- The Wallet Instance shall initiate each operation by requesting a cryptographic challenge from the RWSCD. This challenge must be designed to prevent replay attacks and must be cryptographically signed and self-contained.
- The Wallet Instance shall construct an operation request and authenticate it, preferably using a JSON Web Signature (JWS) in JSON serialisation format.
- The Wallet Instance shall ask the user for the PIN and re-generate the PIN-derived private key based on the salt securely stored during the registration phase.
- The authenticated request must be signed by the possession factor (hardware-bound private key) and by the knowledge factor (PIN-derived private key), to demonstrate proof of possession for both keys.
- The authenticated request, along with the associated account identifier, shall be transmitted to the RWSCD.

Verification and Processing

For example, in the scenario outlined above:

- The RWSCD shall verify the request received using the data associated with the account identifier provided.
- The verification sequence shall proceed as follows:
 1. Validate the challenge contained in the request sent by the Wallet Instance, to detect and prevent replay attacks.
 2. Verify the possession factor (hardware-bound public key).
 3. Verify the knowledge factor (PIN-derived public key).
- The PIN retry counter shall be securely managed by the RWSCD. The RWSCD must not store or have access to neither the plaintext PIN nor the PIN-derived private key, and only store the PIN-derived public key.
- The RWSCD must not store or have access to the hardware-bound private key. Instead, it shall only store the hardware-bound public key.

Operation Execution

- Upon successful verification of the operation request, the RWSCD shall proceed to process the corresponding operation.

API and Supported Operations

- An overview of supported operations shall be provided as part of the documentation of the Solution.
- The detailed API specification will be published at a later stage and must be supported by the Solution.

Use of PID Secret Key for Verifiable Presentations

- The Solution shall support the use of the PID secret key, generated and securely stored on the RWSCD, to sign Verifiable Presentations in accordance with the standards defined in Section 3 Clause 4.2.3.5.

Functional Requirements

- The RWSCD shall support the use of the PID for authentication and selective disclosure as defined in Section 3 Clause 4.2.3.6.2.
- The RWSCD shall use the PID secret key to cryptographically sign Verifiable Presentations that are requested by the Wallet Instance.
- Regarding the signed Verifiable Presentation, the Solution shall support the proof mechanisms corresponding to the standards defined in Section 3 Clause 4.2.3.5.

- The PID secret key shall be used exclusively for signing identity-related data and must not be repurposed for other cryptographic operations.

Security and Privacy Requirements

- The PID secret key shall remain within the secure boundary of the RWSCD and must not be exported, transmitted, or exposed to external systems.
- All signing operations shall be performed within a secure execution environment, ensuring protection against unauthorised access and tampering.
- The RWSCD shall ensure that each Verifiable Presentation is signed in a manner that preserves user privacy, including support for selective disclosure where applicable.
- The RWSCD shall validate the authenticity and authorisation of the request before performing any signing operation.
- The system shall log all signing activities, including the timestamp, requesting entity, and operation outcome, for audit and compliance purposes.

Standards Compliance

- The implementation shall comply with the relevant requirements of the [EUDI Regulation] and relevant Implementing Acts. In particular, the HSM must support [EUDI Regulation] requirements and the management of the RWSCD shall follow ETSI TS 119 431-1 requirements for server signing, applied "mutatis mutandis" to the management of a RWSCD.
- The cryptographic algorithms used for signing shall meet current industry best practices and regulatory requirements.

4.2.3 *Technical specifications of the Solution compliant with the [EUDI Regulation]*

The Solution provided by the awarded bidder shall be compliant with the standards referred to in this document. Current work undertaken by ETSI shall be considered, even if the standards are not finalised by the time this Call for Tenders is issued.

4.2.3.1 *General functions of the Wallet Unit*

The Wallet Solution shall be implemented such that there is an authentication mechanism that allows the user to authenticate to the Wallet Unit. According to Article 3(1) of [CIR 2024/2979], none of the actions described in Article 5a(4) of [EUDI Regulation] can be performed if the user has not been successfully authenticated by the Wallet Unit. Given that the Wallet constitutes a high-level electronic identification means in accordance with [EUDI Regulation], the associated authentication procedures shall adhere to the requirements set out in Commission Implementing Regulation (EU) 2015/1502 referred in [CIR 2024/2979], as well as the relevant interpretative guidance.

4.2.3.2 *Wallet Attestations*

The WUA is provided and signed by the Wallet Provider, as per Article 3 of [CIR 2024/2979], who uses the TEE of the phone as a second WSCD, used for the WUA secret key, in fulfilment of Article 6.2 of [CIR 2024/2979].

The WUAs provided shall be signed in a way that respects the conditions set out in Article 3(2) of [CIR 2024/2979]. By Article 6 of [CIR 2024/2979], each Wallet Unit shall contain WUAs, which contain public keys, and the corresponding private keys shall be protected by a WSCD under the control of that Wallet Instance. By Article 7(1) of [CIR 2024/2979], WUAs shall be revocable by the Wallet Provider.

The format, content, lifecycle and revocation of a WUA used during the issuance of a PID/EAA should follow the specifications outlined in [ARF TS03].

The awarded bidder shall implement all necessary technical and organisational measures to ensure, at all times, the authenticity and integrity of the Wallet Solution, including via the use of WIAs.

4.2.3.3 *PID/EAA*

The Wallet User shall be able to request the issuance of PIDs/EAs. For this purpose, as per the Topic 10 of the [ARF], the Wallet Solution shall support the OpenID4VCI protocol specified in [OpenID4VCI], as profiled by the 'OpenID for Verifiable Credential Issuance' profile specified in [HAIP]. It shall also support the [W3C Digital Credentials API] if fully standardised.

By Articles 3 and 4 of [CIR 2024/2977] and Article 8 of [CIR 2024/2979], the Wallet Solution shall support the usage of PIDs and EAs issued in compliance with the list of standards set out in the Annex II of [CIR 2024/2979], i.e.:

- [ISO/IEC 18013-5]
- [W3C VCDM v1.1]

Moreover, it should support the format described in [SD-JWT VC], as well as EAs issued in compliance with [ETSI TS 119 472-1] when final.

By Article 10(1) of [CIR 2024/2979], the Wallet Solution shall be able to process EAs with the common embedded disclosure policies set out in Annex III of [CIR 2024/2979]. The mechanism allowing embedded disclosure policies shall be compliant with [ETSI TS 119 472-3] when final.

4.2.3.4 *Wallet Unit components*

4.2.3.4.1 *WSCD*

The WSCD where the PID secret key will be stored is the RWSCD. Other secret keys, such as WUAs secret keys and EAs secret keys, will be stored either on the TEE or SE of the phone.

The awarded bidder shall provide an option, to be availed of at the discretion of the Contracting Authority, whereby when installing the Wallet Solution onto the user's phone, the software should be able to identify if a SE is present on the phone. If a SE is present, it may be used in place of the TEE, and if used, it shall be compliant with the standards listed in Annex I of [CIR 2024/2979].

4.2.3.4.2 *WSCA*

Each WSCD shall have its WSCA. The awarded bidder shall provide a WSCA corresponding to each WSCD, and the Wallet Instance shall be able to communicate with it in a secure manner through a cryptographic secure interface as well.

4.2.3.4.3 *RP verifier component*

The RP verifier component shall be provided by the awarded bidder. It shall be able to verify the authenticity of a RP before presenting them with attributes. It shall be a part of the Wallet Unit.

4.2.3.5 *Presentation of attributes*

According to Article 5 of [CIR 2024/2982], the Wallet Solution shall support protocols and interfaces for remote and in-person presentation of attributes to RPs. The interfaces shall be compliant with [ETSI TS 119 472-2] when final. The Wallet Unit shall respond to successfully authenticated and validated requests from RPs. Both these requirements shall conform to standards [ISO/IEC 18013-5] and [ISO/IEC 18013-7]:

- For **proximity presentation flows**: protocols and interfaces shall be compliant with [ISO/IEC 18013-5]. [SD-JWT VC] compliant attestations shall be presented using [OpenID4VP].
- For **remote presentation flows**: as per the [ARF], messages used to request and send attestations comply with [OpenID4VP]. For [ISO/IEC 18013-5] compliant attestations, it shall use the profile contained in Annex B of [ISO/IEC 18013-7]. For [SD-JWT VC] compliant attestations, it shall use the profile for 'OpenID for Verifiable Presentations for IETF SD-JWT VC' specified in [HAIP]. [SD-JWT VC]-compliant attestations as well as [ISO/IEC 18013-5]-compliant attestations shall be presented using [OpenID4VP].

4.2.3.6 *Authentication (Presentation of PID)*

4.2.3.6.1 *Authentication mechanism*

The authentication mechanism shall be based on the presentation of a PID to a Relying Party and shall follow the standards as stated in the previous Section 3 Clause 4.2.3.5 about proximity presentation flows and remote presentation flows.

The authentication process typically begins when the user clicks "Login" on the Relying Party's website. The frontend requests a login session from the backend, which generates a one-time authorisation request and returns it as a QR code. The user scans this QR code with their EUDIW, which retrieves the full request, including the required credentials and a unique nonce to prevent replay attacks.

The Solution shall also verify in cross-device flows, using mediating APIs, that an interacting device is in close physical proximity to the EUDI Wallet using a secure, direct, and user-mediated local communication channel, such as a short-range wireless communication technology to perform the physical proximity check.

4.2.3.6.2 *Preparation of PID attributes for selective disclosure*

At the design stage, the Contracting Authority shall specify to the awarded bidder which attributes of the Person Identification Data (PID) are to be prepared for selective disclosure. During the PID issuance, the PID Provider shall create a JWT in accordance with the standards specified in Section 3 Clause 4.2.3.5, that contains only hashed claims rather than the actual values, store the real claim values in a separate disclosure array, and sign the JWT with the PID Provider secret key. The Wallet Unit shall keep both the signed JWT and the disclosure array, allowing the holder to selectively choose which claims to reveal later. Furthermore, the awarded bidder shall as a minimum ensure that one of the methods required by the [ARF] to ensure unlinkability is followed (e.g. batch issuance of PIDs) and may propose additional methods.

4.2.3.7 *Signing*

4.2.3.7.1 *QES*

By Article 11 of [CIR 2024/2979], the user shall have free access to a SCA to create QES for non-professional purposes at least. The user shall at least be able to create signatures in PAdES, as specified by [ETSI EN 319 142-1] v1.2.1.

The bidder may also provide users with the ability to create signatures in XAdES (specified by [ETSI EN 319 132-1] V1.3.1), in JAdES (specified by [ETSI TS 119 182-1] V1.2.1), in CAdES (specified by [ETSI EN 319 122-1] V1.3.1), and in ASiC (specified by [ETSI EN 319 162-1] V1.1.1).

4.2.3.7.2 SCA

By Article 12 of [CIR 2024/2079], the SCA can be provided by the entity issuing the Wallet, by a TSP or by a RP. It can be internal or external to the Wallet Instance. Here, the awarded bidder shall provide it as part of the Solution in line with the HLD, and it shall be hosted in the GoM's secure hosting environment. The service shall be compliant with [ETSI TS 119 431-2] V1.2.1, where the requirements regarding the EU advanced X.509 SCASC Policy shall apply (Section 4.2.2 of [ETSI TS 119 431-2] V1.2.1). Moreover, the signature creation shall comply with [ETSI EN 319 102-1]. The complete end-to-end signing process, including document upload, signature application, verification, and confirmation, shall not exceed 60 seconds under normal network conditions for a standard document of up to 10 MB. This duration excludes the time required for the user to tap the card to the mobile device.

4.2.3.7.3 QSCD

Regarding signing and the creation of qualified electronic signatures, the eID Card is the QSCD and protects the signing private key (which is the eID Card signing key). The user interacts with the signer interface component, which then contacts the SCA with the document to be signed. The SCA shall be provided by the awarded bidder, and it is recommended that it is external to the Wallet Provider component.

By Article 11 of [CIR 2024/2979], users shall be able to receive QCs for QES which are linked to a QSCD, which can be local, external or remote. In the Malta context, the eID Card will be used as an external QSCD, and the citizen's QC for QES. The Wallet Solution shall be able to connect to the eID Card through the NFC protocol to reach the QSCD.

4.2.3.8 *Wallet-to-Wallet interactions*

Specifications for Wallet-to-Wallet interactions should follow [ARF TS09].

4.2.3.9 *Backup and Recovery for the EUDIW*

The awarded bidder shall design and implement secure backup and recovery for the EUDIW which is compliant to the requirements of the [EUDI Regulation] and takes into consideration the relevant ARF topics. This strategy must ensure user autonomy and maintain the highest standards of security and privacy. It shall include mechanisms for generating and safeguarding recovery credentials, educating users on their responsibilities and creating the migration object as described by the ARF. The recovery process must enable users to restore their wallet and associated data in the event of device loss or failure without compromising confidentiality or integrity.

4.2.3.10 *Wallet ecosystem components*

4.2.3.10.1 *WUA verifier component*

The WUA verifier component shall be provided by the awarded bidder. It shall be able to verify the authenticity of a WUA and will be used by the PID Provider.

4.2.3.10.2 *Attestation issuer component*

The attestation issuer component shall be provided by the awarded bidder. It shall be able to format data in the appropriate format(s) of PID as per [CIR 2024/2977]. This component will be used by the PID Provider.

4.2.3.10.3 *Wallet Provider*

The Wallet Provider in the EUDIW ecosystem is a foundational component responsible for implementing and maintaining the wallet application in line with the legislative texts, [EUDI Regulation], [CIR 2024/2979] in particular and the [ARF]. The Wallet Provider must build the Wallet Instance that can securely interface with issuers (who provide PID and EAAs) and relying parties (who request identity data for service access), as per [CIR 2024/2982] in particular, using a shared trust infrastructure.

The Wallet Provider shall be capable of signing (see Clause 4.2.3.10.5, PKI, below) and revoking its attestations.

It shall be noted that Wallet Providers are not CA; they issue WUAs that are signed statements and are not X.509 certificates. However, similarly to CA, the signed statements contain a user's public key and obligations remain on these signed statements over their lifecycle (contrarily to classical signatures), namely the obligation to be able to revoke the WUA attestations where relevant. The signing key of the Wallet Provider is thus subject to particular care and will be managed by the PKI that will issue the related signing certificate (see Clause 4.2.3.10.5, PKI, below). The Waller Provider shall also notify, including via an out-of-band manner, if necessary, the User about the revocation.

4.2.3.10.4 *PID Provider*

The PID Provider is the component responsible for issuing verified identity data to the Wallet Instance. The PID Provider ensures that the identity data is issued according to the common standards and protocols defined in legislative texts, [EUDI Regulation] and [CIR 2024/2977] in particular, and the ARF. This data, such as name, date of birth, and nationality, is cryptographically bound to the Wallet. The Wallet Provider shall be capable of signing (see Clause 4.2.3.10.5, PKI, below), re-issuing and revoking PIDs as specified above. The circumstances for PID re-issuance and revocation shall be determined in full at design stage and may require that the awarded bidder interfaces with national identity infrastructures to receive notifications of eID Card revocation to trigger PID revocation.

It shall be noted that PID Providers are not CA; they issue PIDs that are signed statements. However, similarly to CA, the signed statements contain a user's public key and obligations remain on these signed statements over their lifecycle (contrarily to classical signatures), namely the obligation to be able to revoke the PID where relevant. The signing key of the PID Provider is thus subject to particular care and will be managed by the PKI that will issue the related signing certificate (see Clause 4.2.3.10.5 PKI, below).

The PID Provider shall support as applicable any methods for unlinkability as proposed by the bidder in response to the requirements in Clause 4.2.3.6.2.

4.2.3.10.5 *Public Key Infrastructure (PKI)*

The Public Key Infrastructure (PKI) used to issue the required certificates, along with the associated Hardware Security Modules (HSMs), will be hosted within the Government of Malta's secure hosting environment. The Awarded Bidder shall provide the PKI software and

hardware including the HSMs, and deploy everything within the hosting environment in the MITA data centres. All HSMs used must be able to support eIDAS requirements. This PKI shall issue:

- Signing certificates for the signing of the PIDs by the PID Provider;
- Signing certificates for the signing of Wallet Provider's attestation by the Wallet Provider;
- Signing certificates for the signing of the registers by the Registrar;
- WRPACs;
- Any other certificates as per Implementing Acts that are in the public domain on the date of the publication of this tender.

The PKI and related services are depicted in Figure 2 below:

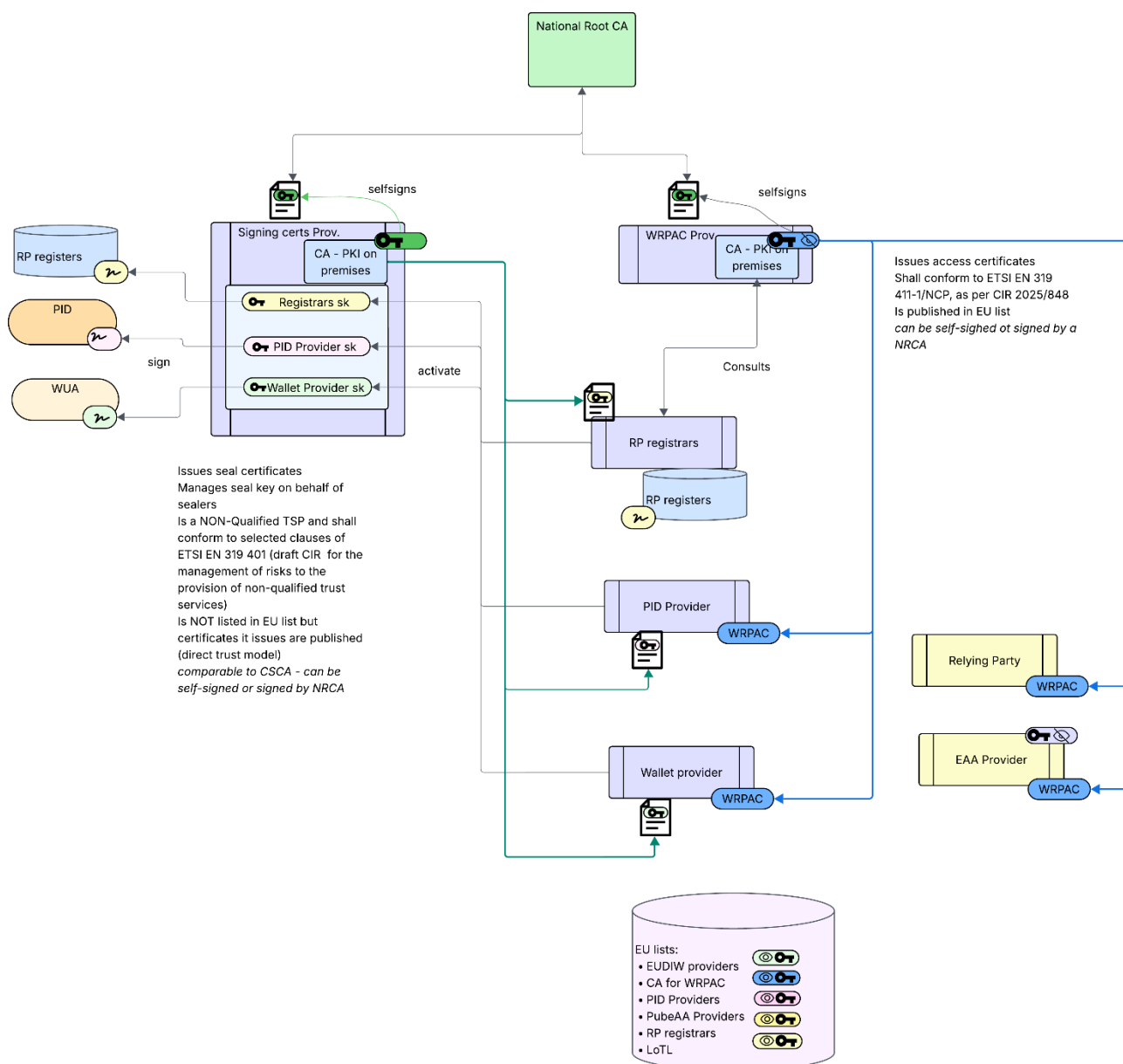


Figure 2: PKI and related services

The CA(s) issuing the signing certificates listed above is (are) a TSP (since issuing signature/seal certificates is a trust service). The signing certificate used by this (these) CAs

to issue certificates are NOT listed in a EU list and do not need to be published in a national trusted list since the signing certificates they issue to PID Provider, Wallet Provider and Registrar are published in a EU list, benefiting thus from direct trust.

The CA issuing WRPAC shall comply with the Normalised Certificate Policy (NCP) as defined in ETSI EN 319 411-1, version 1.4.1 as required by [CIR 2025/848].

NOTE: ETSI published a profile of EN 319 411-1, [TS 119 411-8] that provides requirements for the CA issuing WRPAC and that should be considered by the awarded bidder.

It is also recommended to follow [ETSI TS 119 475] for the issuance of the WRPAC, in particular for profiling these certificates on the basis on the information from the register, provided that this TS aligns with [ARF TS02] and [ARF TS05] which shall take precedence.

The signing certificate of this CA shall be listed in an EU list.

The awarded bidder shall ensure the conformance of the above PKI solution to the requirements of the [EUDI Regulation] on TSPs, particularly with reference to [CIR 2025/2160] for the management of risks to the provision of non-qualified trust services, including the annex that references selected clauses of ETSI EN 319 401.

The awarded bidder shall support that for both CA type, issuing signing or WRPAC certificates, can be self-signed or signed by a National Root CA since the trust model of the [EUDI Regulation] supports direct trust in either issuing CA or end-entities certificates.

Even if the legal framework imposes to follow ETSI EN 319 411-1/NCP for WRPAC CA only, the CA issuing the signing certificates listed above shall also follow this norm that is a benchmark in the PKI field.

NOTE: This norm is required for CA issuing qualified signing certificate as per [CIR 2025/1943] that refers to EN 319 411-2 endorsing EN 319 411-1.

It is preferred that the bidder offers two distinct CAs for the two purposes even if there are commonalities in the technical requirements and standards to be followed, because they are ruled by two different CIRs on one hand and because the subscribers for each CAs are pretty different in nature, entailing different procedures (e.g. registration) and interfaces (e.g. connection to the Registers of WRP for the WRPAC CA).

In the HLD depicted in Figure 1, and for the reasons evoked in Clause 4.2.3.10.3 Wallet Provider and Clause 4.2.3.10.4 PID Provider, it is requested that the PKI in charge of issuing the signing certificates listed above will also be in charge of managing the signing key on a HSM, on behalf of their owner (i.e. the PID Provider, the Wallet Provider and the Registrar). The management of these keys is subject to requirements:

- Requirements pertaining to eID LoA High apply to the Wallet, as per Article 5a of the [EUDI Regulation]; PID Providers shall perform identity verification of the wallet user in accordance with the requirements of [CIR 2015/1502] and the Wallet and its authentication function shall conform to [CIR 2015/1502] which entails requirements on the protection of the assets of both the WUA provider and the PID Provider.
- As per [EUDI Regulation], requirements from Article 24.2 apply to providers of EUDIW. Consequently, they shall also apply to the WUA and PID issuance. Here again, the requirements in [EUDI Regulation] on TSPs shall be ensured, particularly with reference

to [CIR 2025/2160] for the management of risks to the provision of non-qualified trust services including the annex that references selected clauses of ETSI EN 319 401.

- As per [EUDI Regulation], requirements from Article 24.2 apply to providers of EUDIW. Consequently, they shall also apply to the WUA and PID issuance. Here again, the requirements in [EUDI Regulation] on TSPs shall be ensured, particularly with reference to [CIR 2025/2160] for the management of risks to the provision of non-qualified trust services including the annex that references selected clauses of ETSI EN 319 401. For what regards the Registrars, [CIR 2025/848] requires they must use appropriate means and in accordance with the laws and procedures of the Member State where the national register is established. In Malta, a Registrar shall be appointed to set up the RP registers. National data registers are central to the digital transformation of public administration, enabling efficient, secure, and interoperable data management across government entities. These registers are governed by the Data Governance Council, which oversees the *Register of Registers* which is a comprehensive inventory of legally mandated data repositories used across the public sector. The Public Administration Data Strategy 2023-2027 positions data as a national asset and outlines a framework for its ethical use, sharing, and reuse. It promotes the creation and adoption of a unified national data infrastructure. This infrastructure supports interoperability, role-based access, and enterprise-wide records management.

The awarded bidder shall supply all the supporting documentation for the PKI including as follows:

- Certificate Policy (CP): Describes the rules, scope, trust levels, and intended uses for certificates within the PKI.
- Certification Practice Statement (CPS): Details the specific practices, procedures, and operational processes the Certification Authority (CA) follows to implement the Certificate Policy, including security controls and certificate lifecycle management.
- Certificate Revocation List (CRL) Policy: Specifies procedures for revoking certificates, how revocation information is published, and the frequency and methods for updating and distributing CRLs, where applicable.
- Subscriber Agreement: Outlines the responsibilities, obligations, and liabilities of certificate subscribers (end users or entities) in their relationship with the CA.
- Relying Party Agreement: Defines the duties, validation procedures, and limitations of liability for entities that rely on the validity of certificates.
- Key Management Procedures: Establishes how cryptographic keys are generated, stored, distributed, used, backed up, recovered, and destroyed.
- Audit and Compliance Policy: Sets requirements for regular audits and compliance checks, including audit frequency, scope, and reporting.
- Incident Response Policy: Provides procedures for detecting, reporting, investigating, and remediating security incidents affecting the PKI.
- Privacy Policy: Explains how personal data collected during certificate issuance and management is handled, including data collection, retention, and protection measures.

The existing PKI for the issuance of the eID Card authentication and signature certificates, as well as the issuance of document signer certificate to let the national eID System sign the identity data stored in the card, is out of the scope of this project.

4.2.3.10.6 Registers maintenance component - Relying Party Registrar

The awarded bidder shall provide the software components necessary to establish and maintain a national register with information regarding Relying Parties established in Malta, the Relying Party Registrar, in accordance with [CIR 2025/848] and [CIR 2024/2980].

4.2.3.11 *Version 2 - Other requirements for the Solution developed in line with the [EUDI Regulation]*

4.2.3.11.1 *Certification of the EUDIW*

The awarded bidder shall actively support the Contracting Authority in its efforts to achieve certification of the European Digital Wallet in accordance with applicable EU regulations, standards, and guidelines. The awarded bidder shall assist in the preparation and execution of conformance, interoperability, and security testing as required by the certification process, including collaboration with designated testing bodies or authorities. The awarded bidder shall also cooperate with external auditors, assessors, or certification bodies by providing access to systems, logs, and personnel as needed to facilitate the certification process. The Contracting Authority requires the awarded bidder to allocate up to two hundred (200) person days in support of the implementation of this initiative.

4.2.3.11.2 *Interoperability*

The awarded bidder shall ensure full interoperability of the EUDIW across mobile phone models equipped with NFC technology and operating systems, including but not limited to Android and iOS.

4.2.3.11.3 *Pseudonyms*

By Article 14 of [CIR 2024/2979], support of generation of pseudonyms shall be done in accordance with [W3C WebAuthn].

4.2.3.11.4 *EUDIW Trust Mark*

The display of the EUDIW Trust Mark should follow the specifications presented in [ARF TS01].

4.2.3.11.5 *Data deletion request*

The protocols and interfaces for requesting the erasure of personal data to RPs should follow the specifications presented in [ARF TS07].

4.2.3.11.6 *Reporting of RPs*

The protocols and interfaces for reporting RPs to DPAs should follow the specifications presented in [ARF TS08].

4.2.3.11.7 *Data portability, download and transaction logs*

The formats, contents and security measures for the implementation of data portability, download and transaction logs, should follow the specifications presented in [ARF TS10]. The migration shall be done in a way that ensures LoA high as set out in [CIR 2015/1502], as per Article 13 of [CIR 2024/2979].

4.2.3.11.8 *Build, Operate, Maintain and Support*

The awarded bidder shall be responsible for the complete delivery of the Solution, encompassing its design, development, deployment, operation, and ongoing support. This commitment shall cover a period of seven (7) years from the date of commissioning of the Version 1. Additionally, the Contracting Authority with agreement of the Contractor reserves

the right to extend the agreement by two (2) extensions of twenty-four (24) months each under the same terms and conditions.

Operate, Maintain and Support also includes the necessary actions and systems to continuously monitor the maintenance of applicable certifications, including the certification of the Solution.

Operate, Maintain and Support also includes the necessary security requirements, in particular wallet related services shall follow the applicable clauses of ETSI EN 319 401 as per ENISA EUDIW Cybersecurity Certification Draft candidate scheme.

The Contracting Authority at its own discretion may request handing over of the Operation and/or Maintenance and/or Support of the Solution or part thereof.

4.2.3.11.9 *Documentation Requirements*

At the design stage, the awarded bidder is required to deliver comprehensive documentation that captures all aspects of the system's intended functionality and structure. This includes a detailed requirements specification covering both functional and non-functional requirements, as well as use cases or user stories that illustrate how the system will be used. The awarded bidder must also provide architectural and detailed design documents, such as high-level architecture diagrams, data flow diagrams, and entity-relationship diagrams, to clearly describe the system's structure and data relationships. Interface design specifications, including API definitions and user interface wireframes, must be included. Furthermore, the awarded bidder is obligated to document security considerations through a security architecture and risk assessment, and to map compliance requirements to ensure regulatory alignment. Project management documentation, such as project plans, resource allocation plans, and risk management plans, must be supplied to guide the project's execution. An initial test strategy and test plan should also be provided to outline the approach for system validation.

During the implementation stage, the awarded bidder is responsible for delivering all technical and operational documentation necessary for the successful deployment and maintenance of the system. This includes source code documentation, build and deployment guides, and configuration management documents to ensure the system can be reliably built and maintained. The awarded bidder must also provide detailed testing documentation, including test cases, test scripts, and records of test results and defects, as well as user acceptance testing plans. Operational documentation, such as system administration manuals, maintenance procedures, and backup and recovery plans, must be provided to support ongoing system management. The awarded bidder is also required to deliver user documentation, including user manuals, quick reference guides, and training materials, to assist end-users and support staff. Finally, the awarded bidder must maintain change management documentation, such as change requests, approvals, and release notes, to ensure that any modifications to the system are properly tracked and communicated.

At the operations, maintenance, and support stage, the awarded bidder is obligated to provide all documentation necessary for the ongoing operation, support, and continuous improvement of the system. This includes up-to-date system operation manuals, maintenance schedules, and procedures for routine and preventive maintenance. The awarded bidder must also provide incident and problem management documentation, including logs, troubleshooting guides, and escalation procedures. Regular updates to the system's configuration and inventory documentation are required, as well as records of patches, upgrades, and system changes. The awarded bidder should also deliver service level

reports, performance monitoring documentation, and capacity planning reports to ensure the system continues to meet agreed service levels. Additionally, updated user support materials, such as FAQs, knowledge base articles, and training refreshers, must be supplied to assist users and support teams throughout the system's operational life.

4.2.3.11.10 *Hosting, Security and Service Levels*

The Solution shall be hosted in its entirety (including the PKI) in the GoM's secure hosting environment, using Colocation within MITA data centres in accordance with the hosting and security schedules specified in Appendix III. The hosting architecture shall be deployed across a geographically separated dual data centre configuration, ensuring redundancy, high availability, and failover capabilities for all critical components, including the HSMs and associated cryptographic services. For clarity, all hardware necessary to host the Solution shall be provided, installed, configured and maintained by the bidder. The Contracting Authority requires network-attached HSMs deployed as rack-mounted appliances. Solutions based on embedded or host-dependent HSM technologies (e.g., PCI/PCle cards installed within servers) will not meet the architectural and security requirements of this procurement. The Solution shall provide the service levels, recovery point and time objectives as specified in Appendix III. The Solution shall support volumetrics as specified in Appendix III.

4.3 ***Project Management***

4.3.1 *Responsible Body*

The Beneficiary is the Malta Digital Innovation Authority.

4.3.2 *Management Structure*

The Malta Digital Innovation Authority shall nominate a focal point (Project Leader) for the undertaking of this Contract. The Service Provider shall also nominate a contact-point for the undertaking of this Contract being Key Expert 1 - Project Manager.

Notwithstanding the Solution will be hosted within MITA data centres, the Contracting Authority shall remain responsible for contract management and shall serve as the primary point of contact for the Awarded Bidder, except for those components which GoM assigns to other public bodies.

4.3.3 *Facilities to be provided by the Contracting Authority and/or other parties*

Not Applicable.

4.3.4 *Mandatory EU Cybersecurity Compliance*

The Awarded Bidder and Wallet Solution shall be compliant with applicable cybersecurity requirements laid down in Union and national law, including but not limited to those relating to the identification of high-risk suppliers, and ensure that their suppliers of software, security solutions and products with digital elements as defined by the Cyber Resilience Act comply with these requirements and conform to the relevant security standards and requirements throughout the duration of the contract.

The Awarded Bidder shall adopt technical, operational and organisational measures, to document and maintain risk assessments, manage risks including cybersecurity, prevent and respond to incidents, and cooperate with competent authorities, as required by the applicable EU and national legislation. Such legislation may include but not limited to, the CRA, NIS2, the GDPR, the Data Act, applicable national or European Cybersecurity

Certification Schemes adopted pursuant to the CSA and revised Regulations, such as the EUCC scheme, ensuring its compliances as a third party supplier and contributing effectively to the compliance of the Contracting Authority. The Awarded Bidder shall notify the Contracting Authority of any actively exploited vulnerability without undue delay.

The Awarded Bidder shall, for the duration of the Contract, authorise and fully cooperate with cybersecurity audits, assessments, inspections, or testing (including but not limited to technical, organisational, and process-based audits) as required by applicable EU and national legislation, or as reasonably required by the Contracting Authority for the purposes of verifying compliance with contractual, legal, regulatory, and security obligations. Such audits may be carried out by the Contracting Authority or by third parties authorised by it or by competent / market surveillance / certification authorities. The Awarded Bidder shall provide timely access to relevant systems, facilities, documentation, personnel, and information.

5. Logistics and Timing

5.1 - Location

The entire project shall be executed in the Maltese Islands (Malta and Gozo) and shall serve the business carried out by the Malta Digital Innovation Authority during business hours under Central European Time (CET). The solution infrastructure (including servers) shall be hosted on-premises at the MITA data centres. Operational activities that require physical access to the infrastructure shall be carried out at the MITA data centres as necessary. No specific location is being identified as the main operational base that the Service Provider should use. The Service Provider will provide development and/or management from its own premises with the possibility of being required to provide support at other sites as identified by the Contracting Authority when necessary.

Some of the Awarded Bidder's Key Experts, as well as personnel responsible for operational activities, will be required to be physically present in Malta during implementation of the contract as required for operation and maintenance purposes, to attend meetings and address a crisis or major issues.

5.2 - Commencement Date & Period of Execution

The intended commencement date and the period of execution of the contract will be the date specified in the Notice of Commencement, which notice shall be communicated to the Awarded Bidder in writing by not later than twelve (12) calendar weeks from the date of the last signature on contract agreement.

The Contracting Authority shall organise a Briefing meeting with the Awarded Bidder for commencement.

Article 18.1 of the Special Conditions will determine the actual commencement date and period of execution.

6. Requirements

6.1 - Personnel and Key Experts

6.1.1 Key Experts

The Awarded Bidder shall provide details of the following list of Key Experts proposed for the execution of the contract together with CVs, certificates and respective documentation attesting to the below requirements. CVs, experience claimed and copy of relevant qualifications of the proposed resources, to be submitted online through the prescribed Response Format and by using the Tender Preparation Tool provided at tendering stage.

The selection procedures used by the Awarded Bidder to select these experts shall be transparent, and shall be based on pre-defined criteria, including professional qualifications, language skills and work experience. The findings of the selected experts shall be recorded. The selection of experts shall be subject to approval by the Contracting Authority.

Key Expert 1: One (1) Project Manager

Responsible for the day-to-day management of the project including project initiation, planning, execution, monitoring, controlling, risk identification and resolution and closure throughout the duration of the Contract. The project manager will be the main point of reference between the Contracting Authority and the Awarded Bidder. Must have the minimum requirements below:

- a) as a minimum, be in possession of an academic qualification equivalent to MQF level 6 (or equivalent) in a field related to Management, Information Communication Technology, Engineering or a comparable subject field;
- b) possess good communication skills with good command of the English and/or Maltese language both written and spoken;
- c) have project management and leadership skills;
- d) have a minimum of 5 to 7 years' experience in ICT or related area; and
- e) have successfully delivered at least one large project worth over €2 million - project to be clearly mentioned in CV, indicating the role performed on this project.

Key Expert 2: One (1) Solution Architect

Lead the architecture stream of the project, to ensure that the system design adheres to industry's best practices and in line with requirements set out in this tender. Must have experience in designing mobile and backend applications. Must have the minimum requirements below:

- a) as a minimum, be in possession of an academic qualification equivalent to MQF level 6 (or equivalent) in a field related to Information Communication Technology or a comparable subject field;
- b) possess good communication skills with good command of the English and/or Maltese language both written and spoken;
- c) possess very good technical knowledge on designing mobile and backend solutions;
- d) have a minimum of 5 to 7 years' experience in ICT or related area, out of which have at least 3 to 5 years' experience designing mobile and backend solutions.

Key Expert 3: One (1) Lead Developer

A senior technical expert responsible for overseeing the end-to-end development of both mobile applications and backend systems, including API architecture and integration. The Lead Developer provides technical leadership, manages project timelines, and acts as the primary point of contact for all development-related matters within the project. This role

ensures technical excellence, coordinates cross-functional development teams, and guarantees that all solutions meet the highest standards of security, scalability, and performance. Must have the minimum requirements below:

- a) as a minimum, be in possession of an academic qualification equivalent to MQF level 6 (or equivalent) in a field related to Software Development, Information Communication Technology, Engineering or a comparable subject field;
- b) possess good communication skills with good command of the English and/or Maltese language both written and spoken;
- c) have software development and leadership skills;
- d) have a minimum of 5 to 7 years' experience in software development or related area; and
- e) have been involved in development of at least one related project worth over €1 million - project to be clearly mentioned in CV, indicating the development roles performed on this project.

Key Expert 4: One (1) Cybersecurity Specialist

The Cybersecurity Expert is responsible for ensuring the security and integrity of all digital assets within the project, including mobile applications, backend systems, and APIs. This role involves conducting risk assessments, defining security requirements, and implementing best practices to protect against cyber threats. The expert leads incident response efforts and provides guidance to development teams on secure coding and architecture. The Cybersecurity Expert acts as the primary authority on all matters related to information security throughout the project lifecycle. Must have the minimum requirements below:

- a) as a minimum, be in possession of an academic qualification equivalent to MQF level 6 (or equivalent) in a field related to Cybersecurity, Information Communication Technology, Engineering or a comparable subject field;
- b) possess good communication skills with good command of the English and/or Maltese language both written and spoken;
- c) have a minimum of 3 to 5 years' experience in cybersecurity or related area; and
- d) have been involved in cybersecurity of at least one related project worth over €1 million - project to be clearly mentioned in CV, indicating the roles performed on this project.

Key Expert 5: One (1) Trust Services Specialist

The Trust Services Specialist is responsible for the setup, operation, and ongoing management of trust services as required by the [EUDI Regulation]. This expert possesses deep knowledge of Public Key Infrastructure (PKI), digital signatures, electronic seals, and related trust services. The role includes designing secure trust service architectures and overseeing the issuance and management of digital certificates. The Trust Services Specialist acts as the primary authority on trust service operations, supporting the project's digital identity and trust objectives. Must have the minimum requirements below:

- a) as a minimum, be in possession of an academic qualification equivalent to MQF level 6 (or equivalent) in a field related to Information Communication Technology, Engineering or a comparable subject field;
- b) possess good communication skills with good command of the English and/or Maltese language both written and spoken;
- c) have a minimum of 3 to 5 years' experience in trust services or related area; and
- d) have been involved in trust services for at least one related project worth over €1 million - project to be clearly mentioned in CV, indicating the roles performed on this project.

Key Expert 6: One (1) Legal Specialist

The Legal Specialist is responsible for ensuring that all project components comply with the [EUDI Regulation], GDPR, Cybersecurity Act and other relevant legal frameworks. This expert oversees the certification process for trust services, digital identity solutions, and related systems, ensuring alignment with regulatory requirements. With a strong legal background and in-depth understanding of eIDAS, the specialist provides guidance on legal risks, prepares and reviews compliance documentation, and liaises with supervisory authorities and certification bodies. The Legal Specialist acts as the primary authority on legal and regulatory matters throughout the project lifecycle. Must have the minimum requirements below:

- a) as a minimum, be in possession of a recognised academic qualification equivalent to MQF Level 6 (subject to a minimum of 180 ECTS/ECVET credits or equivalent) in Law;
- b) possess good communication skills with good command of the English and/or Maltese language both written and spoken;
- c) have a minimum of 3 to 5 years' experience in technology law, EU regulation; and
- d) have been involved in technology and trust services for at least one related project worth over €1 million - project to be clearly mentioned in CV, indicating the roles performed on this project.

Key Expert 7: One (1) Systems and Network Engineer

The Systems and Network Engineer is responsible for deploying, configuring and hardening on-premises infrastructure supporting the Solution. This includes implementation and operation of hyper-converged infrastructure, configuration and management of enterprise networking including segmentation, firewalls, load balancing and secure connectivity between data centres. The expert is also responsible of supporting the integration of PKI components and HSMs in collaboration with the Trust Services Specialist together with ensuring infrastructure security baselines patching, monitoring, logging and backup/restore operations are correctly implemented.

The Systems and Network Engineer, who will be based in Malta, will contribute to operational readiness through documentation, runbooks and knowledge transfer and should work closely with other engineers to ensure alignment with the overall Solution architecture. Must have the minimum requirements below:

- a) as a minimum, be in possession of an academic qualification equivalent to MQF level 6 (or equivalent) in a field related to Information Communication Technology, Engineering or a comparable subject field;
- b) possess good communication skills with good command of the English and/or Maltese language both written and spoken;
- c) have a minimum of 3 to 5 years' experience in mission-critical, high availability, and security sensitive environments.

6.1.2 *Other experts*

CVs for experts other than the Key Experts are not examined prior to the signature of the Contract. They should not be included in tender submission.

The Awarded Bidder shall select and hire other experts as required.

All experts must be independent and free from conflicts of interest in the responsibilities accorded to them.

The selection procedures used by the Awarded Bidder to select these other experts shall be transparent, and shall be based on pre-defined criteria, including professional qualifications and language skills. The findings of the selection panel shall be recorded. The selection of experts shall be subject to approval by the Contracting Authority.

6.2 - Accommodation

Office accommodation shall be the responsibility of the Awarded Bidder and no extra claim in this regard shall be requested.

6.3 - Facilities to be provided by the Awarded Bidder

The awarded bidder shall ensure that experts are adequately supported and equipped. In particular it shall ensure that there is sufficient administrative, secretarial and interpreting provision to enable experts to concentrate on their primary responsibilities. It must also transfer funds as necessary to support its activities under the contract and to ensure that its employees are paid regularly and in a timely fashion.

7. Reports

7.1 - Reporting Requirements

Interim Progress Reports are to be prepared as per Section 2, Special Conditions, Article 24 during the period of execution of the contract.

Progress meetings are to be carried out throughout the duration of the contract as required by the Contracting Authority.

There must be a final progress report and final invoice at the end of the period of execution. The draft final progress report must be submitted at least one month before the end of the

period of execution of the contract. Note that these interim and final progress reports are additional to any required in Article 4.2 of these Terms of Reference.

7.2 - Submission & Approval of Progress Reports

Digital copies of the progress reports referred to above must be submitted to the Project Manager identified in the contract. The progress reports must be written in English. The Project Manager is responsible for approving the progress reports.

8. Monitoring and Evaluation

8.1 - Definition of Indicators

The Contracting Authority and the awarded bidder will meet weekly until the fulfilment of Milestone 16 from the Effective Date of the Contract, and every 4 weeks thereafter. If the Contracting Authority deems it necessary, meeting may take place more frequently. The Contracting Authority is responsible for:

- a) Overseeing the execution of the Contract;
- b) Overseeing the design, development and deployment of the two versions of the solution;
- c) Monitoring and managing the delivery of maintenance services;
- d) Reviewing the day-to-day performance of the awarded bidder including following the deployment, during the operational and maintenance stages; and
- e) Seeking to amicably resolve disputes that may arise between the parties in relation to this Contract.

Appendix I - The National eID System and Integration Protocols

The eid.gov.mt system is Malta's official electronic identity platform, designed to provide citizens and residents with secure access to a wide range of government services online. At its core, the system enables users to authenticate themselves once and then seamlessly access multiple e-Government services without the need to log in repeatedly. This single sign-on approach streamlines the user experience and supports both convenience and security.

Eligibility for the system extends to all eID Card holders. Registration can be completed at servizz.gov or Identità offices or by selecting the relevant option when applying for an eID card. Once identity verification is complete, users receive an activation link via email, allowing them to set up their eID account quickly and securely.

The platform offers two levels of authentication assurance. The entry level requires an ID number, password, and a time-based one-time password for two-factor authentication. For the highest level of security, users can authenticate using the chip and PIN on their eID Card, which is particularly important for sensitive transactions.

User support is a key focus, with clear procedures for account recovery and ongoing improvements to accessibility and usability. Help is available through the Identità helpdesk or the eID Section, and users are guided through each step of the activation and recovery processes.

From a technical perspective, eid.gov.mt is hosted in Azure Cloud, making use of an infrastructure which has an SLA of 99.95%, and can therefore support the proposed dependency by the Solution in the PID generation process. The eid.gov.mt system is being updated to ensure that the data set complies in full with the mandatory requirements of the PID, by introducing the fields for *BirthPlace* and *Nationality*.

The OpenID Connect (OIDC) is an identity layer built on top of the OAuth 2.0 protocol. It allows third-party applications, known as service providers, to verify the identity of users based on authentication performed by an Authorisation Server, in this case, the eid.gov.mt system. OIDC enables secure Single Sign-On (SSO) and provides a standardised way for applications to obtain basic user profile information in the form of ID tokens, which are JSON Web Tokens (JWTs).

The integration of eid.gov.mt with OIDC is documented in *eID OpenID Connect SSO Integration Document.pdf*, which outlines the procedures and technical requirements for connecting external systems to the Maltese eID platform. This document describes how service providers can configure their applications to use eid.gov.mt as an identity provider. The process involves registering the application with the eID system, configuring redirect URIs, and handling the OIDC authentication flows, such as the Authorisation Code Flow. This flow ensures that after a user authenticates with eid.gov.mt, the application receives an authorisation code, which it can exchange for an ID token and, optionally, an access token.

The protocol supports various features, including the use of the *idtokenhint* parameter for session management and the *postlogoutredirect_uri* for handling logout scenarios. The integration document also covers identity provider configuration and customisation options, ensuring that the system can be tailored to meet the specific needs of different service providers.

Security is a central aspect of the OIDC implementation on eid.gov.mt. The system leverages strong authentication mechanisms, including multi-factor authentication, and ensures that all communications are protected using TLS.

In summary, connecting to eid.gov.mt via OpenID Connect allows service providers to offer secure, standards-based authentication for their users, leveraging Malta's national eID infrastructure. The process is well-documented and designed to ensure both interoperability and robust security.

Appendix II - eID Card Integration Documentation and Sample Code

1. Documentation supporting use of Java Card Applets

Subject to the signing of the relevant Non-Disclosure Agreements, taking into consideration security, privacy and any relevant national and EU legislation, the Contracting Authority shall endeavour to provide documentation to support the use of the Java Card applets. This shall be without prejudice of any confidentiality agreements between the Government of Malta, including any Ministry, Agency, Department, Entity or Authority, and third-party providers of the eID system and commercially sensitive and proprietary documentation and rights of said third-parties.

The operating system and the underlying chip platform on which the Java Card applets operate may be subject to change from time to time due to technological, security, or supply-related considerations. Accordingly, no representation is made as to the continued use of any specific platform, the Awarded Bidder shall ensure that its solution is sufficiently adaptable to accommodate such changes within the scope of the contracted solution. Any warranties or guarantees concerning functionality, performance, or compatibility, including following changes to the operating system or underlying chip platform, shall be the sole responsibility of the Awarded Bidder. For the avoidance of doubt, the Awarded Bidder shall not, under any circumstances, rely on the absence, limitation, or perceived insufficiency of documentation as grounds for non-performance, delay, delivery, or potential solution non-conformities.

2. Terms of Use

The Contracting Authority has provided sample code solely for illustrative and reference purposes. The awarded bidder is permitted to use, adapt, or incorporate this code into their proposed solution at their own discretion.

However, by doing so, the awarded bidder assumes full and exclusive responsibility for the code's suitability, correctness, security, and integration. The contracting authority expressly disclaims any and all liability arising from the use of the sample code, and shall not be held accountable for any issues, damages, or deficiencies resulting therefrom.

3. Sample Code for Wallet Instance to eID Card Interface

It is important to note that users may be using their eID Card electronically for the first time during the Wallet enrolment. As such, the Wallet Solution must accommodate first-time eID Card usage, including the mandatory PIN change process. While the sample code provided does not cover this scenario, it is expected that the bidder addresses and implements this requirement effectively.

Android

Refer to *android-eid-card-demo.zip*

iOS

Refer to *ios-eid-card-demo.zip*

APDU Command Set Used for Sample Code

Refer to *Sample Code APDU Command Set.pdf*

Appendix III - Hosting and Service Level Requirements

Hosting Requirements

Version 1 shall be hosted on the Azure Cloud and the Solution (Version 2) shall be hosted in its entirety through Colocation within the MITA data centres in accordance with the requirements as specified in *Schedule 1 - Hosting Environment.pdf*

The GoM Azure Cloud is compliant to ISO/IEC 27001:2022 as per *Azure ISO Certificate.pdf*

Security Requirements

The Solution shall be secured in accordance with the requirements as specified in *Schedule 3 - Security Requirements.pdf*

Service Level Requirements

The Solution shall be designed to deliver a high level of reliability, supporting a service availability of 99.95%. This service level commitment ensures that the solution remains accessible and operational for users, minimising downtime and supporting continuous business operations.

The Solution in its entirety shall support a Recovery Point Objective (RPO) of 15 minutes and a Recovery Time Objective (RTO) of 2 hours.

- Recovery Point Objective (RPO) of 15 minutes: This means that, in the event of a system failure or disaster, the maximum amount of data that could be lost will not exceed 15 minutes' worth of

transactions or changes. The system must be designed so that backups or data replication occur frequently enough to ensure that any data loss is limited to the most recent 15 minutes.

- **Recovery Time Objective (RTO) of 2 hours:** This specifies that, following a disruption, the Solution must be fully restored and operational within 2 hours. The RTO defines the maximum acceptable downtime, ensuring that business operations can resume quickly and minimizing the impact on users and stakeholders.

Volumetrics

The Solution is projected to experience steady growth in active Wallet Units over the contract period. Below are the proposed estimates, for the projected number of PID authentications and electronic signatures, starting from the launch to the public of the EUDIW Solution (Version 2) and the for the subsequent 5 years. It is anticipated that the number of active users, PID authentications, and electronic signatures will stabilise from Year 5 onwards.

	Year 1	Year 2	Year 3	Year 4	Year 5
Number of Users	50,000	100,000	200,000	300,000	400,000
PID Authentication (successful logins)	1,250,000	2,500,000	5,000,000	7,500,000	10,000,000
Electronic Signature	500,000	1,000,000	2,000,000	3,000,000	4,000,000

These volumetric projections are intended to inform capacity planning and ensure the solution's scalability and performance throughout its lifecycle.

SECTION 4 - SUPPLEMENTARY DOCUMENTATION

1. Draft Contract Form

2. Specimen Performance Guarantee

3. Ultimate Beneficiary Owner (UBO) form

These are available to view and download from the 'Resources Section' at: www.etenders.gov.mt.

4. Annexes

4.1 Abbreviations and References

4.2 android-eid-card-demo.zip

4.3 Azure ISO Certificate.pdf

4.4 eID Card Interface Sample Code.java

4.5 eID Card Interface Sample Code.swift

4.6 e-ID OpenID Connect SSO Integration Document.pdf

4.7 ios-eid-card-demo.zip

4.8 Sample Code APDU Command Set.pdf

These are available to view and download from the 'Annexes' folder in the Contract documents of this CfT at: www.etenders.gov.mt.

5. General Conditions of Contract

The full set of General Conditions for Works Contracts (Version 4.8), for Supplies Contracts (Version 4.8) and for Services Contracts (Version 4.8) can be viewed/downloaded from the 'Resources Section' at: www.etenders.gov.mt.

It is hereby construed that the tenderers have availed themselves of these general conditions and have read and accepted in full and without reservation the conditions outlined therein, and are therefore waiving any standard terms and conditions which they may have.

These general conditions will form an integral part of the contract that will be signed with the successful tenderer/s.

6. General Rules Governing Tendering

The contents of this procurement document complement the latest version of the General Rules Governing Tenders applicable on the date of the publication of this tender, the Terms of Use and the Manual for Economic Operators applicable to Government's e-Procurement Platform (available from the Resources section of www.etenders.gov.mt).