



[25/09/2026]

[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)]

Clarification Note # [30]

To all prospective bidders

Reference is made to the above-captioned tender for which the deadline for submission of offers is **[05/11/2026]** at **[09:30am]**.

Please find a set of clarifications which are construed to form an integral part of the tender document.

Question No. [01]: *Operations, Maintenance, Monitoring and Support*

From the various documents it is evident that a Operations, Maintenance, Monitoring and Support platform needs to be included, to meet all the requirements for unified operational monitoring, alerting, business service, SLA, dashboarding, reporting, audit and ITSM-integration platform. questions are :

1) Is this required also for the temporary Phase 1 cloud hosted setup?

2) since the final solution is hosted onprem at MITA data Centers, does the platform to deliver Operations, Maintenance, Monitoring and Support has to also be deployed on premises, or for this layer of the solution it can be cloud SaaS hosted? to be noted that in the area of Operations, Maintenance, Monitoring and Support, a SaaS based platform is nowadays integrating a lot of AI intelligence for proactive management/monitoring, whilst onprem solution will not avail of such functionality.

Answer No. [01]:

1) As per Clause 4.2.3.11.8 'Build, Operate, Maintain and Support', "this commitment shall cover a period of seven (7) years from the date of commissioning of the Version 1." Consequently, the Operations, Maintenance, Monitoring and Support requirements apply from the commencement of Version 1 and apply to it.

- 2) As per Section 3, Appendix III, “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.” Furthermore, Section 3, Clause 4.2.3.11.10 states that “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.” Schedule 3, Clause 03.3 requires the contractor to “Ensure that Customer data shall not be stored outside the Solution, if applicable, without the Customer’s prior approval.” The same clause also states that “Furthermore, the storage of any personal data shall be in line with the Data Processing Agreement.” The bidders are to submit a bid that is in line with the CFT requirements.
-

Question No. [02]: *ISO/IEC 27001 Requirement for Consortium Members*

Dear Sir/Madam,

Having reviewed the Procurement Documents for CT2274/2026 – European Digital Identity Wallet (EUDIW), we hereby submit the following request for clarification.

Q1 – ISO/IEC 27001 Certification Requirement in Consortium Structures

Section 4.2.2 requires ISO/IEC 27001 certification for “the Economic Operator, as well as any subcontractors involved in the processing of data or delivery of security-relevant components”.

In the case of a tender submitted by a consortium composed of multiple Economic Operators with different responsibilities, please clarify whether ISO/IEC 27001 certification is required for:

a) all consortium members, irrespective of their allocated scope of work; or

b) only those consortium members and subcontractors that are involved in the processing of personal data, operational service delivery, trust service provision, access to production environments, or the delivery of security-relevant components.

Please confirm which interpretation applies for the purposes of this procurement.

Yours faithfully,

Answer No. [02]: The ISO/IEC 27001 certification requirement is established under Section 1, Article 5(d) – Quality Assurance Schemes and Environmental Management Standards, and further addressed under Article 7.3 of the Special Conditions which states that “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”. It is the

responsibility of bidders to identify any consortium members or subcontractors involved in the processing of data or delivery of security-relevant components within their proposed solution and to ensure compliance with the ISO/IEC 27001 requirement.

Question No. [03]: *Request for Clarification*

Hardware / HSM / Hosting

1. Does the staging environment required under Clause 4.2.1.3.1, which must "mirror" the production environment in terms of configuration, performance and security controls, require the same dual-site redundancy (2 data centres) required for production, or can it be implemented on a single site?

Answer No. [03]: Section 3, Clause 4.2.1.3.1 requires the bidder to provide “a dedicated staging environment that is logically and physically separate from both the development and production environments” and further states that the staging environment “must closely mirror the production environment in terms of configuration, performance, and security controls.”

Question No. [04]: *Request for Clarification*

Hardware / HSM / Hosting

2. What level of redundancy is required for the HSMs (N+1 or N+2) to meet the RPO of 15 minutes and the RTO of 2 hours defined in Appendix III?

Answer No. [04]: It is the bidder’s responsibility to propose and implement an approach that satisfies the requirements of this CfT. In relation to the level of redundancy, the bidder remains fully responsible for ensuring that the proposed architecture complies with all requirements of the Call for Tender, including, but not limited to, the prescribed RTO and RPO requirements in Appendix III.

Question No. [05]: *Request for Clarification*

Hardware / HSM / Hosting

3. With regard to hardware refresh due to End-of-Life/End-of-Support, as provided for under Article 50.1 of the Special Conditions: does the Contracting Authority have any expectation or indicative budget as to the expected frequency of replacement, or is this cost entirely to be estimated by the Awarded Bidder in the financial offer?

Answer No. [05]: Section 2, Article 50.1 establishes the contractor's obligations in relation to hardware replacement arising from End-of-Life, End-of-Sale, or End-of-Support situations. No indicative budget, replacement frequency, or refresh cycle is being prescribed by the Contracting Authority. Bidders shall estimate and include any costs associated with such hardware replacement in their financial offers, as necessary.

Question No. [06]: *Request for Clarification*

Hardware / HSM / Hosting

4. Is there a list of pre-approved or already certified HSM models accepted by the MDIA/MITA, or is it at the bidder's discretion to propose the model provided it meets the eIDAS/[EUDI Regulation] requirements?

Answer No. [06]: No list of pre-approved, approved or pre-certified HSM models is being provided by the Contracting Authority. The selection of the HSM vendor and model is at the bidder's discretion, provided that the proposed solution complies with all requirements of the Call for Tenders. As previously clarified (Clarification Note 7 Question No 3), no restrictions are imposed on the selection of vendors or hardware models, provided that the proposed equipment is compatible with standard and existing 19-inch racks, can be accommodated within racks with a maximum depth of 1000 mm already available` at the two MITA Data Centres, and complies with standard enterprise power and cooling requirements, without necessitating any special or non-standard power, cooling, or environmental provisions. Bidders are also encouraged to refer to Clarification Note 24 Question No 16.

Notwithstanding the above, the awarded bidder shall remain solely responsible for ensuring that the proposed solution, including the entire supply chain, all associated components, and all hardware and software supplied, fully complies with and satisfies all requirements, obligations, standards, service levels, and performance commitments set out in the Call for Tenders.

Question No. [07]: *Request for Clarification*

Hardware / HSM / Hosting

5. What level of physical segregation is required between the PKI components and the remaining components of the Solution (Clause 4.2.2) — distinct racks, distinct rooms, or distinct data centres?

Answer No. [07]: The required level of segregation shall depend on the final technical architecture and security model proposed by the tenderer, including the classification and criticality of the relevant PKI components, the proposed physical and logical security controls, access-control arrangements, resilience requirements, and the associated risk assessment.

The proposed solution shall, in all cases, comply with the applicable [EUDI Regulation], relevant ETSI standards predominantly ETSI EN 319 401 and other applicable security requirements, including the requirement for security critical trust service components to be located within an appropriately protected security perimeter and accessible only to authorised personnel with strict role segregation.

The adequacy of such arrangements, including whether additional segregation at rack, room or data-centre level is required, shall be assessed in the context of the overall solution and shall remain subject to the Contracting Authority's evaluation and discretion during the selection process of the solution.

Question No. [08]: *Request for Clarification*

Human Resources / Key Experts

6. *The requirement that Key Expert 7 (Systems and Network Engineer) be "based in Malta" — is an extended or rotational deployment arrangement acceptable, or does this imply effective residence in Malta from the start of the contract?*

Answer No. [08]: The ‘Systems and Network Engineer’ needs to be physically present in Malta to fulfil the responsibilities as per Section 3, Clause 6.1.1, which start from configuration and deployment, and includes operation for the duration of the contract. As per Section 2, Article 18.2 “the period of execution of the contract shall be of ninety (90) months” which includes, but is not limited to, the operation of the Solution. For KE7 (Systems and Network Engineer), bidders are kindly requested to propose a natural person that possess as a minimum the requirements set in Tender Document - Section 3 – Article - 6.1.1 - Key Experts. The Key Experts Form requires Name and Surname, Nationality, Age, Qualifications and Professional authorisation (where applicable). These fields can only be completed by one natural person, not by a company or team.

Question No. [09]: *Request for Clarification*

Human Resources / Key Experts

7. *For the "Other Experts" referred to in Clause 6.1.2, is there any minimum requirement regarding the percentage of resources resident in Malta within the wider team, beyond the Key Experts?*

Answer No. [09]: There is no minimum requirement regarding the percentage of resources based in Malta within the wider team beyond the requirement explicitly specified for Key Expert 7 as per Section 3, Clause 6.1. In addition, bidder may choose to opt for the add-on as per BPQR criterion 1.7 (a) for Key Expert 1 and in doing so commit to basing Key Expert 1 in Malta.

Question No. [10]: *Request for Clarification*

Technical Scope

8. *Can it be confirmed that the development, personalisation, issuance and maintenance of the physical eID Card (including its issuing PKI) are entirely outside the scope of this contract, as indicated in Clauses 4.2.2 and 4.2.3.10.5, and that the Awarded Bidder's responsibility is limited*

to integrating the Wallet with the existing eID Card (via NFC/PACE) as an authentication mechanism and external QSCD for the creation of QES?

Answer No. [10]: Yes, as per Section 3, Clause 4.2.2.2 “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.” As per Section 3 Clause 4.2.3.7.3 “The Wallet Solution shall be able to connect to the eID Card through the NFC protocol to reach the QSCD.” Figure 1 clearly shows that the physical eID Card are outside the scope of this contract.

Question No. [11]: *Request for Clarification*
Technical Scope

9. Does responsibility for integration with eid.gov.mt (national authentication) include changes to the eid.gov.mt system itself, or is it strictly integration on the Wallet Solution side?

Answer No. [11]: The awarded bidder is not required to perform any changes to the eid.gov.mt system itself. Any changes to the national eID infrastructure remain the responsibility of the respective system owner. As per Section 3, Clause 4.2.2.2: “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.” Furthermore, “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).”

Question No. [12]: *Request for Clarification*
Technical Scope

10. Which specific item(s) of the Financial Bid Form correspond to the 7,000 Person Hours of consultancy (Clause 4.2.1.2, relating to legislative changes) and the 20,000 Person Hours of development (Clause 4.2.1.3.6, relating to new use cases)? Are these hours to be priced as a separate time-and-materials item (e.g. via an hourly rate per Key Expert profile), invoiced and paid only as actually consumed and confirmed by timesheets (as suggested by the payment mechanism for items 13, 14 and 16 under Article 26.1) — i.e. on a "use it or lose it" basis — or are they already deemed to be included within the fixed milestone-linked payments for Version 1 and Version 2, and therefore payable regardless of whether they are actually requested?

Answer No. [12]:

The 7,000 Person Hours are for consultancy relating to changes arising during contract implementation from new legislation, implementing acts and standards corresponding to Item 16, “Consultancy services on changes from new Legislation, Implementing Acts and Standards”, of the Financial Bid Form. The 20,000 Person Hours for the development of new use cases correspond to Item 14, “Development of use cases”.

The Contracting Authority confirms that the 7,000 consultancy hours and the 20,000 development hours form part of the scope of the contract and must be priced through the corresponding items of the Financial Bid Form. Their utilisation shall be determined by the Contracting Authority on a case-by-case basis in accordance with the applicable contractual provisions and subject to agreed delivery requirements.

As per Section 2, Article 26.1 “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” and “Payment 20 shall be released on a monthly basis for item 14 of the financial bid as confirmed by the awarded bidder and verified by the Contracting Authority.”

All other tender documents, conditions and requirements, which are not superseded by this clarification remain in place.

Department of Contracts