



[23/09/2026]

[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 # [26]

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]: *Tender document, Section 3, Article 4.2.1.3.1 We understand that the bidder is required to provide three environments: development, staging, and production. We would appreciate clarification on the following points:*

- a) Development environment Is the development environment considered part of the required project deliverables?*
- b) If so, must it be hosted within the same infrastructure and locations as the staging or production environment, or is hosting in the bidder's own data centre acceptable?*
- c) Staging environment Is the staging environment required to be deployed in both production data centres, or is deployment in a single data centre sufficient?*
- d) Must the staging environment mirror the production environment in terms of performance, capacity, availability, and resilience?*
- e) If full production equivalence is not required, could you please specify which requirements may be relaxed for the staging environment (e.g. performance, capacity, high availability, disaster recovery, or resilience requirements)?*
- f) It is mentioned that the staging environment is "logically and physically separate". How is this statement to be interpreted within a shared MITA tenant?*
- g) Will MITA provision separate Resource Groups, separate subscriptions, or separate regions for the staging environment?*

Answer No. [01]:

a) The tender requirements refer to development, testing and production environments maintaining “Logical or physical separation of environments for development, testing, and production” as per Section 3, Clause 4.2.1.3.7 and require “Automated secure configuration baselines for all environments (development, testing, production)” as per Section 3, Clause 4.2.1.3.7.6. For these requirements to be achieved, a development environment must exist and be provisioned by the contractor as part of the solution delivery. Acceptance and Testing to verify whether Milestones have been met will be performed either using mobile apps made available to the CA, in the staging or production environments as applicable. Section 3, Clause 4.2.1.3.7 defines the ‘Secure Development Practices’ requirements for the Solution, including but not limited to the development environment.

b) Section 3, Clause 4.2.1.3.7 demands “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.” The CfT does not prescribe a specific hosting location for development environments. Bidders are responsible for ensuring that environments are appropriately segregated and operated in accordance with the security requirements of the tender.

c) The CfT requires the provision of a dedicated staging environment that is logically and physically separate from the development and production environments as per Section 3, Clause 4.2.1.3.7. The CfT does not require the staging environment to be deployed across both production data centres. Accordingly, deployment of the staging environment in a single data centre is acceptable, provided that all requirements are met.

d) e) As per Section 3, Clause 4.2.1.3.1 “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”. The bidder shall propose an appropriate staging environment that satisfies these objectives.

f) g) There will be two subscriptions available, and segregation may also be achieved through the use of separate regions where appropriate. The bids submitted should be in line with the requirements in the CfT. Bidders should base their proposals on the requirement that the staging environment be logically and physically separate from the development and production environments.

Question No. [02]: *Tender document, Section 3, Article 4.2.1.3.6*

a) *Is the Verification Engine required to be delivered solely as software components, documentation, APIs and source code, or does the scope also include implementation,*

deployment, hosting, operation, maintenance and support of Verification Engine instances used by Public Body Relying Parties?

- b) If operational deployment is in scope, is a centrally hosted Verification Engine expected, or should the bidder support deployments operated individually by each Public Body?*
- c) If Public Bodies are expected to self-host the Verification Engine, what level of onboarding, technical support and operational assistance is expected from the awarded bidder?*
- d) Are the costs for deployment and operation of Verification Engine instances by Public Bodies expected to be included in the financial proposal, or are these considered future onboarding activities outside the scope of the initial implementation?*

Answer No. [02]:

a) The ‘Attestation Verifier Component’ defined in Section 3, Clause 4.2.1.3.6 and depicted in Figure 1 is external to both the Wallet Instance and the PID Provider. It is a standalone component including the complete source code, such that it can be integrated by Public Bodies in other applications. The awarded bidder shall develop, support and maintain this component. Support and maintenance is limited only to the version provided to the CA, and not versions as modified by the Relying Parties.

b) The intent is to provide Public Bodies the verification engine that they can integrate within their own applications, therefore operational deployment is not in scope.

c) The CfT requires the awarded bidder to deliver the ‘Attestation Verifier Component’, including its complete source code, provide the necessary technical integration documentation to support and guide the public bodies during onboarding. As per Section 3, Clause 4.2.3.11.9 “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”.

d) Not in scope as per Answers (a) and (b) above.

Question No. [03]: *Tender document, Section 3, Article 4.2.1.1 For Version 1 of the app, it is stated that the solution is preferably compliant with the EU Age Verification Blueprint. Could the Contracting Authority clarify whether the role of the Proof of Age Attestation Provider (AP) must be implemented within the Azure environment, or whether the Bidder may subcontract this function to a QTSP that would manage the required PKI infrastructure and perform the attestation services on behalf of the Maltese Government? In other words, is outsourcing the AP function to a QTSP (outside Azure) allowed?*

Answer No. [03]: In accordance with Section 3 Clause 4.2.1.1 and BPQR criterion 1.1 (a): “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)." Moreover, as per BPQR addon criterion 1.1 (f) and 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". This does not preclude subcontracting this function to a QTSP.

Question No. [04]: *Schedule 1, Schedule 3 Must infrastructure services, including but not limited to CDN, DDoS protection, WAF, DNS, load balancing, and similar networking/security services, be hosted within the target platform environment (Azure for V1 and the MITA data centres for V2), or is the use of external managed service providers permitted? If permitted, please describe any applicable restrictions or requirements.*

Answer No. [04]: Bidders shall be responsible for proposing a solution architecture that meets all applicable CFT requirements and does not depend on the use of MITA's perimeter network components.

Internet facing services shall be deployed by the bidder on site to ensure minimum latency and optimal service delivery, however, with respect to DDoS and CDN capabilities, the bidder may propose a SaaS or cloud-based model.

The eventual cost for these capabilities may be included in Item 15 of the Financial Bid, as part of the Operation, Maintenance and Support of Version 2.

Question No. [05]: *Tender document, Section 2, Article 4.2.3.10.5 Extract: "the awarded bidder shall supply all supporting documentation for the PKI, including the following...". Should this requirement be interpreted as the bidder delivering these artefacts to the Contracting Authority, or is it assumed that the bidder is responsible for the hosting, publication, availability, and ongoing management of these artefacts throughout the contract period?*

Answer No. [05]: The requirement that the "awarded bidder shall supply all the supporting documentation for the PKI" should be understood as an obligation to provide the relevant PKI artefacts and documentation to the Contracting Authority and maintain them through the duration of the contract. The CA is responsible for hosting and publication of these artefacts.

Question No. [06]: *For Version 2 – Other requirements for the Solution developed in line with the [EUDI Regulation] regarding section 4.2.3.11.8 Build, Operate, Maintain and Support: Please specify your understanding of the word "operate" in regards to security requirements over the duration of the contract and what should be included.*

Answer No. [06]: Operate, Maintain and Support includes, amongst others, 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” as per Section 3, Clause 4.2.3.11.8. Furthermore, Section 3 Clause 4.2.3.11.8 states that “The awarded bidder shall be responsible for the complete delivery of the Solution, encompassing its design, development, deployment, operation, and ongoing support.” Finally, Section 3 Clause 4.2.3.11.9 also outlines security implications “At the operations, maintenance, and support stage” obliging the Awarded Bidder “to provide all documentation necessary for the ongoing operation, support, and continuous improvement of the system”. In the context of the security requirements and the Build, Operate, Maintain model, "operate" entails, among others, the day-to-day running of the solution and security controls, including monitoring, incident handling, log management, patching, maintaining service levels, and ensuring the solution remains secure and available in production.

Question No. [07]: *CT2274_2026 - Tender document - Digital Identity Wallet, §4.2.1.3.6; §4.2.3.11*

Please explain who is responsible for the distribution of Wallet application security updates, mandatory version enforcement and ongoing application maintenance during operations.

Answer No. [07]: The awarded bidder, acting on behalf of the Contracting Authority, shall be responsible of these activities. As per Section 3, Clause 4.2.3.11.8 “The awarded bidder shall be responsible for the complete delivery of the Solution, encompassing its design, development, deployment, operation, and ongoing support”. Section 3, Clause 4.2.1.3.5 states that the “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).” Additionally, Section 3, Clause 4.2.1.3.7 details how security updates are to be provided.

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

Department of Contracts