



[04/09/2026]

[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 # [20]

To all prospective bidders

Reference is made to the above-captioned tender for which the deadline for submission of offers is **[15/10/2026]** at **[09:30am]**.

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

Question No. [01]: *Clarification Requests*

Clarification Query 1: Independent Third-Party Penetration Testing

With reference to the requirement for penetration testing by independent third parties, could the Contracting Authority clarify whether the Contractor is expected to directly procure and fund the external accredited third-party penetration testing entity under the global price, or whether the Contracting Authority/MITA will separately engage an independent auditor for these assessments?

Answer No. [01]: As listed in BPQR Criterion 1.6 (c) the Awarded Bidder is expected to procure and fund “Penetration testing by independent third parties” as part of the contract cost if they opt to use this addon. The Contracting Authority reserves the right to, at its own expense, engage an independent auditor to review and validate the penetration testing assessments and associated remediation measures in line with Section 2, Article 44.4.

Question No. [02]: *Clarification Requests*

Clarification Query 2: Threat Intelligence Feeds and SIEM Infrastructure

Regarding the requirement for sector-relevant commercial cybersecurity threat intelligence feeds and real-time SIEM monitoring:

- *should bidders include commercial feed subscription licensing costs within their financial offer, or will GoM/MITA provide access to existing threat intelligence subscriptions?; and*
- *is the Contractor required to procure, deploy, and manage a standalone SIEM instance within the colocation setup, or will security logs be forwarded to MITA's central SOC/SIEM?*

Answer No. [02]: As per Section 3, Article 4.2.1.3.7.14, there should be “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.” The Bidders will not be provided access to existing GoM/MITA threat intelligence subscriptions.

Section 3, Clause 4.2.1.3.7 states that “The winning bidder shall maintain current independent verification of the effectiveness of its technical and organisational security measures.” It is expected that the bidder provides the components, services and licences necessary to satisfy the security, monitoring, logging, incident management and service level requirements as specified. The Awarded Bidder is not to assume that Security Logs will be forwarded to MITA's central SOC/SIEM to fulfil the requirements of this CFT.

Question No. [03]: *Clarification Requests*

Clarification Query 3: SAST and DAST Tooling Licensing

In relation to SAST and DAST execution within secure CI/CD pipelines, please confirm whether bidders are expected to include SAST/DAST software license fees in their financial offer, or if integration should be established with MITA's existing application security testing tools.

Answer No. [03]: As per Section 3, Clause 4.2.1.3.7.2 it is mandatory that “Static Application Security Testing (SAST) and Dynamic Application Security Testing (DAST) shall be executed prior to major releases or deployments.” As per BPQR Criterion 1.6 (b), Integration with CI/CD pipelines is an optional addon. Such licenses are considered “Vendor Retained” in line with Section 2, Article 14.7 and Awarded Bidder is not to assume integration with MITA's existing application security testing tools.

Question No. [04]: *Clarification Requests*

Clarification Query 4: Baseline Frequencies for Operational Audits & Drills

To ensure a level playing field and consistent pricing across all tenderers, could the Contracting Authority define the baseline annual frequency expected during the operational phase for:

- *Operational Security Architecture Reviews; and*
- *Incident Response Drills and Simulations.*

Answer No. [04]: BPQR Criteria 1.6 (a) is graded with ‘Max of 2 marks’ and requests “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”. Similarly, BPQR Criteria 1.6 (i) (also graded with a ‘Max of 2 marks’) requests “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”.

It is expected that the bidder defines these proposals and plans, which will be graded accordingly.

Question No. [05]: *Clarification Requests*

Clarification Query 5: Scope of RASP Implementation

Could the Contracting Authority clarify whether Runtime Application Self-Protection (RASP) capabilities are expected to be implemented exclusively on the mobile application instances (Android/iOS), or if RASP is also required across backend server components and microservices?

Answer No. [05]: BPQR Criteria 1.6 (g) which is optional and graded with 2 add-on marks, asks the bidder to explain the extent and proposed use of RASP capabilities.

Question No. [06]: *Clarification Requests*

Clarification Query 6: Allocation of Person-Hours for Cybersecurity Standards Updates

Section 3 Clause 4.2.1.2 stipulates an allocation of 7,000 Person Hours for consultancy services on changes stemming from new legislation, implementing acts, and standards. Could you confirm whether development work required to adapt the system to new Cyber Resilience Act (CRA) standards, NIS2 requirements, or EUCC schemes arising post-award will be deducted from this 7,000-hour pool?

Answer No. [06]: Section 3, Clause 4.2.1.2 states “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.” Development work deviating from the CTF is covered by Contract Modifications as specified in Section 2, Article 20.

Question No. [07]: *Clarification Requests*

Clarification Query 7: On-Premises Hosting Requirement Scope

Does the on-premises hosting requirement apply strictly to the core identity components of the solution (Wallet Provider, PID Provider, PKI, and Register)? Specifically, is supporting tooling for fraud detection, behavioral analytics, or anomaly detection—which operates on wallet activity logs rather than issuing, verifying, or storing credentials—exempt from being considered part of the Wallet Solution subject to this hosting requirement?

Answer No. [07]:

The Solution shall be hosted in its entirety (including the PKI) in the GoM's secure hosting environment, using Colocation within MITA data centres as per Section 3, Clause 4.2.3.11.10.

Section 3, Clause 4.1.4, 10 defines “‘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.”

Question No. [08]: *Clarification Requests*

Clarification Query 8: Fraud and Anomaly Detection Data Storage vs. Processing

For components performing fraud detection, anomaly detection, or behavioral analytics based on wallet transaction logs, must the detection and analytics processing run on infrastructure physically located in Malta, or does this residency requirement apply only to the storage and retention of the underlying logs and source data?

Answer No. [08]: Refer to Answer No. [07] above.

Question No. [09]: *Clarification Requests*

Clarification Query 9: Personnel Residency Requirements

Aside from the residency requirement specified for the Systems and Network Engineer, are there physical residency requirements for other personnel performing security monitoring, incident response, or analytics review functions?

Answer No. [09]: Section 3, Clause 5.1 states that “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”. With regards to Key Expert 1- Project Manager, as per BPQR criteria, 1.7(a) additional marks will be awarded if “based in Malta for the duration of the project”.

Question No. [10]: *Clarification Requests*

Clarification Query 10: Intellectual Property Classification for Commercial Products

When a security or fraud-detection component is based on a pre-existing commercial product rather than being custom-built, should the technical offer classify the underlying product as third-party IP (perpetually licensed to the Contracting Authority), while treating only the specific rule sets, dashboards, and integrations developed for this project as assignable IP?

Answer No. [10]: Yes, confirmed.

Question No. [11]: *Clarification Requests*

Clarification Query 11: Consortium Eligibility Criteria

Are consortium members permitted to combine their experience, turnover, and insurance to meet the tender's eligibility criteria?

Answer No. [11]: Refer to General Rules Governing Tenders, Article 2, in particular Articles 2.3, 2.4 and 2.5.

Question No. [12]: *Clarification Requests*

Clarification Query 12: Data Center Perimeter Network Components

Do the data centers hosting the Wallet Solution utilize perimeter network components, such as Application Delivery Controllers (ADCs) or a Content Delivery Network (CDN)?

Answer No. [12]: 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.

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

Department of Contracts