



[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 # [25]

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]: *For the technical and professional ability criterion requiring at least two similar projects delivered between 2023 and 2025, with a cumulative value of at least €5,000,000, can MDIA confirm whether “Trust Services” refers to trust services as defined under Article 3(16) of Regulation (EU) No 910/2014 (eIDAS)?*

Answer No. [01]: The Contracting Authority confirms that, for the purposes of this selection criterion, "Trust Services" can be understood as trust services within the meaning of the [EUDI Regulation].

Question No. [02]: *Can the intermediary services be delivered through a hybrid model, where PID issuance and qualified QEAA issuance are hosted on-premises within MITA, while non-qualified EAA issuance is provided through a cloud service? If so, would this cloud component, offered as an optional add-on and not as a dependency of the certifiable EUDIW core, be compatible with the IP-assignment requirements under Article 14 and the runtime-independence requirements under Article 46?*

Answer No. [02]: PID issuance is part of the PID Provider components as per Section 3, Clause 4.2.3.10.4. The PID Provider component forms part of Version 2 of the Solution as defined in Section 3, Clause 4.1.4 and as per Section 3, Clause 4.2.3.11.10 “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 IP

of the PID Provider is defined in Section 2, Article 14.7 and subject to the IP category as identified in the Ownership Matrix defined in the same article. The CfT does not include in scope issuance of EAAs or Q-EAAs, but the wallet user shall be allowed to request, store and present such attestations which will require integration with issuers of EAAs/Q-EAAs. Finally, as per Section 3, Clause 4.2.1.3.6, “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.”

Question No. [03]: *Can verification services also be delivered through a hybrid model, with the Verification Engine and corresponding source code deployed on-premises for public-body Relying Parties, while verification for cross-border and private-sector Relying Parties is provided through a cloud acceptance service?*

Answer No. [03]:

There are three different verification components as follows:

- One verification component that is part of the Wallet Instance and is referred to as ‘RP Verification Component’ and ‘RP verifier component’ within the CfT as per
 - Section 2, Articles 14.6, 14.7, 18.2
 - Milestone 9
 - Section 3 Clause 4.2.3.4.3
- One verification component that is part of the PID provider component and is referred to as ‘WUA Verifier component’ in Section 3, Clause 4.2.3.10.1.
- One verification component labelled as ‘Attestation Verifier Component’ in Figure 1 that is external to both the Wallet Instance and the PID provider as per Section 3 Clause 4.2.1.3.6 “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.”

The ‘Attestation Verifier Component’ is a bespoke deliverable and will be fully owned by the CA. The CA’s license term with Relying Parties that are Public Bodies is beyond the scope of this CFT. Ownership of the Solution is defined in Section 2, Article 14 and "the Solution (Version 2) shall be hosted in its entirety through Colocation within the MITA data centres" as per Appendix III. For clarity, the answers provided should not, however, be construed as limiting the bidder’s responsibility to include any other components that may be required for the proper functioning and delivery of the solution in line with the specified requirements.

Question No. [04]: *Is the public awareness, marketing, and citizen-adoption communications campaign within the bidder's scope, or will it be retained by MDIA or Government? If it is within scope, should it be funded within the estimated contract value, or through the additional-services and use-case pools?*

Answer No. [04]: Section 3 Clause 4.2.1.3.6 states that “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 meet the Branding obligations set out in Section 3, Clause 4.2.1.3.4 as per Milestone 1. Public awareness, marketing and citizen-adoption communications campaigns will be retained by the Contracting Authority.

Question No. [05]: *Can commercial threat-intelligence feeds and risk-assessment services be provided as external subscriptions or APIs, rather than as IP-assigned bespoke deliverables, provided that they are consumed by the on-premises SIEM?*

Answer No. [05]: 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.” Therefore, external subscriptions or APIs can be used if acquired in the name of the Contracting Authority.

Question No. [06]: *Tender document Section 2: 14.7 The tender documentation states that all intellectual property rights to the Bespoke Deliverables must be transferred in full ownership to the Contracting Authority. Could you clarify whether this requirement excludes the use of the EU Reference Implementation or any other open-source software components for those parts of the solution where full ownership transfer is required? Alternatively, can we assume that the use of open-source licensed solution (components) or commercial licensed solution (components) for the components: Wallet Provider, PID Provider, Relying Party Registrar, Signing Certificate Provider (PKI), WPRAC Provider, RP Verification Component, Wallet Instances, is permitted, provided that the Contracting Authority receives the necessary perpetual rights, and that the full ownership requirement applies only to the Malta-specific custom developments delivered under this contract?*

Answer No. [06]: Section 2, Article 1.3 provides a definition of “Bespoke Deliverables” and clearly states that “Bespoke Deliverables do not include Third-Party Components or Vendor-Retained Components”. The Ownership Matrix defined in Section 2, Article 14.7 lists the Components for which “Full Ownership” is mandatory, that are Wallet Provider, PID Provider, Relying Party Registrar, Signing Certificate Provider (PKI), WPRAC Provider, RP Verification Component and Wallet Instances. The submitted bid, specifically BPQR Criteria 2.8 (a) and (b), will define the ownership of Version 1 and the SCA respectively and the use of open-source and

commercially licensed components is not precluded for these components. However, bidders shall ensure compliance with the intellectual property, source code and deployment requirements set out in Article 14.

Question No. [07]: *Schedule 2 – § 1.2 Help Desk Tender Document §4.2.1.2 Technical support for wallet users Extract: "The Awarded Bidder will provide to the Contracting Authority such technical advice by telephone help desk or e-mail as is necessary to resolve the Contracting Authority's difficulties and queries in using the Solution."*

a) Please confirm whether this is a help desk to assist government ICT staff.

b) Please confirm what is meant by "using the Solution" exactly.

c) Also in the main document it says: "4.2.1.2 Version 2 - Wallet Solution functionalities 13) Wallet Users shall be able to easily request technical support and report technical problems and other incidents (item 10);" This seems to refer to a help desk for end users (citizens). Please clarify the scope and the distinction with the helpdesk requirement stated in Schedule 2 §1.2.

Answer No. [07]: a) Yes, the help desk is to assist government staff (both ICT and non-ICT) as per referred Schedule 2, Section 1.2 that states "The Awarded Bidder will provide to the Contracting Authority such technical advice by telephone help desk or e-mail as is necessary to resolve the Contracting Authority's difficulties and queries in using the Solution." Section 3, Clause 4.2.2 includes requirements that the "Contracting Authority shall have the flexibility to determine and assign the ownership of individual architectural components to other entities" and that "Transfer of ownership of a particular component will imply transfer of rights and obligations." Such entities are expected to be able to raise incidents and service requests to the help desk.

b) If the CA is informed of incidents and/or issues with the components delivered by the awarded bidder (irrespective of the source reporting such incidents or issues), and the CA cannot address those queries, the CA will forward it to the awarded bidder as part of the help desk. In addition, if the CA experiences issues with the backend functionality of any of the components, these will also be raised through the help desk. Using the Solution also refers to the integration between the components. Therefore, the Contracting Authority and other entities (as per (a) above) using the Solution shall submit shall report incidents and issues, and service requests using the help desk.

c) Section 2, Clause 4.2.1.2 (13) states that "Wallet Users shall be able to easily request technical support and report technical problems and other incidents (item 10)", where item 10 refers to Article 5(10) of the [EUDI Regulation]. This functionality is distinct from the aforementioned help desk and is mandated by the regulation to be provided to end users as part of standard Wallet Instance functionality. These requests for technical support and reports of technical problems and other incidents are submitted to the CA.

Question No. [08]: *Schedule 1 – 10.5 Network Connectivity and Routing Extract: "‘Access from the Internet to the Solution (for Solutions hosted on-premise) will be managed by the Contractor and MITA.’ Please confirm whether the cost of internet traffic is or isn't charged to the Contractor. Please provide more details regarding internet security mechanisms which are de facto provided by MITA (this does not negate the requirement that we as Contractor are expected to manage security for our own network infrastructure). Please provide more information on the split of roles and responsibilities between the Contractor and MITA.*

Answer No. [08]: For Version 2, the Contracting Authority will provision and fund its own links with local Internet Service Providers for any required connectivity. MITA will not provide any shared hosting/operations services in support of the Solution. It is expected that the bidder will provide the components, services and licenses necessary to satisfy the security, monitoring, logging, incident management and service level requirements as specified.

Question No. [09]: *Schedule 1, Article 6.1 Colocation and network Extract: "(c) network connectivity to the Data Centre, Malta Government NETwork (MAGNET) can also be provided." Please confirm whether this is a possibility (conditional, to be negotiated) or a hard commitment. Please explain whether the usage of MAGNET differs between version 1 (Azure-hosted) and version 2 (MITA data centre-hosted).*

Answer No. [09]: In the proposed architecture for Version 1 and Version 2, there is no dependency on MAGNET-related resources. Any reference to MAGNET should therefore be considered optional and relevant only in the unlikely event that a bidder requires such access as part of its proposed solution. However, any connectivity requirements would therefore be assessed in the context of the final solution design.

Question No. [10]: *Could you please provide the projected V1 user numbers, authentication volumes, and age-verification transaction rates for the period between V1 go-live and V2 launch?*

Answer No. [10]: The number of users for Version 1 is expected to gradually grow from its launch and not exceed 50,000 by the time Version 2 is launched. Other volumes and transaction rates should be reasonable, proportionate to that volumetrics, and consistent with the intended national deployment of Version 1.

Question No. [11]: *Schedule 1, Article 6. Colocation Extract: "MITA's hosting fees for Colocation can be found here – <https://mitaquotecalculator.gov.mt/> " The provided link is not accessible without credentials. Please provide instructions on how to obtain the necessary credentials.*

Answer No. [11]: For Version 2, the contracting Authority will be covering MITA's hosting fees for Colocation, and therefore these shall not be included in the Financial Bid.

Question No. [12]: *Tender document, Section 3, Article 4.2.1.1 Extract: " This mobile application may not necessarily be compliant with the [EUDI Regulation] but will leverage existing infrastructure where possible..."*

a) What specific "existing infrastructure" is expected to be leveraged for Version 1? please provide details.

b) Are there existing PKI services, or any reusable national trust infrastructure, which are available for Version 1?

Answer No. [12]:

a) Existing infrastructure refers to the physical eID cards in circulation, the existing national eID infrastructure and related authentication mechanisms where applicable. As per Section 3, Clause 4.2.1.1 "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". BPQR Criterion 1.1 (e) awards 2 add-on marks to bidder who commit to provide "a Version 1 that authenticates with Malta's national eID infrastructure at LoA High on launch". Other than the existing national eID infrastructure referenced in the tender for authentication, bidders shall assume responsibility for procuring, licensing, deploying and operating all components required to implement and support Version 1.

b) With regards to PKI in Version 1, there is no National Trust Infrastructure available for reuse. The Awarded Bidder is allowed to make use of third-party Trust Services to issue the proof of age attestations. However, this needs to transition to rely on the on-premises PKI for Version 2 as per Section 3, Clause 4.2.3.10.5. In accordance with Section 3 Clauses 4.2.1.1 and 4.2.1.3.3, BPQR Criterion 1.1 (f) awards 2 add-on marks if "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 (add-on)."

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

Department of Contracts