



[03/09/2026]

[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 # [18]

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]: *CT2274_2026 - Tender document - Digital Identity Wallet, 4.2.3.11.8*
Please clarify if a remote support from inside and outside of Malta would be excepted in case of solving critical incidents.

Answer No. [01]: Please refer to Clarification Note14, Question [07].

Question No. [02]: *CT2274_2026 - Tender document - Digital Identity Wallet, 4.2.3.11.8*
Please confirm that only the CA can raise incidents and service requests to the helpdesk.

Answer No. [02]: Please refer to Clarification Note14, Question [08].

Question No. [03]: *Technical and Professional Ability*
Regarding Selection Criterion (c) – Technical and Professional Ability, the procurement documents state that "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)."

We understand that, where the bidder submits a certificate of satisfactory/good execution issued and signed by the contracting authority (e.g. a European Institution, the European Commission, an EU Agency or another international organisation), and such certificate explicitly confirms the successful execution of the contract as well as its total contractual value, this evidence should be considered sufficient to demonstrate compliance with this requirement, as it is an official document issued by a public contracting authority and therefore provides independent and reliable confirmation of the successful execution and value of the contract, without the need to provide a separate declaration signed by a warranted Auditor.

Could you please confirm whether our understanding is correct?

Answer No. [03]: Please refer to Clarification Note 8, Question [02].

Question No. [04]: *Clarification 7Aug 1*

Appendix III Appendix III – Hosting and Service Level Requirements Appendix III states that “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”.

Could you kindly confirm that there are no requirements for Colocation hosting in the MITA data centres for Version 1? If there are any requirements that need to be considered in this regard, could you kindly confirm what these requirements are?

In addition, could you kindly confirm your expectations for the PKI in Version 1?

3 Ref: Clauses 4.2.1.1, 4.2.1.3.3, 4.2.1.3.6, ProofOfAge Credential Issuance

4.2.2 Version 1 issues a cryptographically secured ProofOfAge attestation which is subsequently presented to relying parties. It is stated this will also continue to be used in Version 2.

The Tender Document does not, however, specify how this attestation will be issued. The Version 2 architecture diagram in Section 4.2.2 also only shows a PID Provider in scope and does not show a Pub-EAA Issuer nor does the PKI seem to consider this.

Do you believe you could kindly elaborate more on this topic and how you would like this to be issued and covered especially from a backend perspective? This includes during both Version 1 and 2 of the application.

Answer No. [04]:

As per Appendix III, “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”.

With regard to Version 1, Section 3, Clause 4.2.1.1 states that “This mobile application may not necessarily be compliant with the [EUDI Regulation] but will leverage existing infrastructure where possible.” And that “backend functionality must be hosted within the MITA’s Off-Premise Hybrid Cloud Platform (Microsoft Azure).”

As per BPQR 1.1 (a) and 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).” With regards to PKI in Version 1, 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).”

Question No. [05]: *Clarification 7 Aug 2*

3, Appendix II Ref: Section 3 Clauses 4.2.2.2, 4.2.3.4.1, 4.2.3.4.2 and 4.2.3.7.3; Appendix II; Figures 1 and 2 eID Card interface and the role of the JavaCard applet

Clause 4.2.2.2 states that "the JavaCard applet on the eID Card" manages the card session, and that "The awarded bidder is to create the interface between the Wallet Instance and the eID Card". Figures 1 and 2, however, show a component labelled "WSCA: JavaCard applet" positioned on the Wallet Unit side of the diagram, and the NFC link is drawn between the "QSCD eID card" and that component. Could the Contracting Authority please confirm:

a) That the JavaCard applet is resident on the eID Card and is provided by the Government of Malta, and that the component to be developed by the Awarded Bidder is the phone-side NFC/PACE interface within the Wallet Unit;

b) Whether the applet is intended to be treated as a WSCA within the meaning of Clause 4.2.3.4.2, given that Clause 4.2.3.4.1 identifies only the RWSCD and the TEE/SE as WSCDs, and that the eID Card is described as a QSCD; and

c) Whether the eID Card interface is required to serve both the qualified signature path (Clause 4.2.3.7.3) and the LoA High authentication path used for PID issuance (Clause 4.2.2.2), or whether these are to be implemented as separate components.

Answer No. [05]:

- a) The JavaCard applet resides on the Maltese eID card. As per BPQR Criterion 2.6(a) the bidder shall describe how the “Wallet Unit shall Integrate with the eID Card to enable secure communication via PACE protocol over NFC on Android and iOS”.
- b) The eID Card is a QSCD and not intended to be treated as a WSCA. The references to WSCDs in Section 3, Clause 4.2.3.4.1 remain applicable. The diagram is intended to illustrate component interactions and does not alter the classification of the eID Card. As per Section 3, Clause 4.2.2 “The RWSCD shall utilise one or more Hardware Security Modules (HSM) to securely manage and protect cryptographic keys, including the PID secret key.”
- c) The eID Card interface shall support both the LoA High authentication path used for PID issuance and the qualified signature functionality required by the solution.

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.” As per Section 3 Clause 4.2.3.7.3 “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.”.

Question No. [06]: *Clarification 7Aug 3*

3 Ref: Figures 1 and 2; Section 3 Clause 4.2.3 Components appearing only in Figures 1 and 2

The following components appear in Figures 1 and 2 but are not named anywhere in the text of the Tender Document: "RWSCD Client", "Presentation Component", "Storage area" and "Attestation Verifier Component". Could the Contracting Authority please confirm, for each of them, whether it constitutes a required deliverable, which clause of the Terms of Reference establishes the requirement, and — in the case of the "Attestation Verifier Component" — how it relates to the verification-related components named in the text (the Verification Engine, the RP verifier component and the WUA verifier component)?

Answer No. [06]: The following are all part of the Wallet Instance and shall be provided by the Awarded Bidder.

RWSCD Client - the component that will be communicating with the RWSCD.

Storage area - will be used to store “sensitive data stored on the mobile device and “shall be strongly encrypted and isolated from other applications” as per Section 3, Article 4.2.1.3.7.10.

Presentation Component – responsible for presentation of attributes as per Section 3, Article 4.2.3.5.

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. The ‘Attestation Verifier Component’ is a standalone component external to both the Wallet Instance and the PID provider, and as per Section 3 Clause 4.2.1.3.6 “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.”

Question No. [07]: *Clarification 7Aug 4*

3 Ref: Section 3 Clauses 4.2.3.7.1, 4.2.3.7.2 and 4.2.3.10.5 Qualified time-stamping for PAdES long-term validity

Clause 4.2.3.7.1 requires that users be able to create qualified electronic signatures in PAdES format as specified by ETSI EN 319 142-1 v1.2.1, and Clause 4.2.3.7.2 requires the Signature Creation Application to comply with ETSI TS 119 431-2 v1.2.1 and ETSI EN 319 102-1.

ETSI EN 319 142-1 defines several conformance levels — PAdES-B-B, B-T, B-LT and B-LTA — which differ in whether a signature time-stamp, validation material or archival time-stamps are incorporated. The Tender Document specifies the format but does not specify the level.

The choice of level has material consequences for both architecture and cost: any level above B-B requires electronic time-stamps, yet the Tender Document does not identify a time-stamping authority, and time-stamping certificates are not among those to be issued by the PKI under Clause 4.2.3.10.5.

Could the Contracting Authority please clarify:

a) Which PAdES conformance level the Solution is required to produce as a minimum — B-B, B-T, B-LT or B-LTA;

b) If a level above B-B is required, whether a qualified electronic time-stamping service is to be provided by the Contractor as part of the Solution, or whether an existing Government of Malta or third-party qualified TSA is to be used; and

c) If an existing service is to be used, which service, and whether access and any associated subscription or per-transaction costs are to be borne by the Contracting Authority or by the Contractor.

Answer No. [07]:

a) As per Section 3, Article 4.2.3.7.1 and 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.” Therefore, Version 2 will be launched with, at minimum, PAdES conformance level B-B. The inclusion of further conformance levels will be subject to Contract Modification as specified in Section 2, Article 20.6.

b) Refer to answer (a) above.

c) Refer to answer (a) above.

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

Department of Contracts