



[18/09/2026]

[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 # [22]

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]: *A — Award criteria, scoring and elimination*

Ref	Document	Section / clause	Page
QA_033	4_CT2274_2026 - Tender document - Digital Identity Wallet; 1_c4t_13926846_1.xml (award criteria file published in the ePPS workspace)	Section 1 – Instructions to Tenderers, Clause 6.2; and the thresholds recorded in the ePPS award criteria file against the marking sub-criteria of criteria 1.6 and 1.7	8 (Clause 6.2); the ePPS file is unpaginated

"Clause 6.2 provides that ""If thresholds are set for each/any of the criteria/sub-criteria by setting a value out of 100, those offers that do not obtain the set threshold for the individual criterion/sub-criterion will be eliminated."" No threshold value appears against any criterion in the BPQR Criteria table.

The award criteria file published in the ePPS workspace does record thresholds. Among them: 34 against the markings for criteria 1.6 c), 1.6 d) and 1.6 j), each of which carries one mandatory mark and two add-on marks; 67 against the markings for criterion 1.6 l), which carries two mandatory marks and one add-on mark; 25 against criterion 1.6 e); 33 against the markings for criterion 2.2 d); and 20, 34 or 50 against the markings for each Key Expert.

On several of these, a tenderer that satisfies the mandatory requirement but offers no add-on would obtain a proportion of the marks below the threshold recorded — one mark of three is 33 per cent, against a threshold of 34.

The Contracting Authority is requested to confirm:

(a) the threshold applicable to each criterion and sub-criterion, and that these values are published to tenderers;

- (b) how the score out of 100 is computed for a criterion scored as a list of options, and in particular whether it is the proportion of the available marks obtained;
- (c) whether a threshold is met by attaining the stated value, or only by exceeding it;
- (d) whether, on the sub-criteria identified above, satisfying the mandatory requirement alone results in elimination; and
- (e) if so, whether the elements described as ""add-on"" are in substance required."

Answer No. [01]:

- a) The thresholds applicable in the ePPS award criteria correspond to the minimum pass mark set as a percentage to the respective criterion/sub-criterion of the BPQR table in the tender document. Where necessary, for mandatory criteria only, the percentage equivalent on ePPS set as threshold has been rounded upwards to the next whole percentage point. The set threshold is the minimum score evaluators can award if the bidder satisfies the mandatory criteria. For example, under criterion 1.6(c), one (1) mark represents the mandatory requirement out of a maximum three (3) marks. This corresponds to 33.33% and is represented in ePPS as 34%. A bidder satisfying the only mandatory requirement will therefore be awarded 34%.
- b) Each criterion/sub-criterion in the BPQR table contains a defined number of marks and the percentage reflected in ePPS represents the corresponding proportion of the awarded marks.
- c) A threshold is met by attaining the stated value.
- d) and e) The BPQR table has 48 marks out of 200 (i.e 24%) as add-on criterion. Criteria 6.2 of the ITT states that "Tenderers must achieve an average technical score of 60%." Criterion identified as "add-on" are not mandatory requirements and failure to satisfy an add-on requirement will not, in itself, result in elimination. Add-on requirements serve to award additional marks for additional quality. As such if a bidder does not offer any add-ons but satisfies fully all mandatory criteria will score more than 60% overall.

Question No. [02]: *A — Award criteria, scoring and elimination*

QA_034	1_c4t_13926846_1.xml (award criteria file published in the ePPS workspace); Technical Offer and Organisation & Methodology	ePPS award criteria file, technical envelope — the sections "BPQR Criteria" and "Technical Questionnaire"	the ePPS file is unpaginated
---------------	--	---	------------------------------

"The technical envelope of the award criteria file published in the ePPS workspace contains two top-level sections. ""BPQR Criteria"" carries a weight of 100 and a threshold of 60. ""Technical Questionnaire"" carries a weight of 0 and a threshold of 100.

The Contracting Authority is requested to confirm:

- (a) whether the Technical Questionnaire carries any weight in the technical score, or is an eligibility check assessed on a pass or fail basis;
- (b) the consequence of a negative answer against any line of the Technical Questionnaire in the Technical Offer and Organisation & Methodology document, and in particular whether it results in the elimination of the offer; and
- (c) whether the threshold of 100 requires every line of the questionnaire to be answered affirmatively."

Answer No. [02]:

a, b & c) The Technical Questionnaire carries no weight in the BPQR technical score. It constitutes a technical compliance requirement and is assessed on a pass/fail basis. The threshold of 100 in the ePPS Technical Questionnaire reflects the requirement for the bidder to satisfy all applicable mandatory requirements contained therein. A bidder will be awarded either 100 or 0 for the technical questionnaire. The questionnaire must be duly completed. A negative response or a response demonstrating that the proposed solution does not comply with a mandatory requirement of the tender, shall result in the offer being considered technically non-compliant.

Question No. [03]: *A — Award criteria, scoring and elimination*

QA_002	4_CT2274_2026 - Tender document - Digital Identity Wallet	Section 1 – Instructions to Tenderers, Clause 6.2	8 and 9
---------------	--	---	---------

"Clause 6.2 provides, at page 8, that ""When evaluating technical offers, each evaluator awards for each criterion/sub-criterion a score out of a maximum of 100 in accordance with the technical criteria and any sub-criteria as outlined in the evaluation grid.""

It further provides, at page 8, that ""If thresholds are set for each/any of the criteria/sub-criteria by setting a value out of 100, those offers that do not obtain the set threshold for the individual criterion/sub-criterion will be eliminated.""

It provides, at page 9, that ""Tenderers must achieve an average technical score of 60%. The average technical score is arrived at by adding the individual weighted scores of each evaluator divided by the number of evaluators. Those tenderers that do not obtain the minimum set average technical score will be eliminated.""

The Contracting Authority is requested to clarify:

(a) how the average technical score is calculated — whether it is the number of marks multiplied by the marks on ePPS, expressed as a percentage, for each requirement; and

(b) whether ""evaluator"" means an individual person, or the group of persons who will carry out the evaluation."

Answer No. [03]:

a) Each evaluator shall independently award the applicable score for each criterion/sub-criterion in accordance with the published BPQR evaluation grid. The marks attributable to all criteria/sub-criteria are then aggregated to obtain that evaluator's total technical score out of the maximum 200 marks. The Average Technical Score is then calculated by adding the individual technical percentage scores awarded by all evaluators and dividing the result by the number of evaluators.

b) Evaluator means an individual person.

Question No. [04]: A — Award criteria, scoring and elimination

QA_006	4_CT2274_2026 - Tender document - Digital Identity Wallet	Section 1 – Instructions to Tenderers, Clause 6 Criteria for Award — the "Marks" and "Marks on ePPS" columns of the BPQR Criteria table	9 (BPQR Criteria); 10 to 22 (criteria table)
--------	--	---	---

"The BPQR Criteria table at pages 10 to 22 carries a column headed ""Marks"" and a column headed ""Marks on ePPS"". The heading ""BPQR Criteria"" at page 9 refers to marks, and it is not clear whether the reference is to ""Marks"" or to ""Marks on ePPS"".

The Contracting Authority is requested to clarify the difference between the ""Marks"" column and the ""Marks on ePPS"" column."

Answer No. [04]: The “Marks” column is the number of marks set for each criteria. The Column “Marks on ePPS” is the given marks set as a percentage.

Question No. [05]: A — Award criteria, scoring and elimination

QA_007	4_CT2274_2026 - Tender document - Digital Identity Wallet	Section 1 – Instructions to Tenderers, Clause 6 Criteria for Award, description at the head of the BPQR Criteria table	10
--------	--	--	----

"The description in the first row of the criteria table at page 10 provides that where the contents of the documentation ""exceed all minimum requirements, thus offering a higher quality bid, higher points will be allotted (up to the maximum score)"".

The Contracting Authority is requested to clarify:

- (a) the relation between points and marks, and how the final technical score is calculated; and
(b) to provide a worked example of such a calculation."*

Answer No. [05]: Points refers to the score awarded in respect of the relevant BPQR criterion/sub-criterion in percentage, whilst “Marks” refers to the weighting allocated to that criterion/sub-criterion within the overall maximum technical score of 200 marks.

Where a sub-criterion carries a maximum of three (3) marks consisting of one (1) mandatory mark and two (2) separate add-on marks:

- compliance with the mandatory requirement only = $1/3$ marks = 33.333...%;
- compliance with the mandatory requirement and one add-on = $2/3$ marks = 66.666...%;
- compliance with the mandatory requirement and both add-ons = $3/3$ marks = 100%.

Please refer to clause 6.2 of the ITT section which states how the final technical score is calculated including formulas used.

Question No. [06]: A — Award criteria, scoring and elimination

QA_005	4_CT2274_2026 - Tender document - Digital Identity Wallet	Section 1 – Instructions to Tenderers, 5. Selection and Award Requirements, paragraph (b) Economic and Financial Standing, under the heading "Average yearly turnover"	6
--------	--	---	---

"Paragraph (b) Economic and Financial Standing provides that ""The bidder must provide a signed declaration by a warranted Auditor appointed by the economic operator, which confirms the

minimum average yearly turnover during the past three (3) financial years shall be not less than €2,500,000 - per year"".

A declaration by a warranted Auditor is required a second time under paragraph (c) Technical and Professional Ability, at the same page, in respect of the cumulative value of projects.

The Contracting Authority is requested to clarify the meaning of the term ""warranted Auditor"".

Answer No. [06]: For the purposes of this requirement, a “warranted Auditor” means a person who is legally authorised and duly registered to practise as an auditor in the jurisdiction in which that person is established. In the case of an auditor established in Malta, this shall mean a person holding a valid Practising Certificate in Auditing in accordance with the Accountancy Profession Act (Chapter 281 of the Laws of Malta). For auditors established outside Malta, the auditor shall possess an equivalent authorisation, registration or professional entitlement issued or recognised by the competent authority in the auditor's country of establishment.

Question No. [07]: *A — Award criteria, scoring and elimination*

QA_023	Key Experts Form (Declaration of Availability); 4_CT2274_2026 - Tender document - Digital Identity Wallet	Key Experts Form, Declaration of Availability, final paragraph; Section 1 – Instructions to Tenderers, Clause 6 Criteria for Award, BPQR Criteria table, Part 1 "Solution, Legal, and Operational Domains", criterion 1.7 "Key Experts"	the Key Experts Form is unpaginated; criterion 1.7 is at page 15
---------------	---	---	--

"The Tender Documents require each proposed Key Expert to sign a Declaration of Availability which includes the following statement:

""Furthermore, should this tenderer be successful, I am fully aware that if I am not available at the expected start date of my services for reasons other than ill-health or force majeure, I may be subject to exclusion from other tender procedures and contracts and that the notification of award of contract to the tenderer may be rendered null and void.""

That paragraph requires an individual employee to make a commitment which may have direct contractual consequences for the Tenderer, including cancellation of the award. Employees are generally not authorised to make commitments or assume liabilities on behalf of their employer, which is the legal entity participating in the procedure. Under French labour law (Code du travail), an employee generally cannot bind the employer, and commitments capable of binding the employer or affecting its contractual rights may be undertaken only by its duly authorised representatives.

Furthermore, after submission of the tender, the Tenderer cannot control circumstances affecting the continued employment of individual experts, such as resignation, retirement or recruitment by third parties. The Tenderer would therefore be exposed to a disproportionate risk of losing the award through events beyond its reasonable control.

The Contracting Authority is requested to confirm whether the final paragraph of the Declaration may instead be signed by a duly authorised representative of the Tenderer, who can validly commit

the company, while the proposed Key Expert signs only the declaration relating to his or her availability and willingness to participate in the project."

Answer No. [07]: The Statement of Availability is to be completed and signed personally by the individual Key Expert concerned. The form expressly states that it is “to be completed by each individual key expert if required” and requires the name and signature of the Key Expert.

The final paragraph of the Statement of Availability, including the declaration concerning the repercussions of non-availability for reasons other than ill-health or force majeure, forms part of the declaration to be acknowledged and signed by the individual Key Expert and may not instead be signed by an authorised representative of the Tenderer.

The statement constitutes a personal declaration by the proposed Key Expert concerning his/her availability and awareness of the conditions associated with such availability. It does not constitute a declaration made by the Key Expert on behalf of, or with authority to legally bind, the bidder/tenderer.

Furthermore, as per Section 2, Article 17: ‘Replacement of Personnel and Trainees’, a Key Expert may be replaced throughout the performance of this contract due to legitimate sickness and/or other extenuating circumstances, including also the non-performance of such individuals as decided upon by the Contracting Authority, the Contractor is obliged to provide the Contracting Authority with a detailed profile of the individual to replace the original Key Expert for approval prior to being entrusted with any tasks related to this contract. Any replacement is to meet the tender requirements.

Question No. [08]: *B — Intellectual property and contract*

QA_024	4_CT2274_2026 - Tender document - Digital Identity Wallet	Section 2 – Special Conditions, Article 14: Intellectual and Industrial Property Rights, Clause 14.5 (a) and Clause 14.7 (Ownership Matrix); Article 1: Definition and Conventions, Clause 1.3	28 (Clause 14.5 (a)); 29 (Clause 14.7); 23 (Clause 1.3)
---------------	--	---	--

"Clause 14.5 (a) requires the delivery of "Full source code for all Bespoke Deliverables including configuration files, infrastructure-as-code definitions, and automated test suites if applicable". The Ownership Matrix at Clause 14.7 records "Full title assignment guarantee; source code delivery at every release" against the Full Ownership category only. Clause 1.3 provides that "Bespoke Deliverables do not include Third-Party Components or Vendor-Retained Components".

The Contracting Authority is requested to confirm that the obligation to deliver source code under Clause 14.5 (a) and under the Ownership Matrix extends solely to Bespoke Deliverables and to the components recorded in the Full Ownership row, and that no delivery of source code is required in respect of Third-Party Components or Vendor-Retained Components."

Answer No. [08]: 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. The submitted bid, specifically BPQR Criteria 2.8 (a) and (b), will define the ownership of Version 1 and the SCA respectively.

Question No. [09]: *B — Intellectual property and contract*

QA_025	4_CT2274_2026 - Tender document - Digital Identity Wallet	Section 2 – Special Conditions, Article 14, Clauses 14.5, 14.6 and 14.7; Article 45: Operational Continuity, Clause 45.1	29 (Clauses 14.5, 14.6, 14.7); 45 (Clause 45.1)
---------------	--	--	---

"Clause 14.6 provides that ""Third-Party Components shall be licensed under terms permitting the Contracting Authority to use, modify, deploy, and sublicense without restriction."" The Ownership Matrix at Clause 14.7 addresses only ""Licences for third-party open-source dependencies"" and records no entry for third-party components licensed on commercial terms. Clause 14.5 further provides that ""The Contractor shall not introduce proprietary dependencies without prior written approval of the Contracting Authority.""

Components licensed on commercial terms — including hardware security module firmware, certified cryptographic libraries and vendor software development kits — are not, as a matter of market practice, available on terms permitting modification and unrestricted sublicensing. A requirement to obtain such terms would exclude the certified components on which a compliant Wallet Solution depends.

The Contracting Authority is requested to confirm:

(a) the regime applicable to third-party components licensed on commercial terms;
(b) whether the requirement at Clause 14.6 is intended to apply to such components; and
(c) whether deposit of such components with the approved escrow agent under Clause 45.1, together with a licence permitting use and deployment for the purposes of the Contract, satisfies the Contracting Authority's requirements."

Answer No. [09]: (a) & (b) Components licensed on commercial terms, subject to the Contracting Authority's prior written approval pursuant to Section 2, Article 14.6, shall be regulated in terms of the provisions of Section 2, Article 14.7, specifically "The Contractor is to obtain and continue to maintain on behalf of the Contracting Authority all necessary approvals, consents, licences and permissions (legal, statutory, regulatory, contractual or otherwise) for third-party licences necessary for the operation, maintenance, monitoring and support of Version 1 and Version 2. This includes, but is not limited to, Operating Systems for the on-premises hardware and containers, security and monitoring solutions, backup solutions. The Contractor is to provide proof of purchase and licences to the Contracting Authority on an annual basis and on request by the Contracting Authority."

With regards to part (c), the Economic Operator is kindly referred to Section 2, Article 1.3 (3) which defines 'Escrow Materials' to include, where applicable, Version 1 and the SCA component including any documentation, policies, lifecycle management, runtime policy engine, infrastructure-as-code (IaC) definitions and configurations as applicable. The bidder's answers to BPQR Criterion 2.8 (a) and (b) will, amongst others, determine the applicability of escrow requirement for Version 1 and the SCA component respectively.

Question No. [10]: *B — Intellectual property and contract*

QA_026	4_CT2274_2026 - Tender document - Digital Identity Wallet	Section 2 – Special Conditions, Article 45: Operational Continuity, Clause 45.1; Article 1, Clause 1.3; Article 14, Clause 14.6; Section 1 – Instructions to Tenderers, Clause 6 Criteria for Award, BPQR Criteria table, Part 2 "Components for Version 2", criterion 2.8 "Intellectual Property", items (a) and (b)	45 (Clause 45.1); 23 (Clause 1.3); 29 (Clause 14.6); 22 (criterion 2.8)
---------------	--	---	--

"Clause 45.1 provides that ""Unless full ownership of the Escrow Materials is granted to the Contracting Authority, the Contractor shall deposit the Escrow Materials with an approved escrow agent"". Clause 1.3 defines Escrow Materials as including Version 1 and the SCA component, and defines Bespoke Deliverables as including ""the wallet core and all components of Version 1 and Version 2"". Clause 14.6 assigns all intellectual property rights in Bespoke Deliverables to the Contracting Authority.

Read together, full ownership of Version 1 is granted in every case, and the escrow obligation at Clause 45.1 cannot be triggered. Criterion 2.8 nevertheless invites tenderers to describe the title in intellectual property for Version 1 and for the SCA Component, ""confirming full ownership"", as add-on criteria — which presupposes that a tenderer might not confirm it.

The Contracting Authority is requested to clarify how Clause 45.1 is intended to operate in respect of Version 1 and the SCA Component; whether the escrow route remains available where a tenderer proposes to deliver these components on the basis of pre-existing proprietary materials rather than by full assignment; and whether a tenderer taking that route forgoes only the add-on marks under criterion 2.8, or is treated as non-compliant."

Answer No. [10]: In relation to the title in respect of Version 1 and the SCA Component, Escrow requirements apply where full ownership is not granted to the Contracting Authority, as per BPQR Criteria 2.8 (a) and (b) respectively and without prejudice to Section 2, Article 1.3 (1) and Section 2, Article 14.6. In all other cases, title in IP is to be regulated as per Section 2, Article 14.7.

Question No. [11]: *B — Intellectual property and contract*

QA_027	4_CT2274_2026 - Tender document - Digital Identity Wallet	Section 2 – Special Conditions, Article 1, Clause 1.3 (definition of Bespoke Deliverables); Article 14, Clause 14.6	23 (Clause 1.3); 29 (Clause 14.6)
---------------	--	---	--------------------------------------

"Clause 1.3 defines Bespoke Deliverables as materials ""(a) created, developed, or produced by or on behalf of the Contractor specifically for the purposes of this Contract; or"" ""(b) created through material adaptation of pre-existing materials where the resulting output is tailored to this Contract and the Solution."" The same clause provides that ""Materials produced using resources paid for under this Contract are presumed to be Bespoke Deliverables unless the Contractor establishes that they were produced entirely from pre-existing materials without material adaptation.""

The Contracting Authority is requested to clarify the boundary of ""material adaptation"" for the purposes of this definition, and in particular to confirm the treatment of a pre-existing wallet platform owned by the Contractor which is configured, integrated or parameterised for the purposes of this Contract without modification of its underlying proprietary code base — specifically, whether

such a platform remains the property of the Contractor and falls outside the assignment at Clause 14.6. The Contracting Authority is further requested to indicate what evidence it expects in order for the Contractor to discharge the presumption."

Answer No. [11]: Material adaptation is considered to be any change which has the effect of tailoring existing material to this Contract and the Solution, without prejudice to the requirements of the Ownership Matrix contained within Section 2, Article 14.7. The Contracting Authority accepts any evidence, provided that such evidence sufficiently proves, in the opinion of the Contracting Authority, that the materials in question are not Bespoke Deliverables.

Question No. [12]: *B — Intellectual property and contract*

QA_009	4_CT2274_2026 - Tender document - Digital Identity Wallet	Section 3 – Specifications / Terms of Reference, 4. Scope of the Work, Clause 4.2.1.3.6 "Support for uptake"	60
---------------	--	--	----

"Clause 4.2.1.3.6 provides that ""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 Contracting Authority is requested to clarify:

- (a) the requirements applicable to this Verification Engine — technical, functional and non-functional; and*
- (b) the conditions under which the Verification Engine is to be provided to Relying Parties."*

Answer No. [12]:

a) As per Section 3, Clause 4.2.3.4.3 “The RP verifier component shall be provided by the awarded bidder. It shall be able to verify the authenticity of a RP before presenting them with attributes. It shall be a part of the Wallet Unit.”

b) As per Section 3, Clause 4.2.1.3.6 the Verification Engine “will be made available to Relying Parties that are Public Bodies” as needed by the Contracting Authority.

Question No. [13]: *B — Intellectual property and contract*

QA_028	4_CT2274_2026 - Tender document - Digital Identity Wallet	Section 3 – Specifications / Terms of Reference, 4. Scope of the Work, Clause 4.2.1.3.6 "Support for uptake"; and Clause 4.2.3.4.3 "RP verifier component" and Clause 4.2.3.10.1 "WUA verifier component"	60 (Clause 4.2.1.3.6); 73 (Clause 4.2.3.4.3); 75 (Clause 4.2.3.10.1)
---------------	--	---	---

"Clause 4.2.1.3.6 requires the awarded bidder to deliver a Verification Engine ""including its complete source code, which will be made available to Relying Parties that are Public Bodies"".

The Terms of Reference separately specify an "RP verifier component", of which Clause 4.2.3.4.3 provides that "The RP verifier component shall be provided by the awarded bidder. It shall be able to verify the authenticity of a RP before presenting them with attributes. It shall be a part of the Wallet Unit.", and a "WUA verifier component", of which Clause 4.2.3.10.1 provides that it "shall be provided by the awarded bidder" and "will be used by the PID Provider".

The Contracting Authority is requested to confirm:

- (a) the relationship between the Verification Engine and these components — whether it is one of them, comprises both, or is a distinct deliverable;*
- (b) the licence terms under which the source code is to be made available to Relying Parties that are Public Bodies;*
- (c) whether those Relying Parties may modify the source code or redistribute it to any third party;*
- (d) whether the Contractor is required to provide warranty, maintenance or support in respect of any version so modified or redistributed; and*
- (e) where the Verification Engine is or includes the RP verifier component, whether delivery of its complete source code entails delivery of source code forming part of the Wallet Unit."*

Answer No. [13]:

a) 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.”

b) The ‘Attestation Verifier Component’ 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.

c) See (b) above

d) No, support and maintenance only apply for the version provided to the CA.

e) See (a) above

Question No. [14]: *B — Intellectual property and contract*

QA_008	4_CT2274_2026 - Tender document - Digital Identity Wallet	Section 2 – Special Conditions, Article 14: Intellectual and Industrial Property Rights, Clause 14.3; and Article 42: Confidentiality of Data, Clause 42.1	28 (Clause 14.3); 41 (Clause 42.1)
---------------	--	---	---------------------------------------

"Clause 14.3, at page 28, provides that ""The Contractor shall not have the right to use any data, reports, works or other property owned by the Contracting Authority for its own purposes without obtaining the prior written consent of the Contracting Authority"".

Clause 42.1, at page 41, provides that ""The Contractor will not (and will ensure that its subcontractors and employees do not) store, copy or use data which is not in the public domain (other than as a result of a breach by the Contractor of its other obligations under the Contract) or was properly in the possession of the Contractor prior to receiving the data from the Contracting Authority for any purpose other than to the extent necessary to perform its obligations under the Contract.""

The Contracting Authority is requested to clarify the contradiction between these two provisions."

Answer No. [14]: Section 2, Articles 14.3 and 42.1 operate cumulatively. Article 42.1 regulates the Contractor's handling of data and information, limiting its storage, copying and use to what is necessary for the performance of the Contract. Article 14.3 applies to "any data, reports, works or other property owned by the Contracting Authority". It prohibits the Contractor from using such property for its own purposes unless the Contracting Authority has provided prior written consent. Accordingly, the Contractor may use Contracting Authority data, reports, works and other property to the extent necessary to perform its contractual obligations. Any use beyond the performance of the Contract, including use for the Contractor's own purposes, requires the prior written consent of the Contracting Authority.

Question No. [15]: *B — Intellectual property and contract*

QA_017	4_CT2274_2026 - Tender document - Digital Identity Wallet	Section 2 – Special Conditions, Article 18: Execution of the Contract, Clause 18.2 and its milestone table	30 (Clause 18.2); 32 (milestone table)
---------------	---	--	---

"The milestone table at Clause 18.2 records ""21 months from signing of the contract"" against the build milestones, and records ""90 months (duration of the contract)"" against ""Hosting, Operations, SLA, Maintenance, Training, Review of Regulatory and Standards Updates and Support.""

The Contracting Authority is requested to clarify whether the 90 months of contract duration include the 21 months of Build."

Answer No. [15]: Yes, confirmed that the 21 months are part of the 90 months of contract duration.

Question No. [16]: *C — Security and regulatory scope*

QA_022	Schedule 3 – Security Requirements; 4_CT2274_2026 - Tender document - Digital Identity Wallet	Schedule 3, 01. Definitions and 03. Security Requirements (sub-sections 03.1 to 03.33); 4_CT2274_2026 - Tender document - Digital Identity Wallet: Section 2 – Special Conditions, Article 26, Clause 26.1; Section 3 – Specifications / Terms of Reference, Appendix III; Section 1 –	Schedule 3 pages 1 to 14; tender document page 37 (Clause 26.1), page 90 (Appendix III),
---------------	---	--	--

		Instructions to Tenderers, 5. Selection and Award Requirements, paragraph (d)	page 7 (ISO/IEC 27001)
--	--	---	------------------------

"Schedule 3 allocates its sub-sections by a single sentence at 03. Security Requirements: ""The Contractor shall have the following responsibilities.""

The thirty-three sub-sections are of materially different natures. Some govern the logical security of the Solution and are within the Contractor's control: 03.16 Access Control, 03.17 Account Management, 03.24 Control of technical vulnerabilities, 03.26 Hardening, 03.27 Audit Logging, 03.32 Correct Processing in Software Applications. Others govern the physical and environmental security of premises and media (03.9), the information security management system of the Contractor's own organisation (03.2, 03.4, 03.5, 03.7, 03.8), controls specific to virtualised cloud infrastructure (03.30), and controls addressed to users of the Government's internal environment (03.19 Clear-desk and clear screen, 03.20 Connecting to MAGNET, 03.21 Teleworking).

Appendix III provides, at page 90, 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"". Physical and environmental control of the hosting facilities therefore rests with the cloud service provider and with MITA respectively, and not with the Contractor.

Schedule 3 contains one express limitation of the Contractor's obligations: ""In case of Supply of Equipment and Maintenance and Support Services the obligations of the Contractor shall be limited to Customer Data residing on the Hardware that is supported and maintained by the Contractor and/or Customer Data to which the Contractor may otherwise have access to whether directly or indirectly in providing the Service.""

The Contracting Authority is requested to confirm:

(a) the applicability of each sub-section of 03 to the Contractor, separately for Version 1 and for Version 2, distinguishing requirements for which the Contractor is responsible, those for which responsibility rests with MITA or with the cloud service provider, and those which do not apply to this Contract — in the form of a responsibility matrix, or by confirming that tenderers may propose one for approval;

(b) whether the limitation quoted above applies to this Contract;

(c) that where a requirement is not applicable to the Contractor by reason of the hosting model, a tenderer may state that requirement to be out of scope with a reasoned justification, without being treated as non-compliant in the evaluation;

(d) that requirements addressed to the Contractor's own organisation may be evidenced at organisational level, for example through the ISO/IEC 27001 certification required at Section 1, Clause 5, paragraph (d), page 7; and

(e) that compliance in respect of Version 2 is to be assessed against the architecture proposed and accepted at design stage, and at which milestone the compliance report is due.

The Contracting Authority's attention is also drawn to Clause 26.1, at page 37 of the tender document, which refers to "the hosting responsibilities detailed in Schedule 3 (Hosting Environment)", whereas Schedule 3 is the Security Requirements Schedule and the Hosting Schedule is Schedule 1."

Answer No. [16]: (a) Schedule 3 provides that “The Contractor shall have the following responsibilities” and further requires the Contractor to be responsible for the security of the Solution or Service. The obligations listed in Schedule 3 are typical ISMS controls that are irrespective of where the Solution is hosted. These go beyond the location of the Solution but also cover other elements such as the offices used by the Awarded Bidder from which it accesses remotely the solution. During the execution of the contract the Awarded Bidder may be expected to attain and maintain ISO/IEC 27001 as per Section 2, Article 7.3 that states “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 throughout the contract duration, evidence of which shall be provided to the Contracting Authority when requested.” Additionally, attaining and maintaining ISO/IEC 27001 certification may be influenced by National and EU legislation as per Section 3, Clause 4.3.4.

(b) The contract is not for Supply of Equipment and Maintenance and Support Services for said equipment only, but goes beyond that including the design, development, maintenance, operation and support of both versions of the Solution.

(c) Refer to answer (a) above.

(d) Section 1, Clause 5 (B) (d) which states that “The economic operator, as well as any subcontractors involved in the processing of data or delivery of security relevant components, must be certified against ISO/IEC 27001. Evidence of valid certification shall be provided as part of the bid submission” is in relation to documentation that is to be evidenced as part of the bidding process. This is without prejudice to the requirements stipulated in the CfT and as explained in (a) above.

(e) Compliance requirements have been stipulated in various sections of the CfT, for example but not limited to Section 3, Clause 4.3.4 ‘Mandatory EU Cybersecurity Compliance’. The Awarded Bidder is expected to fulfil those obligations irrespective of whether such obligations are evidenced with reporting, milestones or deliverables. Deviations from fulfilling the necessary obligations will be considered a breach of contract.

Section 2, Article 26.1 states that "The Contractor shall fulfil the hosting responsibilities detailed in Schedule 3 (Hosting Environment)." The Contracting Authority wishes to clarify that the Hosting Schedule referenced here is Schedule 1.

Question No. [17]: *C — Security and regulatory scope*

QA_035	4_CT2274_2026 - Tender document - Digital Identity Wallet; Figure 1 - High Level Diagram	Section 3 – Specifications / Terms of Reference, Appendix III; Figure 1 - High Level Diagram (Docs, Forms and Annexes)	90 (Appendix III); Figure 1 is unpaginated
--------	--	--	--

"Figure 1 assigns each component of the architecture a colour, and its legend gives each colour a meaning: ""Component to be provided by GoM""; ""Component to be provided by Wallet prov.""; ""Actor for which bidder provides the underlying solution""; ""Actor for which bidder is not involved""; and ""Component not necessarily- provided by GoM/Wallet prov.""

The Contracting Authority is requested to confirm:

- (a) whether Figure 1 is contractually binding as to the allocation of components between the Government of Malta, the Contractor and third parties, and forms part of the specification;*
- (b) which party is to provide the components coloured as not necessarily provided by the Government or the Wallet provider, in particular the Attestation Verifier Component; and*
- (c) that where Figure 1 and the text of Section 3 differ as to which party provides a component, the text prevails."*

Answer No. [17]:

- a) The High-Level Diagram in Figure 1 is part of the specification, and therefore contractually binding.
- b) 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.”
- c) “Component not necessarily- provided by GoM/Wallet prov” indicates that there may be multiple instances of this component, one of which has to be provided by the bidder (but this would not be the only possible instance of this component).

Question No. [18]: *C — Security and regulatory scope*

QA_031	4_CT2274_2026 - Tender document - Digital Identity Wallet	Section 3 – Specifications / Terms of Reference, 4. Scope of the Work, Clause 4.3.4 "Mandatory EU Cybersecurity Compliance"; and Clause 4.2.1.3.7 "Secure Development Practices"	82 (Clause 4.3.4); 62 and 63 (Clause 4.2.1.3.7)
---------------	--	--	---

"Clause 4.3.4 requires the awarded bidder to ""ensure that their suppliers of software, security solutions and products with digital elements as defined by the Cyber Resilience Act comply with these requirements and conform to the relevant security standards and requirements throughout the duration of the contract"", and refers to the Cyber Resilience Act, NIS2, the GDPR and the Data Act. Clause 4.2.1.3.7 requires protection against unauthorised modification ""in line with the Cyber Resilience Act's requirement to protect the integrity of data, commands, programs and configuration"".

These provisions address the obligations of the Contractor's suppliers and specific design measures, but do not state whether the Solution itself is to be treated as a product with digital elements within the meaning of the Cyber Resilience Act.

The Contracting Authority is requested to confirm:

- (a) whether the Solution, or any of its components, is required to be conformant with the Cyber Resilience Act as a product with digital elements, including conformity assessment and CE marking where applicable;
- (b) if so, which components are in scope and by which milestone conformity is to be demonstrated; and
- (c) the evidence of supplier conformity expected under Clause 4.3.4, and whether it is to be provided at bid stage or during contract execution."

Answer No. [18]:

a, b) Section 2, Article 4.3.4 states that "The Awarded Bidder and Wallet Solution shall be compliant with applicable cybersecurity requirements laid down in Union and national law, including but not limited to those relating to the identification of high-risk suppliers, and ensure that their suppliers of software, security solutions and products with digital elements as defined by the Cyber Resilience Act comply with these requirements and conform to the relevant security standards and requirements throughout the duration of the contract."

c) Milestone 16 in Section 2, Article 18.2, states that the Awarded Bidder shall "Support the Contracting Authority attain certification of the Solution according to national or EU scheme, whichever is applicable at the time." Further documentation as evidence of supplier conformity, include but not limited to pertinent technical documentation as per Article 31 of the Cyber Resilience Act, supporting documentation in relation to reporting obligations pursuant to Article 14 of the Cyber Resilience Act, certificate in relation to pertinent conformity assessment, certificate and supporting documentation in relation to the EUCC and national or EUDIW scheme, and other applicable supporting documentation as required by the Contracting Authority, including by the pertinent legislations as referred to in the tender document. This is expected to be provided during execution of the contract. In relation to the Cyber Resilience Act, it can also be suggested to review supporting documentation such as the FAQs on the CRA Implementation: <https://ec.europa.eu/newsroom/dae/redirection/document/122331>.

Question No. [19]: C — Security and regulatory scope

QA_032	4_CT2274_2026 - Tender document - Digital Identity Wallet	Section 1 – Instructions to Tenderers, Clause 6 Criteria for Award, BPQR Criteria table, Part 2 "Components for Version 2", criterion 2.7 "Remote Wallet Secure Cryptographic Device (mandatory)", item (a); and Section 3 – Specifications / Terms of Reference, 4. Scope of the Work, Clause 4.2.1.3.7 "Secure Development Practices"	21 (criterion 2.7 (a)); 63 (Clause 4.2.1.3.7)
--------	--	---	---

"Criterion 2.7 (a) allocates marks where the proposed RWSCD operation shall ""Meet the functional, security, privacy requirements [2 marks], and industry best practices for robust cryptographic algorithms to address emerging threats (such as quantum computing risks) [2 marks]"". Clause 4.2.1.3.7 provides that ""Any encryption algorithms must be reviewed on a biannual basis and updated in line with evolving best practices, emerging threats (such as quantum computing risks), and applicable regulations such as the CRA.""

Quantum-related requirements therefore attach to the Remote Wallet Secure Cryptographic Device and to the periodic review of algorithms. The requirement governing data in transit states only that it be protected ""using strong cipher suites"", without reference to quantum resistance.

The Contracting Authority is requested to confirm:

- (a) whether the Solution's communication flows — including transport security and the protocols used for PID issuance, presentation and signature operations — are required to be resistant to attack by a cryptographically relevant quantum computer;*
- (b) if so, whether post-quantum or hybrid key establishment is required from first release, or is to be introduced through the biannual review under Clause 4.2.1.3.7; and*
- (c) whether quantum resistance is expected for data at rest and for the long-term integrity of issued attestations, or is limited to the RWSCD as criterion 2.7 (a) suggests."*

Answer No. [19]:

- a) Section 3 Clause 4.2.2 (and relevant subclauses) does not stipulate that the Solution is resistant to attacks by a cryptographically relevant quantum computer. However, BPQR Criterion 2.7 (a) will award marks to reflect whether industry best practices for robust cryptographic algorithms to address emerging threats (such as quantum computing risks) will be included. As per Section 3, Clause 4.2.1.3.7 “encryption algorithms must be reviewed on a biannual basis and updated in line with evolving best practices, emerging threats (such as quantum computing risks), and applicable regulations such as the CRA. The awarded bidder is expected to discuss the outcomes of this review with the Contracting Authority and changes are subject to the Contracting Authority’s sign-off.”
- b) Bidders may include these requirements from first release with marking as per BPQR Criterion 2.7 (a) reflecting this. The biannual reviews as per Section 3, Clause 4.2.1.3.7 are mandatory.
- c) The requirements in Section 3, Clause 4.2.1.3.7, applies to the entire Solution, and are not limited to the RWSCD component.

Question No. [20]: *D — Service levels and operating model*

QA_029	Schedule 2 – Maintenance and Support Services	Part A, 2. Service Levels — Clause 2.4 Coverage Hours; Clause 2.1 Incident Categorisation; Clause 2.3 Availability of the Solution; Clause 2.5 Penalties	2 and 3 (Clause 2.1); 4 (Clauses 2.3 and 2.4); 5 (Clause 2.5)
---------------	---	--	---

"Clause 2.4 provides that ""The Awarded Bidder will provide the Maintenance and Support Services during Normal Working Hours, with the exception of Incidents classified as Critical that shall be serviced on a 24 by 7 basis."" Clause 2.1 provides that, for priorities other than Priority 1, the Service Levels commence and apply only during Normal Working Hours. Clause 2.3 requires a service availability of 99.95%, and Clause 2.5 attaches penalties to failures against the Service Levels.

The Contracting Authority is requested to confirm:

- (a) whether the 99.95% availability commitment is measured across the full calendar period, including hours outside Normal Working Hours;*

(b) whether a Priority 2 Incident arising outside Normal Working Hours attracts any out-of-hours response obligation, given that availability penalties may continue to accrue during that period; and

(c) whether the Contracting Authority expects the service desk to be staffed on a 24 by 7 basis, or only the escalation path for Critical Incidents."

Answer No. [20]:

a) Confirmed. The 99.95% availability commitment is measured across the full calendar period, including hours outside Normal Working Hours.

b) Schedule 2, Clause 2.1 states that "Where the Incident is classified as Priority 2 and 3, the Contracting Authority may raise the Incident at any time provided that the Service Levels shall commence and apply only during Normal Working Hours. In the event that the Solution is not restored during Normal Working Hours, the Restoration Time shall be suspended and shall continue to run on the next working day."

c) Schedule 2, Clause 2.1 'Help Desk' states that the "help desk will be available continuously during Coverage Hours or as otherwise specified." Schedule 2, Clause 2.4 'Coverage hours' states that "The Awarded Bidder will provide the Maintenance and Support Services during Normal Working Hours, with the exception of Incidents classified as Critical that shall be serviced on a 24 by 7 basis."

Question No. [21]: *D — Service levels and operating model*

QA_018	Schedule 2 – Maintenance and Support Services	Part A, 2. Service Levels, Clause 2.1 Incident Categorisation	3
---------------	---	---	---

"Clause 2.1 provides that ""Where the Incident is classified as Priority 1, then the Contracting Authority may raise the Incident during and outside Normal Working Hours"".

The Contracting Authority is requested to provide the Normal Working Hours expected for this contract."

Answer No. [21]: Normal working hours should be interpreted generally as Monday to Friday from 07:45hrs to 17:00hrs excluding Public Holidays in Malta. This is irrespective of support for Critical incidents (24x7 for maintenance support).

Question No. [22]: *D — Service levels and operating model*

QA_011	Schedule 2 – Maintenance and Support Services	Part A, 2. Service Levels, Clause 2.1 Incident Categorisation, Table 2.1	3
---------------	---	--	---

"Table 2.1 states a restoration time of 24 hours for a Low (Priority 3) Incident.

Considering eight working hours per day, the Contracting Authority is requested to confirm that this restoration time is three working days."

Answer No. [22]: Schedule 2, Clause 2.1 states that "Where the Incident is classified as Priority 2 and 3, the Contracting Authority may raise the Incident at any time provided that the Service Levels

shall commence and apply only during Normal Working Hours. In the event that the Solution is not restored during Normal Working Hours, the Restoration Time shall be suspended and shall continue to run on the next working day.”

Question No. [23]: D — Service levels and operating model

QA_012	Schedule 2 – Maintenance and Support Services	Part A, 2. Service Levels, Clause 2.1 Incident Categorisation, and Table 2.1	2 and 3
--------	---	--	---------

"Clause 2.1 provides that ""In the case where service has been restored through a Workaround, the Awarded Bidder has to Resolve the Incident within five (5) Working Days or as agreed to with the client (the ""Resolution Time"")."" It further provides that ""Penalties can be applied where the Response Time and Resolution Time has not been achieved"".

The term Resolution Time is used several times in Clause 2.1, whereas Table 2.1 uses only the term Restoration Time.

The Contracting Authority is requested to confirm that, whatever the priority, the Resolution Time is five working days after the Restoration Time, that is, after the application of a workaround."

Answer No. [23]: Restoration Time is the time within which the service or solution must be restored to operation. Schedule 2, Table 2.1 sets Restoration Times of 4 hours (Priority 1), 8 hours (Priority 2), and 24 hours (Priority 3). Resolution Time is the time within which the underlying Incident must be resolved after service has been restored through a workaround. Clause 2.1 states that "In the case where service has been restored through a Workaround, the Awarded Bidder has to Resolve the Incident within five (5) Working Days or as agreed to with the client (the 'Resolution Time')." "

Question No. [24]: D — Service levels and operating model

QA_019	Schedule 2 – Maintenance and Support Services	Part A, 2. Service Levels, Clause 2.6 Downtime	5
--------	---	--	---

"Clause 2.6 provides that ""Both Parties will agree in advance on scheduled downtime through a change management process.""

The Contracting Authority is requested to confirm that such scheduled downtime is treated as ""Available"" for the purposes of the availability calculation."

Answer No. [24]: The Solution is expected to achieve an availability level of not less than 99.95% over a period of 12 months, using the following formula:

Availability = $(1 - (\text{Unscheduled Downtime} / \text{Service Time})) \times 100$

Where “Service Time” will be the time that the Solution should be available and excludes any scheduled downtime. Approved scheduled downtime agreed in advance through the change management process and authorised by the Contracting Authority shall not be considered when calculating service availability. Such periods are excluded from the availability calculation and therefore do not constitute service unavailability for SLA measurement purposes.

Question No. [25]: *D — Service levels and operating model*

QA_020	Schedule 2 – Maintenance and Support Services; 4_CT2274_2026 - Tender document - Digital Identity Wallet	Schedule 2, Part A, 2. Service Levels, Clause 2.5 Penalties; and 4_CT2274_2026 - Tender document - Digital Identity Wallet: Section 2 – Special Conditions, Article 24: Interim and Final Progress Reports	5 (Schedule 2); 35 (Article 24)
---------------	--	--	---------------------------------

"Clause 2.5 of Schedule 2 provides that ""The awarded bidder will include all necessary detail in their monthly reports to enable the Contracting Authority to determine the service levels and availability"".

Article 24 of the tender document provides that on ""completion of Milestone 16 till end of contract: quarterly reports on the operation, maintenance and support"" are to be delivered.

The Contracting Authority is requested to clarify whether the awarded bidder is to provide monthly or quarterly reports."

Answer No. [25]: A monthly report with necessary detail to determine the Service Levels and availability the Solution achieved and calculate any applicable penalties is requested as per Schedule 2. Every Quarter, following the completion of Milestone 16, a more detailed report is requested as per Section 2, Article 24.

Question No. [26]: *D — Service levels and operating model*

QA_021	4_CT2274_2026 - Tender document - Digital Identity Wallet; Schedule 2 – Maintenance and Support Services	Section 1 – Instructions to Tenderers, Clause 6 Criteria for Award, BPQR Criteria table, Part 1 "Solution, Legal, and Operational Domains", criterion 1.3 "Hosting and Operation (mandatory)", item (a); and Schedule 2 generally	11 (criterion 1.3); 12 (item (a))
---------------	--	---	-----------------------------------

"Criterion 1.3 (a) requires the bidder to demonstrate how ""they shall deliver, operate, maintain, and support the solutions over the duration of the contract, in accordance with Section 3 Clause 4.2.3.11.8."" Operation is therefore among the obligations, whereas Schedule 2, which governs Maintenance and Support Services, sets no service level for the operation of the Solution.

The Contracting Authority is requested to clarify:

- (a) the scope of the maintenance and support services during the contract duration, given that operation is required by criterion 1.3 (a) but is not the subject of a service level in Schedule 2;*
- (b) which party is responsible for the administration of the hardware infrastructure and for software administration; and*
- (c) which party is responsible for each level of support — Level 1, Level 2 and Level 3."*

Answer No. [26]:

- a) Kindly refer to Section 3, Clause 4.2.3.11.8 outlines the scope of ‘Build, Operate, Maintain and Support’.
- b) The awarded bidder is responsible, as per Section 3, Clause 4.2.3.11.8.
- c) The awarded bidder is responsible for each level of support.

Question No. [27]: *D — Service levels and operating model*

QA_003	4_CT2274_2026 - Tender document - Digital Identity Wallet	Section 2 – Special Conditions, Article 1: Definition and Conventions, Clause 1.3 Definitions, definition 4 ("Maintenance")	23
--------	--	---	----

"Clause 1.3 defines ""Maintenance"" as ""post-acceptance work maintaining the Solution at its originally accepted standard, including routine bug fixes, security patches, and performance monitoring.""

The Contracting Authority is requested to confirm that the vendor will have remote access to the Solution — hosted in the MDIA tenant in Azure for Version 1, and through colocation within the MITA data centres for Version 2 — so that maintenance can be performed remotely."

Answer No. [27]: For Version 1, remote access to the Azure Resource Group can be granted to the contractor. For Version 2, the Contracting Authority will provision its own links with local Internet Service Providers for any required connectivity. The Awarded Bidder shall be in charge of setting up remote access.

Question No. [28]: *E — Solution design*

QA_030	4_CT2274_2026 - Tender document - Digital Identity Wallet	Section 1 – Instructions to Tenderers, Clause 6 Criteria for Award, BPQR Criteria table, Part 1 "Solution, Legal, and Operational Domains", criterion 1.1, item (d); Section 3 – Specifications / Terms of Reference, 2. Contract Objectives and Expected Results, Clause 2.1 Overall Objectives and Clause 2.2 Specific Objectives; Appendix III	11 (criterion 1.1 (d)); 51 (Clause 2.1); 52 (Clause 2.2); 90 (Appendix III)
--------	--	---	---

"Criterion 1.1 (d) requires, as a mandatory criterion, ""a plan, which includes both technical and UX aspects, for a smooth changeover from Version 1 to the EUDIW Solution (Version 2) in a way for the functionality of Version 1 to be available in Version 2 from first release"". Clause 2.2 requires ""Support in the transition from Version 1 to Version 2, providing a user-friendly experience when migrating to Version 2.""

The two versions are specified on different cryptographic and hosting architectures. Clause 2.1 provides for a Solution incorporating a ""Wallet Provider using Remote HSMs as the Wallet Secure Cryptographic Device – Version 2"", while Appendix III provides 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"".

Where these architectural differences prevent the cryptographic binding of an existing Version 1 user from being carried over, a technical migration of that user's credentials may not be feasible, and the user would be required to enrol again in Version 2.

The Contracting Authority is requested to confirm:

(a) whether requiring existing Version 1 users to re-enrol in Version 2 is acceptable;

(b) if so, whether a re-enrolment journey satisfies the "smooth changeover" requirement of criterion 1.1 (d), and how it will be assessed; and

(c) whether any target is set for the proportion of Version 1 users to be carried over, or for the period during which both versions must remain available during transition."

Answer No. [28]: a) Requiring existing Version 1 users to re-enrol in Version 2 is not prohibited. The changeover plan provided by each bidder will be marked as per BPQR Criterion 1.1 (d).

b) The "smooth changeover" requirement of BPQR Criterion 1.1 (d) will be assessed from a UX and technical points of view.

c) As per Section 3, Clause 2.2, the Awarded Bidder shall "Support in the transition from Version 1 to Version 2, providing a user-friendly experience when migrating to Version 2." As per Section 2, Article 18.2 "The Contracting Authority reserves the right to extend the contract or part thereof by up to six (6) months at no extra cost, such that the extension does not delay the completion of Milestone 16 by more than six (6) months. No extensions are possible for Milestones 1 and 3. If an extension is granted, the hosting, operation, maintenance and support related to Version 1 shall be at the same rates and terms." Version 1 will be decommissioned as part of this transition. As per Section 3, 1.1 (d) and in accordance with Section 3 Clause 4.2.1.1, "the bidder shall provide a plan, which includes both technical and UX aspects, for a smooth changeover from Version 1 to the EUDIW Solution (Version 2) in a way for the functionality of Version 1 to be available in Version 2 from first release". 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. It is expected that all users will transition to Version 2.

Question No. [29]: E — Solution design

QA_001	4_CT2274_2026 - Tender document - Digital Identity Wallet	Section 1 – Instructions to Tenderers, 1. General Provisions, Clause 1.1 (i)	3
--------	--	--	---

"Clause 1.1 (i) provides that the awarded bidder shall "design, develop, build and deploy a wallet mobile application, hereinafter referred to as Version 1, through which the users can authenticate with the eID server, store identification data downloaded following the authentication with the eID server".

Version 1 is therefore the mobile application. The Contracting Authority is requested to clarify whether, for Version 1, biometric face matching is required in order to establish that the user is the actual holder of the eID card."

Answer No. [29]: The current requirement is as specified in 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".

Question No. [30]: E — Solution design

QA_014	4_CT2274_2026 - Tender document - Digital Identity Wallet	Section 3 – Specifications / Terms of Reference, 4. Scope of the Work, Clause 4.2.1.1 (Version 1); and Appendix II, item 3 "Sample Code for Wallet Instance to eID Card Interface"	56 (Clause 4.2.1.1); 90 (Appendix II)
--------	--	--	---------------------------------------

"Clause 4.2.1.1 provides that ""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."" Appendix II provides that ""It is important to note that users may be using their eID Card electronically for the first time during the Wallet enrolment. As such, the Wallet Solution must accommodate first-time eID Card usage, including the mandatory PIN change process.""

The Contracting Authority is requested to confirm that, in order to achieve LoA High in Version 1, support for the first-time PIN change is mandatory."

Answer No. [30]: Yes, that is correct.

Question No. [31]: E — Solution design

QA_013	4_CT2274_2026 - Tender document - Digital Identity Wallet	Section 3 – Specifications / Terms of Reference, 4. Scope of the Work, Clause 4.2.1.3.1 "Separation of Environments"	58
---------------	--	--	----

"Clause 4.2.1.3.1 provides that ""The awarded bidder shall provision, configure, and maintain a dedicated staging environment that is logically and physically separate from both the development and production environments.""

The Contracting Authority is requested to confirm that the staging environment for Version 1 is also to be hosted in Azure."

Answer No. [31]: Yes, the staging environment for Version 1 backend functionality must be hosted within the MITA's Off-Premise Hybrid Cloud Platform (Microsoft Azure) as per Section 3, Clause 4.2.1.1. 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. [32]: E — Solution design

QA_004	Schedule 1 – Hosting Environment	6. Colocation, Clause 6.2 Backups. (The Azure Cloud option, which applies to Version 1, carries its own backup provision at Clause 5.6.)	Schedule 1 is unpaginated
---------------	----------------------------------	--	------------------------------

"Clause 6.2 of Schedule 1, which applies to the Colocation option, provides that ""The Contractor shall be responsible for all aspects related to backups for data on the hardware, including the Solution and its data, that needs to be backed up per the business requirements of the Solution, in line with the Recovery Time Objective (RTO) and Recovery Point Objective (RPO) of the Solution"".

The Contracting Authority is requested to clarify:

(a) whether Version 2 is required to be installed at two sites — a main site and a disaster recovery site — or at a single site with backup; and

(b) if two sites are required, whether they are to operate in active-passive or active-active mode."

Answer No. [32]: Schedule 1, Clause 6.2 relates specifically to the storage of backups and requires that the backup strategy supports the prescribed RTO and RPO objectives. It is the bidder's responsibility to propose and implement an approach that satisfies the requirements of this clause. In relation to the overall architecture, 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 dual data centre hosting, the service levels specified in the Call for Tender, and the prescribed RTO and RPO requirements.

Question No. [33]: *E — Solution design*

QA_015	4_CT2274_2026 - Tender document - Digital Identity Wallet	Section 3 – Specifications / Terms of Reference, Appendix III – Hosting and Service Level Requirements, under "Service Level Requirements"	90
---------------	--	--	----

"Appendix III provides that ""The Solution in its entirety shall support a Recovery Point Objective (RPO) of 15 minutes and a Recovery Time Objective (RTO) of 2 hours.""

The Contracting Authority is requested to confirm whether this applies to Version 1."

Answer No. [33]: Yes, this applies for both versions.

Question No. [34]: *E — Solution design*

QA_016	4_CT2274_2026 - Tender document - Digital Identity Wallet	Section 3 – Specifications / Terms of Reference, Appendix III – Hosting and Service Level Requirements, under "Volumetrics"	91
---------------	--	---	----

"Appendix III provides an estimated number of users ""starting from the launch to the public of the EUDIW Solution (Version 2) and the for the subsequent 5 years"", rising from 50,000 users in Year 1 to 400,000 in Year 5. No equivalent estimate is given for Version 1.

The Contracting Authority is requested to provide an estimated number of users for Version 1."

Answer No. [34]: 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.

Question No. [35]: *E — Solution design*

QA_010	4_CT2274_2026 - Tender document - Digital Identity Wallet	Section 1 – Instructions to Tenderers, 1. General Provisions, Clause 1.1 (iii)	3
---------------	--	---	---

"Clause 1.1 (iii) provides that ""Every three (3) years following the commissioning of Version 2 of the Solution made available to the public, a design refresh of any public facing interface of the Solution is to be undertaken"".

The Contracting Authority is requested to clarify the meaning of ""public facing interface""."

Answer No. [35]: ‘Public facing interface’ refers to any interface of the Solution that is intended for direct use by external users. This includes, but is not limited to, wallet users interacting with the mobile applications and relying parties or other authorised external stakeholders interacting with websites/portals/registers that make part of the Solution.

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

Department of Contracts