



[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 # [24]

To all prospective bidders

Reference is made to the above-captioned tender for which the deadline for submission of offers is **[05/11/2026]** at **[09:30am]**.

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

Question No. [01]: *Tender Section 3 Clause 4.2.3.11.10; Section 5.1; Clarification Note 01 Answer 02(1):*

Could the Contracting Authority kindly clarify, for Version 1 and Version 2, if any additional environment is expected besides the staging and production environments?

Answer No. [01]: The tender requirements refer to development, testing and production environments maintaining “Logical or physical separation of environments for development, testing, and production” as per Section 3, Clause 4.2.1.3.7 and require “Automated secure configuration baselines for all environments (development, testing, production)” as per Section 3, Clause 4.2.1.3.7.6. For these requirements to be achieved, a development environment must exist and be provisioned by the contractor as part of the solution delivery.

Question No. [02]: *Section 3 Clauses 4.2.3.10.1 to 4.2.3.10.6:*

Could the Contracting Authority kindly confirm whether any components or sub-components of the Solution are already existing and to be reused/integrated, or whether the awarded bidder is expected to provide them fully from scratch, particularly with respect to the Wallet Provider, PID Provider, Relying Party Registrar, PKI, SCA, RWSCD, verifier components, and attestation issuer?

Answer No. [02]: Section 3 Clauses 4.2.3.10.1 to 4.2.3.10.6 of the call for tender define all the dependencies on external components that are outside of scope of this call for tender such as the eID server and eID cards.

Question No. [03]: *Section 3 Clause 4.2.3.10.6:*

Could the Contracting Authority kindly confirm whether the Relying Party Registrar is intended as a completely new national capability, or whether an existing register, register-of-registers component, or related national capability is to be reused, migrated or enhanced?

Answer No. [03]: There is currently no existing national Relying Party Register (RPR), the RPR would be a completely new national capability. The RPR will be required to integrate (where applicable) with existing national systems as follows:

- (i) the national eID/authentication service - for the authentication and identification of users accessing the RPR.
- (ii) MBR's BAROS / Company Register - as an authoritative source for the validation of information relating to Maltese registered legal entities including the entity's registered name, registration number, status and other relevant registration information required as part of the Wallet-Relying Party registration process.

The integration with the Company Register is intended to support the verification requirements under CIR 2025/848, including the verification, where possible through automated means, of information submitted by Wallet-Relying Parties against authentic sources or official electronic records.

Question No. [04]: *Section 3 Clause 4.2.3.10.5; architecture figures:*

Could the Contracting Authority kindly confirm the exact PKI boundary, including whether any National Root CA, trust anchors, or external trust services are customer-furnished / pre-existing, and which parts of the PKI stack are fully in bidder scope?

Answer No. [04]: Figure 1 in the technical specifications of this Call for Tenders shows that the setting up of a new Root CA is not within the scope of this CFT. Otherwise, the Awarded Bidder is to provide, maintain, operate and support all the necessary Trust Services, the entire PKI stack and supporting documentation as listed in Section 3, Clause 4.2.3.10.5 to fulfil the requirements stipulated in the Cft.

Question No. [05]: *Section 3 Clause 4.2.3.11.1; Financial Bid Item 13:*

Could the Contracting Authority kindly confirm who is expected to bear the cost of external certification bodies, conformity assessment laboratories, interoperability testing facilities, or third-party assurance services required to support certification of the Solution?

Answer No. [05]: As per Section 3 Clause 4.2.3.11.1 the contribution expected by the awarded bidder is to “actively support the Contracting Authority in its efforts to achieve certification of the European Digital Wallet in accordance with applicable EU regulations, standards, and guidelines. The awarded bidder shall assist in the preparation and execution of conformance, interoperability, and security testing as required by the certification process, including collaboration with designated testing bodies or authorities. The awarded bidder shall also cooperate with external auditors, assessors, or certification bodies by providing access to systems, logs, and personnel as needed to facilitate the certification process.” Of note in Section 2 are:

- Article 18 which defines Milestone 16
- Article 7.5 which specifies relative performance guarantee for Milestone 16
- Article 26.1, specifically Payment 17, which is tied to Milestone 16.

Hence the CA will be bearing the cost related to the Certification of the EUDIW.

Question No. [06]: *Section 2 Article 14.6-14.7:*

Could the Contracting Authority kindly clarify whether full IP ownership under Section 2 Article 14.7 applies to background components / pre-existing product components developed prior to the contract and used to deliver the listed solution components, where such components are not materially adapted specifically for this contract?

Answer No. [06]: The IP of the components listed in Section 2, Article 14.7 are subject to the IP category as identified in the Ownership Matrix defined in the same article.

Question No. [07]: *Section 2 Article 14.5-14.7:*

Could the Contracting Authority kindly clarify whether the source code for mobile-device components of the solution is required to be delivered under an open-source licence, or whether assignment / delivery under the contract terms is sufficient?

Answer No. [07]: Section 2, Article 14 defines which components are to be assigned with full-ownership title, and this includes the Wallet Instances. Section 3, Clause 4.2.1.2 ‘Version 2 - Wallet Solution functionalities’ states the need “to be compliant with the [EUDI Regulation], and all relevant Commission Implementing Regulations including but not limited to [CIR 2015/1502], [GDPR] and other relevant EU and national legislations”. Article 5a ‘European Digital Identity Wallets’ (3) of the [EUDI Regulation] clearly states that “The source code of the application software components of European Digital Identity Wallets shall be open-source licensed.”

Question No. [08]: *Section 3 Clause 4.2.3.11.1; Section 2 Article 18.2; Section 2 Article 26.1:*

Could the Contracting Authority kindly clarify the treatment of Milestone 16 and Payment 17 where the awarded bidder has delivered all required certification support and remediation activities, but successful certification is delayed due to factors outside the bidder's reasonable control, such as certification body timelines or scheme availability?

Answer No. [08]: The Contracting Authority will be responsible for pursuing certification of the Solution, with the awarded bidder providing "Support the Contracting Authority attain certification of the Solution according to national or EU scheme, whichever is applicable at the time" as per Milestone 16. Milestone 16 and Payment 17 remain subject to the certification-related requirements set out in the tender documentation, including the successful certification of the Solution.

Question No. [09]: *Section 3 Clause 4.2.3.7.3*

Phase 1 only ? For both ? Check with Abdellah

Answer No. [09]: The clarification request is unclear and does not contain a sufficiently defined question.

Question No. [10]: *Clauses 1.3.1, Clause 14, Clause 14.7:*

In relation to Clause 1.3.1 of the Tender documents, we understand that the Contractor shall retain ownership of Bespoke Deliverables classified as Vendor-Retained Components and that deliverables shall not qualify as Bespoke Deliverables where the Contractor establishes that they were produced entirely from pre-existing materials without material adaptation.

In this context:

- *Could the Contracting Authority please clarify whether the ownership transfer requirement set out in Clause 14.7 is intended to apply to components which constitute the Contractor's pre-existing background technology, know-how, proprietary materials or intellectual property rights, such as the Wallet Provider, PID Provider and PKI components?*
- *In order to ensure consistency with Clause 1.3.1 and to preserve the Contractor's pre-existing intellectual property rights, would it be acceptable for the Contractor to grant the Customer an appropriate license to use such components without giving any IP rights for source code for the purposes of the Project?*

Answer No. [10]: The definition 'Bespoke Deliverables', includes among others that "Bespoke Deliverables do not include Third-Party Components or Vendor-Retained Components." The definition of 'Vendor-Retained Components' includes "Contractor's own internal tooling not forming part of the contractual deliverable". The IP of the components listed in Section 2, Article 14.7 are subject to the IP category as identified in the Ownership Matrix defined in the

same article, where Wallet Provider, PID Provider and PKI Components are listed as Full Ownership.

Question No. [11]: *Tender Section 3 Clause 4.2.3.11.10; Appendix III - Hosting Requirements; Schedule 1 - Hosting Environment*

Please clarify the target hybrid hosting architecture for Version 2 between the MITA data centres and the Government of Malta Azure Cloud, including which Solution components and data will be hosted in each environment, what will be replicated between the two environments, whether Azure or either MITA data centre will be used for production, backup or disaster recovery, how failover will operate, and the respective responsibilities of MITA or the awarded bidder for provisioning, operation, monitoring and recovery.

Answer No. [11]: 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”. As per Section 3, Clause 4.2.3.11.10 Hosting for Version 2 shall be within “the GoM’s secure hosting environment, using Colocation within MITA data centres in accordance with the hosting and security schedules specified in Appendix III.” Therefore Version 2 will be completely hosted on-premises.

Version 1 will be decommissioned as part of the transition to Version 2. As per Section 1, Criterion 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.”

Question No. [12]: *Section 3 Clause 6.1.1; Key Experts Form:*

Could the Contracting Authority kindly clarify whether formal MFHEA/MQRIC qualification equivalency recognition for non-Malta academic qualifications must be obtained prior to tender submission, or whether such determination may be requested during evaluation?

Answer No. [12]: Qualifications and MFHEA/MQRIC qualification equivalency are to be obtained prior to the tender submission, as per the Key Experts Form which states that “It shall be the Tenderers’ obligation to ascertain that the qualifications possessed by the Key Experts proposed by them are equivalent to the established MQF/EQF Level prior to tender submission. The Evaluation Committee reserves the right to request the determination of the Malta Further & Higher Education Authority (MFHEA) (previously known as Malta Qualifications Council (MQC)) in checking the equivalency of the qualifications, which shall be final. The Malta Qualifications Recognition Information Centre (MQRIC) is the competent body within the Malta Further and Higher Education Authority (MFHEA) (previously known as NCFHE) that

recognises qualifications against the Malta Qualifications Framework (MQF) and whose portal can be accessed here <https://mfhea.mt/> .

Key Experts whose qualifications do not meet the minimum requirements in terms of equivalency, or the equivalency of which is dubious or cannot be determined, shall be rejected”.

Question No. [13]: *Schedule 1; Section 2 Article 5.1; Appendix III:*

Could the Contracting Authority kindly confirm whether MITA will provide any shared hosting/operations services in support of the Solution, such as virtualization layers, monitoring platforms, SIEM integration, PAM, firewalling, or backup tooling, beyond the facilities expressly stated in the tender?

Answer No. [13]: Bidders shall be responsible for proposing a solution architecture that meets all applicable CFT requirements and does not depend on the use of MITA’s perimeter network components.

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

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

Question No. [14]: *Technical Offer Section 2.3(c):*

Could the Contracting Authority kindly confirm whether the optional registration certificate management capability under the RP Registrar section is intended purely as an add-on scored feature, or whether it may become required during implementation?

Answer No. [14]: BPQR Criterion 2.3(c) states that the Awarded Bidder may “Provide, where applicable, an optional component for issuing and managing registration certificates to each registered Relying Party, the PID Provider and all attribute providers.” In order to be awarded these add-on marks, the bidder is to commit to provide the component and indicate how this will be done by providing the required details. In such case, any payments due are in line with the financial bid for.

Furthermore, even if the Awarded Bidder did not include such component in their submission, as per Section 3, Clause 2.2 the Awarded Bidder is expected to “Implement the necessary components for an EUDIW ecosystem compliant with the [EUDI Regulation] and all applicable Implementing Acts”. Should future amendments to the [EUDI Regulation] demand that registration certificates are to be issued, these need to be implemented by the awarded bidder. Such modification of the contract would fall under Section 2, Article 20.6.

Question No. [15]: *Section 3 Clause 4.2.3.7.2; Section 2 Article 14:*

Could the Contracting Authority kindly confirm whether the Signature Creation Application (SCA) may incorporate third-party or OEM software components, provided that the resulting licensing model complies with Section 2 Article 14?

Answer No. [15]: The use of third-party, OEM, open-source, or commercially licensed components within the Signature Creation Application is not precluded by the tender. Bidders shall ensure that any such components and their associated licensing arrangements comply with the intellectual property, source code delivery, ownership, licensing, and deployment requirements set out in Section 2, Article 14 and that any Bespoke Deliverables as defined in Section 2, Article 1.3 (1) developed under the Contract shall remain subject to the applicable intellectual property provisions. Moreover, BPQR Criteria 2.8 (b) awards 3 add-on marks to the bid if the bidder if the title in Intellectual Property for the SCA Component is confirmed as full ownership.

Question No. [16]: *Section 3 Clauses 4.2.2, 4.2.3.10.5, 4.2.3.11.10:*

Could the Contracting Authority kindly confirm whether there is any minimum certification / assurance level expected for HSMs and other critical cryptographic components, such as Common Criteria, FIPS, or equivalent, beyond the functional and EUDI/eIDAS requirements stated?

Answer No. [16]: The tender requires the proposed solution, including its cryptographic components, to comply with the applicable requirements of Commission Implementing Regulations (EU) 2024/2979 and 2024/2981 as indicated in Section 3 Clauses 4.2.1.3, 4.2.2, 4.2.3 and their respective sub clauses.. Common Criteria certification against an appropriate Protection Profile, including EN 419 221-5 where applicable, may constitute relevant assurance evidence for a cryptographic module used for Wallet or trust-service-related functions. However, the Contracting Authority does not confirm that such certification alone will be sufficient in every case. The proposed HSMs shall provide assurance appropriate to their role in protecting cryptographic keys and performing cryptographic operations. The suitability of any HSM certification, including its scope, evaluated configuration, operating assumptions and role within the final Wallet architecture, will be assessed as part of the applicable conformity-assessment and certification process. Tenderers shall therefore propose HSMs and associated assurance evidence that demonstrably support compliance with the applicable legal and technical requirements.

Question No. [17]: *Schedule 2; Section 5.1:*

Could the Contracting Authority kindly clarify whether Priority 1 incidents may require mandatory on-site attendance in Malta, and if so whether any expected physical response times apply?

Answer No. [17]: The awarded bidder shall make sure that the SLAs as specified in the call for tender are met, which may require on-site attendance as stated in Section 3, Clause 5.1 which states that “Some of the Awarded Bidder’s Key Experts, as well as personnel responsible for operational activities, will be required to be physically present in Malta during implementation of the contract as required for operation and maintenance purposes, to attend meetings and address a crisis or major issues.” Specifically, the ‘Systems and Network Engineer’, is to be based in Malta. Furthermore, Schedule 2 Section 2.1 states “Where the Incident is classified as Priority 1, then the Contracting Authority may raise the Incident during and outside Normal Working Hours. In such an event, the Awarded Bidder undertakes to continue working on the Incident outside Normal Working Hours until the Solution is restored within the Restoration Time.” While the CfT does not specify a minimum time by which the personnel are required to be on site in the case of an incident, the Service Levels for the respective Incident categories are defined in Schedule 2.

Question No. [18]: *Section 3 Clause 6.1.1; Clarification Note 01:*

Could the Contracting Authority kindly confirm whether the requirement for Key Expert 7 to be based in Malta applies for the entire duration of the contract, or only during implementation and/or infrastructure operation phases?

Answer No. [18]: As per Section 3, Clause 6.1.1 the responsibilities of the ‘Systems and Network Engineer’ are “deploying, configuring and hardening on-premises infrastructure supporting the Solution. This includes implementation and operation of hyper-converged infrastructure, configuration and management of enterprise networking including segmentation, firewalls, load balancing and secure connectivity between data centres. The expert is also responsible of supporting the integration of PKI components and HSMs in collaboration with the Trust Services Specialist together with ensuring infrastructure security baselines patching, monitoring, logging and backup/restore operations are correctly implemented” and “contribute to operational readiness through documentation, runbooks and knowledge transfer and should work closely with other engineers to ensure alignment with the overall Solution architecture”. The ‘Systems and Network Engineer’ needs to be physically present in Malta to fulfil the above responsibilities, which start from configuration and deployment, and includes operation for the remaining portion of the contract.

Question No. [19]: *Section 5.1; Clarification Note 01*

Could the Contracting Authority kindly clarify, in light of Section 5.1 and Clarification Note 01, whether the requirement for Key Expert 7 to be based in Malta applies throughout the full

contract duration or only during implementation and/or infrastructure operation phases, and whether there are any additional mandatory local presence expectations during the long-term operate, maintain and support phase beyond Key Expert 7 and occasional onsite attendance when necessary?

Answer No. [19]: As per Question No 18.

Question No. [20]: *Section 1 Article 5(B)(d); Clarification Note 01 Answer 01; Clarification Note 02 Answer 02(1)/(3):*

Could the Contracting Authority kindly clarify what evidence package would be considered sufficient at tender stage to substantiate equivalence to ISO/IEC 27001 where a bidder or relevant subcontractor relies on an alternative certification or assurance framework?

Answer No. [20]: As per reference made to Article 5.6 of the General Rules Governing Tenders “it will be the responsibility of the respective bidders, at tendering stage, to prove that the standards, brands or labels they quoted are equivalent to the standards, brands or labels requested by the Contracting Authority.” Evidence of valid certification shall be provided as part of the bid submission. The sufficiency of the evidence submitted will be assessed as part of evaluation.

Question No. [21]: *DPA; Section 5.1; Clarification Note 01:*

Could the Contracting Authority kindly confirm whether personal data processing and operational support activities may be performed from locations within the EU outside Malta, provided all GDPR and contractual requirements are satisfied?

Answer No. [21]: Version 1 must be hosted within the MITA’s Off-Premise Hybrid Cloud Platform (Microsoft Azure) as per Section 3, Clause 4.2.1.1. Version 2 of the Solution shall be hosted in its entirety (including the PKI) in the GoM's secure hosting environment, using Colocation within MITA data centres, as per Section 3, Clause 4.2.3.11.10. Section 3, Clause 4.1.4, 10 defines ‘Solution’ as “the complete and integrated set of components, systems, services, and deliverables proposed and provided by the awarded bidder to fully meet the functional, technical, operational, and compliance requirements as specified in this document.” The Awarded bidder can use remote access to operate the Solution, without prejudice to the physical presence of Key Expert 7 in Malta.

Question No. [22]: *Clarification Note 02 Answer 02(4); Literature List; Section 3 Clauses 4.2.2.x:*

Could the Contracting Authority kindly clarify whether, once the required RWSCD equipment literature, manufacturer data sheets and technical specifications have been submitted at tender

stage, the proposed RWSCD hardware/provider is expected to remain fixed for contract execution, or whether equivalent substitutions may be permitted later, subject to the Contracting Authority's approval and continued compliance with the tender requirements?

Answer No. [22]: As per Section 1.5 (C) (v) “The scope of the literature is to corroborate a fully compliant technical offer.” The proposed RWSCD hardware is expected to remain fixed for contract execution, without prejudice to Section 2, Article 50.1 that states “The equipment is to be warranted during the entire duration of the contract, or covered with a support agreement where that is not possible for the entire contract duration, for full parts and labour, onsite service, software updates; such period is defined as the warranty period. If any equipment, including but not limited to HSMs, appliances, modules, firmware, software, or related components, reaches End-of-Life, End-of-Sale, or End-of-Support during the duration of the contract, the Contractor shall, at its own cost and without degradation of service, replace the affected equipment with an equivalent or superior supported model subject to approval by the Contracting Authority. The replacement shall maintain compatibility with the existing Solution. The Contractor shall provide prior written notice of any End-of-Life or End-of-Support event and shall complete the replacement or upgrade before support expires, ensuring continuity of warranty, maintenance, firmware updates, security patches, and vendor support.”

Question No. [23]: *Appendix III:*

Could the Contracting Authority kindly provide any additional detail regarding expected volumetrics beyond those listed in Appendix III, particularly for the Relying Parties, EAA issuance volumes, RP verification volumes, and peak concurrency / throughput assumptions?

Answer No. [23]: As per Appendix III, “These volumetric projections are intended to inform capacity planning and ensure the solution’s scalability and performance throughout its lifecycle.”

The Tender document does not provide further projections. Bidders are expected to design, size and dimension their proposed solution based on the volumetrics and capacity requirements specified in Appendix III. Any assumptions concerning the number of Wallet Relying Parties, or other volumes and throughput assumption, should be reasonable, proportionate to that volumetrics, and consistent with the intended national deployment of the EUDIW Solution, whilst keeping in mind the obligations set out in Article 5(f) of the [EUDIW Regulation].

Question No. [24]: *Appendix III; Section 3 Clause 4.2.3.7.2:*

Could the Contracting Authority kindly confirm whether any minimum transaction throughput or latency targets apply beyond the listed availability/RTO/RPO requirements and the SCA end-to-end signing duration requirement?

Answer No. [24]: The proposed solution shall be appropriately designed, dimensioned, and implemented to support the reliable, stable, and efficient operation of the service under anticipated and peak demand conditions, whilst meeting all functional, availability, resilience, security, RTO, RPO, and end-to-end signing duration requirements. The bidder remains responsible for ensuring that the proposed architecture and capacity model are sufficient to achieve these outcomes throughout the contract period.

Question No. [25]: *Section 3 Clauses 4.2.2, 4.2.3.10.5, 4.2.3.11.10:*

Could the Contracting Authority kindly confirm whether any part of the RWSCD / HSM estate may leverage existing government infrastructure, or whether the expectation is that the awarded bidder provides the complete cryptographic platform?

Answer No. [25]: The CfT expects the Awarded Bidder to provide the complete cryptographic platform necessary to meet the tender requirements. The technical specifications in this Call for Tenders do not include the setting up of a new Root CA.

Question No. [26]: *Clarification Note 03 Answer 01; General Rules Governing Tenders Article 3:*

Could the Contracting Authority kindly clarify whether the same economic operator may participate in more than one submission in different roles (e.g. consortium member, named subcontractor, supplier of a key component), and whether any specific tender declaration is required in this procedure beyond the General Rules Governing Tenders?

Answer No. [26]: Submission of tenders shall be guided by the General Rules Governing Tenders v4.10. No additional declaration specifically concerning multiple participation is prescribed by this procurement beyond the requirements of the General Rules Governing Tenders and the tender documents. However, each bidder remains responsible for declaring all applicable subcontractors and entities relied upon through the Tender Response Format and ESPD. An Economic Operator may not participate in the same procurement procedure both individually as a bidder and as a member of a Joint Venture/Consortium or individually, or as a member of a Joint Venture/Consortium, and at the same time be nominated as a subcontractor by another Bidder or Joint Venture/Consortium.

Question No. [27]: *Tender Section 3 Clause 4.2.2.2; Appendix II Sections 1 and 3:*

Please confirm whether representative specimen or test eID Cards covering the card generations and JavaCard applet versions in scope will be provided to the awarded bidder for development, integration and acceptance testing, including cards in the initial state required to test first-time activation and mandatory PIN change.

Answer No. [27]: Test/demo Malta eID cards and corresponding CAN will be provided to the Awarded Bidder following signature of the contract. Any test or sample eID cards provided to the awarded bidder will be limited to cards from the current production or issuance batch and will reflect the chip, operating system, application, and technical configuration presently in use. Further details such as quantity of test eID cards will be discussed with the awarded bidder post contract award.

Question No. [28]: *Tender Appendix III - Service Level Requirements; Schedule 2 Sections 2.3, 2.5 and 2.6:*

Please define how the 99.95% availability commitment will be measured, including the service measurement point, calculation period, treatment of approved maintenance windows, and treatment of outages caused by customer-managed or external dependencies such as the national eID service, government networks and European trust services.

Answer No. [28]: The availability commitment shall apply solely to the components of the Solution that are within the operational control and responsibility of the Contractor. Downtime resulting directly from failures, degradation, unavailability, suspension, maintenance, or performance issues affecting third-party or external dependencies not managed by the Contractor, shall be deemed as “available” for SLA measurement purposes and shall not be included in the calculation of Unscheduled Downtime. Where an incident involves both the Solution and an external dependency, only the portion of the outage demonstrably attributable to the Solution shall be considered when calculating service availability.

Question No. [29]: *Tender Section 3 Clause 4.2.3.11.8:*

Please clarify the applicable process if the Contracting Authority requests the handover of operation, maintenance or support for the Solution or an individual component, including the notice period, required transition deliverables, acceptance criteria, duration of transition assistance and responsibility for the associated costs.

Answer No. [29]: As per Section 2, Article 14.4 “The Contracting Authority shall give the Contractor not less than 30 days' written notice of any intended transfer”. As per Section 3, Clause 4.2.3.11.8 “The Contracting Authority at its own discretion may request handing over of the Operation and/or Maintenance and/or Support of the Solution or part thereof.” The scope is to adapt to unforeseen justifiable national context changes throughout the duration of the contract that may impact the Solution or part thereof. Knowledge transfers should not be included in the financial bid. Required transition deliverables, acceptance criteria, duration of transition assistance and responsibility for the associated costs will be discussed if, and when, required.

Question No. [30]: *Schedule 3 Clause 03.27; DPA; Section 2 Articles 41-42:*

Could the Contracting Authority kindly confirm the required retention periods for: (a) security logs, (b) audit trails, (c) operational logs, and (d) personal data, where such periods are stated to be customer-defined?

Answer No. [30]: Retention periods designated are not prescribed by the tender documentation. These will be determined following contract award through the policies and operational procedures, taking into consideration applicable legal, regulatory and operational requirements.

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

Department of Contracts