Procurement on Supply, Delivery, and Managed Services of Fingerprint, Iris and Facial Authentication Devices for PhilSys-enables Services

Questions and Answers (as of 17 May 2021)

REFERENCE	QUERIES	RESPONSES
Section VII. Technical Specifications A. Technical (Page 36 & 37)	PSA require 1,500 Optical scanners & 500 non-optical scanners. What will be the usage application for each of these different type of scanners?	The devices will be supplied to relying parties for the piloting of their respective PhilSys use cases and for research and development purposes. To provide context on the usage of the devices, kindly refer to the Procurement Information Memorandum posted in the PSA procurement website through this link - https://procurement.psa.gov.ph/sites/default/files/1620731173879_1.%20BioAD%20Procurement%20Info%20Memo_signed.pdf
Section VII. Technical Specifications A. Technical (Page 36 & 37)	For better maintenance, will PSA consider all fingerprint scanners to be Optical?	No. The devices will be supplied to relying parties for the piloting of their respective PhilSys use cases and for research and development purposes. To provide context on the usage of the devices, kindly refer to the Procurement Information Memorandum posted in the PSA procurement website through this link - https://procurement.psa.gov.ph/sites/default/files/1620731173879_1.%20BioAD%20Procurement%20Info%20Memo_signed.pdf
Section VII. Technical	Maximum Capture Time	PSA will provide the

Specifications A. Technical (Page 36 & 37)	4 seconds (this is the time for capturing, processing and giving a final response out to the calling application, after the biometrics are well placed on the sensors) Who will provide the application?	application that sends a capture request to the device. The device provider must furnish the MDS that are compliant with MOSIP L1/SBI 2.0 interface definitions.
Section VII. Technical Specifications A. Technical (Page 36)	For the optical scanner, PSA did not indicate any requirement on Sensor Durability. Will PSA consider 9H Hardness as one of the requirement?	No. 9H hardness might be restrictive. Image quality and the support contract is the focus of the procurement.
Section VII. Technical Specifications A. Technical (Page 36)	Will the scanners be used in mountainous areas yet required to operate in normal operation? i.e. The scanner should operate in normal condition even if the altitude is ≤1,800m?	There is a possibility that the devices will be used in mountainous areas as part of the research and development purpose of the procurement. However, the PSA doesn't think there is a significant impact on the altitude vs capture performance.
Section VI. Schedule of Requirements (Page 33-36)	For the MOSIP management server, when is the expected delivery schedule of the management server after NTP?	It has to be in sync with the device delivery.
Section VI. Schedule of Requirements (Page 33-36)	For the conduct and report of VAPT, is it mandatory for independent tester (laboratory) to conduct the test? Would you consider VAPT conducted by in-house Cyber Security team?	Yes. VAPT is to be done by a third-party.
Section VI. Schedule of Requirements (Page 33-36)	Our understanding is that ISO 27001 certification is only applicable for the FTM and it is not applicable for the MOSIP management server. Could you please confirm this?	ISO 27001 is applicable for FTM secure provisioning server and the management server.
Section VI. Schedule of Requirements (Page 33-36)	What is the scope of the components covered by the	Management server can handle any number of

	VAPT? With a single MOSIP management server handling all the four devices (fingerprint optical, fingerprint non-optical, monocular iris, and facial), can the VAPT be conducted only once after all four devices are deployed?	modalities/models and the VAPT is for the management server. There is no correlation between the device deployment and VAPT timelines. Entire management server must be under the scope of VAPT.
Section VI. Schedule of Requirements (Page 33-36)	For the facial authentication devices, the VAPT is expected within 60 calendar days from NTP while the devices themselves would be delivered within 120 calendar days from NTP. In this case, is there a typo mistake for the delivery schedule of the facial authentication devices VAPT?	Yes. The schedule of requirement for ***Lot 4 - 500 Facial Authentication Devices*** VAPT is amended as follows: From: VAPT – within **sixty (60)** calendar days from NTP To: VAPT – within **one hundred twenty (120)** calendar days from NTP Please refer to the Bid Bulletin No. 1 (https://procurement.psa.gov.ph/sites/default/files/05-13-2021%20BID%20BULLETIN%20NO.1%20-%20BIOMETRIC%20AD%20FOR%20PHILSYS_v2.pdf)
Section VI. Schedule of Requirements (Page 33-36)	Is there any specific requirement on the MOSIP management server, e.g. High Availability, Disaster Recovery environment, etc., taking into consideration the allocated ABC for each lots?	High availability may not be needed as the key rotation frequency/policy can be set accordingly. However there has to be a recovery plan to instantiate the management server before field devices are impacted, as per the key rotation/management server sync policies set by the country.
Bid Submission - Monday, 24 May 2021, at 12:00 PM (Page 10)	Can we request for a bid extension?	No. We will adhere to the May 24, 2021 deadline for submission and opening of bids.

	Can we request for extension on the delivery date	The delivery schedule is subject to agreement after issuance of Notice of Award. PSA may allow staggered delivery provided that at least 500 units or 50% (whichever is lower) of the quantity must be initially delivered on the date stated in the Bidding Documents
Section VI. Schedule of Requirements (Page 32 -35)	In view of global electronic and chip shortage, can we request for an ***additional*** 30 calendar days from NTP for all the delivery.	No. However, staggered delivery may be employed provided that at least 500 units or 50% (whichever is lower) of the quantity must be initially delivered on the date stated in the Bidding Documents
ISO 27001 – within four hundred twenty (420) calendar days from NTP (Page 32 - 35)	Can we request an additional 30 calendar days as these certification may take time to obtain 3rd party approval	Yes, additional 30 calendar days could be added to the delivery of ISO 27001 certification. Thus all provision that pertains to the ISO 27001 certification is amended.
FIPS 140-2 Level 3 HSM – within sixty (60) calendar days from NTP (Page 32 - 35)	Can we request for an additional on the calendar days as these certifications may take time to obtain 3rd party approval	No. The HSM make/model must have the certification already. And the requirement is only to furnish proof that the HSM used is FIPs certified.
VAPT – within sixty (65) calendar days from NTP (Page 32 - 35)	Can we request for an additional on the calendar days as these certifications may take time to obtain 3rd party approval	Yes, additional 30 calendar days could be added to the delivery of VAPT report. Thus all provision that pertains to the VAPT conduct and report is amended.
Section VII. Technical Specifications A. Technical Specifications (Page 36)	SBI 2.0 - FTM supported security. How will MOSIP support this certification?	The hardware must meet the specifications listed in the SBI/MDS 0.9.5. The device provider is expected to provide supporting documents and undertaking as prescribed in the bid

		document.
Section VI. Schedule of Requirements (Page 32)	ISO 27001 certification for management server environment and FTM provisioning environment, is PSA providing the location of the environments, such as an existing data centre? Can it be hosted outside PSA? Can all the different kinds of devices (fingerprint scanner, iris and face authentication devices) be using the same management server and FTM provisioning environment?	It is the responsibility of the device provider to host the device management server, adhere to the specs, facilitate audits and own the full security solution. The same provisioning server and management server can be used for provisioning multiple make/model, and for various relying parties in future.
Section VI. Schedule of Requirements (Page 32 - 35)	Will PSA allow batch delivery for each of the devices? i.e 1,500 units of Single Optical Fingerprint to be deliver in 2 batches	Yes, subject to agreement after issuance of Notice of Award. However, there should be an initial delivery of at least 500 units or 50% (whichever is lower) of the quantity on the date stated in the Bidding Documents.
Sec. I. ITB – Bid Submission, page 10	We would like request for an extension on the deadline of the submission and opening of bids?	Request denied. We will adhere to the May 24, 2021 deadline for submission and opening of bids.
Sec. II. 5. Eligible Bidders, on SLCC	If a contract with a client signed by A alone was undertaken by the contractual joint venture of A and B using the facility that was co- developed by the said joint venture partners under and by virtue of their joint venture agreement whereby it was stipulated that A shall be the contracting party with clients for all joint venture projects, can B be equally credited with the track record and	Yes.

	credit for purposes of determining B's single largest completed contract (SLCC) in relation to this project?	
Sec. V Special Conditions of Contract under GCC Clause 2.2 on Payment terms c. On Acceptance: The remaining thirty percent (30%) of the Contract Price shall be paid to the Supplier on a progressive payment scheme.	We would like to request to revise this payment terms into "full payment" upon acceptance of delivered goods since there is already a retention money that will cover the obligation for the warranty as stipulated in Section 62.1 of the 2016 Revised IRR of RA 9184.	Request denied.
Sec. VI Schedule of Requirements, page 32	We would like to request for an extension from 60CD to 90CD.	The delivery schedule is subject to agreement after issuance of Notice of Award. PSA may allow staggered delivery provided that at least 500 units or 50% (whichever is lower) of the quantity must be initially delivered on the date stated in the Bidding Documents
Sec. VII Technical Specifications, Lot 4 Facial Authentication Devices	Is camera included in the L1 compliance requirements?	Yes. All devices must meet L1/SBI 2.0 compliance as specified in the MOSIP Device Service specifications. Kindly refer to these links: https://docs.mosip.io/platform/biometrics/mosip-device-service-specification#device https://docs.mosip.io/platform/biometrics/biometric-specification

Sec. VII Technical Specifications, 4.1. MDS - The devices must meet L1/SBI 2.0 compliance as specified in the MOSIP Device Service specifications. (The devices must have a hardware-based security offered by a Foundation Trust Module/FTM)	We would like to request if L1 compliance requirements can be waived or at least reduced to L0 compliance? We would like to request if SBI 2.0-FTM requirements can be waived?	Request denied. All devices must meet L1/SBI 2.0 compliance as specified in the MOSIP Device Service specifications. Kindly refer to these links: https://docs.mosip.io/platform/biometrics/mosip-device-service-specification#device https://docs.mosip.io/platform/biometrics/biometric-specification
Sec. VII Technical Specifications 4.2. MDS - The devices must be managed by the device provider (Supplier) through a device management server provisioned and operated by the Supplier, that has a FIPS 140-2 Level 3 HSM protecting the device provider keys. Sub-contracting of the management server functionalities is allowed as long as the device provider key belongs to the device provider and the overall security solution is owned and monitored by the device provider. The sole responsibility of meeting the device security and management and any liabilities/penalties or other clauses that are prescribed in the document are with the device provider alone. Device provider must have	Is it up to the Supplier to recommend hardware server specifications? The Device Management server will also be hosted by PhilSys or on-premise with the Supplier? Who will be responsible for generating the device certificate when device is registered to the Management Server? Can the Device Management Server be located and managed outside the Philippines?	Device management server to be provisioned, hosted, and operated by the Supplier. It is the responsibility of the device provider to host the device management server, adhere to the specs, facilitate audits and own the full security solution. The device management server can be located and managed outside the Philippines.

full ownership of the solution and must be able to support all the audit requirements by the Procuring Entity.		