BIDS AND AWARDS COMMITTEE

Supplemental Bid Bulletin No. 2

23 March 2021

Procurement on Supply, Delivery, and Managed Services of 2,800 Registration Kits for the Philippine Identification System (Philsys)

This Bid Bulletin No. 2 modifies respective portions of the Bidding Documents, issued on 03 March 2021.

The changes to the Bidding Documents, as indicated in the succeeding pages, are being issued in compliance with Section 22.5 of the Revised 2016 Implementing Rules and Regulations of RA 9184. Under this section, the procuring entity is directed to issue an amendment at least seven (7) days before the deadline for submission of the bid.

Except as expressly amended by this Bid Bulletin, all other terms and conditions of the Bidding Documents issued on 03 March 2021 shall remain unchanged and shall remain in full force and effect in accordance with their terms.

For guidance and information of all concerned.

(Sgd.)
MINERVA ELOISA P. ESQUIVIAS
OIC Deputy National Statistician
BAC Chairperson

Procurement on Supply, Delivery, and Managed Services of 2,800 Registration Kits for the Philippine Identification System (Philsys)

BID BULLETIN NO. 2

Bid Bulletin No.	***Reference***	***Specific Page / Section in the Bidding Docs***	***Amendments/Revisions***
BB2 - 1	*Section I. ITB -* Submission of Bids and Opening of Bids	Pg.10 From *"Bids must be duly received by the BAC Secretariat through manual submission at the office address indicated below on or before* ***Thursday, March 25, 2021, at 12:00 PM.*** *Late bids shall not be accepted."* From *"Bid opening shall be on* ***Thursday, March 25, 2021, at 02:00 PM*** *at the given address below. Bids will be opened in the presence of the bidders' representatives who choose to attend the activity."*	The Submission of Bids and Bid Opening is hereby revised as follows: To *"Bids must be duly received by the BAC Secretariat through manual submission at the office address indicated below on or before* ***Monday, April 05, 2021, at 12:00 PM.*** *Late bids shall not be accepted."* To *"Bid opening shall be on Thursday,* ***Monday, April 05, 2021, at 02:00 PM using the Zoom platform****. The meeting link will be provided to the representatives who choose to attend the activity."*
BB2 - 2	*Section VII. Technical Specifications*	Pg. 50 *"12. Device Server* *Features* *Rack Server Function* *Rack Server Specifications"*	*The requirements on "12. Device Server" is hereby removed."*
BB2 - 3	*Section VII. Technical Specifications*	*Pg.52* *"13. Management Server and Management Client"* From *"Functions:* *Biometric devices are expected to get connected with the management server and get a certificate issued by the device provider for its usage in the MOSIP ecosystem."* From *"The management server*	The requirements for "13. Management Server and Management Client" are hereby revised as follows: To *"The Management Server shall be provided and hosted by PSA while the MDS software (which includes management client component that communicates with management server) shall be supplied by the bidder. Bidder shall integrate their MDS with the Management Server through a set of REST APIs."* To "*Management Server*

Bid Bulletin No.	***Reference***	***Specific Page / Section in the Bidding Docs***	***Amendments/Revisions***
		has the following objectives. *1. Validate the devices to ensure it is a genuine device from the respective device provider. This can be achieved using the device info and the certificates of the Foundational Trust Module.* *2. Manage/Sync time between the end device and the server. The time to be synced should be the only trusted time accepted by the device.* *3. Ability to issue commands to the end device for* *a. Cleanup of the device keys* *b. Collect device information to maintain, manage, support, and upgrade a device remotely.* *4. A central repository of all the approved devices from the device provider.* *5. Safe storage of keys using HSM FIPS 140-2 Level 3. These keys are used to issue the device certificate upon registration of the device with the Management Server. The Management Server is created and hosted by the device provider outside of MOSIP software. The communication protocols between the MDS and the Management Server can be decided by the respective device provider. Such communication should be restricted to the above specified interactions only. No transactional information should be sent to this server.*	*The Management Server shall be provided and hosted by PSA.* *Management Server Functions:* *The bidder is expected to work with the PSA to store/load/save the root device provider signing private key in the management server HSM hosted by PSA using a secure operating process laid out by PSA Individual biometric devices are expected to get connected with the management server and get a device certificate (key rotation) issued by the device provider signing key.* *The management server provided by PSA has the following objectives. Full set of management server APIs will be shared for integrating with device MDS.* *1. Validate the devices to ensure it is a genuine device from the respective device provider. The logic to validate if the request to sign is coming from a valid device is explained as part of the management server API documentation shared by PSA.* *2. Manage/Sync time between the end device and the server. The time to be synced should be the only trusted time accepted by the device.* *3. Ability to issue commands to the end device for* *a. Cleanup of the device keys* *b. Collect device information to maintain, manage, support, and upgrade a device remotely.* *4. A central repository of all the approved devices from the device provider.*

Bid Bulletin No.	***Reference***	***Specific Page / Section in the Bidding Docs***	***Amendments/Revisions***
		6. Should have the ability to push updates from the server to the client devices. *Please refer to: https://docs.mosip.io/platform/biometrics/mosip-device-servicespecification”*	*5. Safe storage of keys using HSM FIPS 140-2 Level 3. These keys are used to issue the device certificate upon registration of the device with the Management Server.* *6. Should have the ability to push updates from the server to the client devices.* *Bidder must take the responsibility of upgrading the MDS in case of a MDS specification update or a patch requirement for any reasons. The bidder can work with the PSA and the upgraded software can be pushed to individual MDS instances as per the mechanism available in the management server.* *The Management Server is provided and hosted by PSA. The communication protocols between the MDS and the Management Server are as describe as follows:* *Please refer to Annex A. PSA Management Server APIs of this Bid Bulletin.*
		From *“The Management Client is the interface that connects the device with the respective management server.”*	To “*Management Client* *The MDS software (which includes management client component that communicates with management server) shall be supplied by the bidder.* *The management client is a component within MOSIP Device Service (MDS) that is responsible for handling the device management functionalities and interface with the management server. Please go through MOSIP MDS specifications for the full set of requirements.* *For more details, please refer to this link:*

Bid Bulletin No.	*Reference*	*Specific Page / Section in the Bidding Docs*	*Amendments/Revisions*
		Features of the management client include: *1. For better and efficient handling of devices at large volume, we expect the devices to auto register to the Management server.* *2. All communication to the server and from the server should follow that below properties.* *a. All communications are digitally signed with the approved algorithms.* *b. All communications to the server are encrypted using one of the approved public key cryptographies (HTTPS – TLS1.2/1.3 is required with one of the approved algorithms.* *c. All requests have timestamps attached in ISO format to the milliseconds inside the signature.* *d. All communication back and forth should have the signed digital id as one of the attributes.* *3. It is expected that the auto registration has an absolute way to identify and validate the devices.* *4. The management client should be able to detect the devices in a plug and play model.*	*https://docs.mosip.io/platform/biometrics/mosip-device-service-specification* *Features of the management client include:* *1. For better and efficient handling of devices at large volume, we expect the devices to auto register to the Management server.* *2. All communication to the server and from the server should follow that below properties.* *a. All communications are digitally signed with the approved algorithms as defined in PSA management server APIs.* *b. All communications to the server are encrypted using one of the approved public key cryptographies as defined in PSA management server APIs.* *c. All requests have timestamps attached in ISO format to the milliseconds inside the signature.* *d. All communication back and forth should have the signed digital id as one of the attributes.* *3. The MDS should be able to detect the devices in a plug and play model.* *4. All key rotation should be triggered from the server. The MDS must have the capability to create the device specific key pair within the windows keystore*

<table>
<tr><th>Bid Bulletin No.</th><th>Reference</th><th>Specific Page / Section in the Bidding Docs</th><th>Amendments/Revisions</th></tr>
<tr><td></td><td></td><td>5. All key rotation should be triggered from the server.
6. Should have the ability to detect if it is speaking to the right management server.
7. All upgrades should be verifiable, and the client should have ability to verify software upgrades.
8. Should not allow any downgrade of software.
9. Should not expose any API to capture biometric. The management server should have no ability to trigger a capture request.
10. No logging of biometric data is allowed. (Both in the encrypted and unencrypted format)
Please refer to: https://docs.mosip.io/platform/biometrics/mosip-device-service-specification</td><td>or TPM, get the public key signed by the device provider signing key in management server HSM and get a device certificate issued by management server for that device. The keys are rotated based on commands issued by the management server.
5. Should have the ability to detect if it is speaking to the right management server. Please refer to PSA management server APIs.
6. Should not expose any API to capture biometric. The management server should have no ability to trigger a capture request.
7. No logging of biometric data is allowed. (Both in the encrypted and unencrypted format).
Full set of Management server APIs supporting above requirements are available in Annex A of this Bid Bulletin.”</td></tr>
<tr><td>BB2 - 4</td><td>Section VII. Technical Specifications</td><td>Pg. 44
From:<table><tr><td>“Standards</td><td>Fingerprint (4+4+2) slap capture equipment under Image Specification: ISO/IEC 19794-5:2011 B.1 AFIS Normative”</td></tr></table></td><td>Append a requirement on Standards with the following specifications:
To:<table><tr><td>“Standards</td><td>Fingerprint (4+4+2) slap capture equipment under Image Specification: FBI Appendix F Certified;
and Compliant with ISO/IEC 19794-4:2011 B.1 AFIS Normative.”</td></tr></table></td></tr>
</table>

Bid Bulletin No.	***Reference***	***Specific Page / Section in the Bidding Docs***	***Amendments/Revisions***
BB2 - 5	*Section VII. Technical Specifications* *Iris capturing equipment*	Pg .48 Software API From *“Compliant with the operating system and PhilSys registration client application's device manager specifications to handle device discovery, streaming, capture, and other device lifecycle management requirements as specified in the MOSIP specification document.”*	6. Iris capturing equipment: For the Iris Capturing Equipment under Software API is hereby revised as follows: To *“Compliant with the operating system and PhilSys registration client application to handle device discovery, streaming, capture, and other device lifecycle management requirements as specified in the MOSIP specification document and PSA Management server API specification document.* *For MOSIP specification please refer to this link:* *https://docs.mosip.io/platform/biometrics/mosip-device-service-specification* *For PSA management server API specification please refer to Annex A of this Bid Bulletin.”*
BB2 - 6	*Section VII. Technical Specifications* *Fingerprint (4+4+2) slap capture equipment*	Pg. 46 Software API From *“Compliant with the operating system and PhilSys registration client application's device manager specifications to handle device discovery, streaming, capture, and other device lifecycle management requirements as specified in the MOSIP specification document.”*	5. Fingerprint (4+4+2) slap capture equipment: For the Fingerprint (4+4+2) slap capture equipment under Software API is hereby revised as follows: To *“Compliant with the operating system and PhilSys registration client application to handle device discovery, streaming, capture, and other device lifecycle management requirements as specified in the MOSIP specification document and PSA Management server API specification document.* *For MOSIP specification please refer to this link:* *https://docs.mosip.io/platform/biometrics/mosip-device-service-specification* *For PSA management server API specification please refer to Annex A of this Bid Bulletin.”*

Bid Bulletin No.	***Reference***	***Specific Page / Section in the Bidding Docs***	***Amendments/Revisions***
BB2 - 7	*Section VII. Technical Specifications* *3.HD Webcam*	Pg. 42 Software API From *"Compliant with the operating system and PhilSys registration client application's device manager specifications to handle device discovery, streaming, capture, and other device lifecycle management requirements as specified in the MOSIP specification document."*	3. HD Webcam For the HD Webcam equipment under Software API is hereby revised as follows: To *"Compliant with the operating system and PhilSys registration client application to handle device discovery, streaming, capture, and other device lifecycle management requirements as specified in the MOSIP specification document and PSA Management server API specification document.* *For MOSIP specification please refer to this link:* https://docs.mosip.io/platform/biometrics/mosip-device-service-specification *For PSA management server API specification please refer to Annex A to this Bid Bulletin.*
BB2 - 8	*Section VII. Technical Specifications* *Responsibilities of the Supplier*	Pg. 58 From *"6.4 Upgrade and run the latest version of the software during the contract period in case there is a necessary update to the APIs or registration client specifications."*	Append the requirement under Responsibilities of the Supplier under 6.4: To *"6.4 Upgrade and run the latest version of the software during support contract period including licensing/software ownership if there is a necessary update to the APIs, registration client specifications and other related software."*