Republic of the Philippines
DEPARTMENT OF FINANCE
Roxas Blvd. corner P. Ocampo St., 1004 Manila

BAGONG PILIPINAS

BIDS AND AWARDS COMMITTEE
Supplemental Bid Bulletin No. 1

September 24, 2024

Procurement of Advanced Electronic Signatures (AES) Solution for an Automated DOF Processes
IB No. 2024-14-G

This **Supplemental Bid Bulletin No. 1** is issued to modify or amend the item in the Bid Documents. This shall form an integral part of the Bid Documents.

REFERENCE			AMENDMENT/CHANGE/CLARIFICATION		
Technical Specifications Page 33 - 35			**Technical Specifications Page 33 - 35**		
Item	**Description**	**Statement of Compliance**	**Item**	**Description**	**Statement of Compliance**
A	**Services**		**A**	**Services**	
1	Digital Signature Solution for (1) one year		1	Digital Signature Solution for (1) one year	
2	The solution service provider must conduct software training and knowledge transfer sessions to familiarize users with the system's features.		2	The solution service provider must conduct software training and knowledge transfer sessions to familiarize users with the system's features.	
3	The solution services provider must conduct software prototype testing before actual deployment.		3	The solution services provider must conduct software prototype testing before actual deployment.	
	<Additional>		***4***	***The solution provider must have a prior experience in developing, implementing, customizing and integrating API driven applications.***	
B	**Features**		**B**	**Features**	
	<Additional>		***5***	***The solution must be able to accommodate up to 250 document creators.***	
4	The solution must be able to upload an unlimited document annually.		***6***	The solution must be able to upload an unlimited document annually.	
~~5~~	The solution must allow the self-sign-up feature.		***7***	The solution must allow the self-sign-up feature.	
~~6~~	The solution must have role-based access control with granular permissions.		***8***	The solution must have role-based access control with granular permissions.	
~~7~~	The solution must have a minimum storage capacity of 250 GB.		***9***	The solution must have a minimum storage capacity of 250 GB.	
~~8~~	The solution must be scalable to accommodate future growth in the number of users and documents.		***10***	The solution must be scalable to accommodate future growth in the number of users and documents.	

REFERENCE			AMENDMENT/CHANGE/CLARIFICATION		
~~9~~	The solution must allow individual or group signing capabilities per document.		***11***	The solution must allow individual or group signing capabilities per document.	
~~10~~	The completed and downloaded signed document should not have an expiry date, and all signed documents must remain valid forever.		***12***	The completed and downloaded signed document should not have an expiry date, and all signed documents must remain valid forever.	
~~11~~	The solution must be able to sign documents with or without a Digital Signature Solution Account.		***13***	The solution must be able to sign documents with or without a Digital Signature Solution Account.	
~~12~~	The solution must provide the option for users to sign multiple-page documents in one instance.		***14***	The solution must provide the option for users to sign multiple-page documents in one instance.	
~~13~~	The solution must enable recurring documents to be saved as a template.		***15***	The solution must enable recurring documents to be saved as a template.	
~~14~~	The solution must allow replacement and re-delegation of signers if they are not available.		***16***	The solution must allow replacement and re-delegation of signers if they are not available.	
~~15~~	The solution must generate an audit trail that serves as proof of the transaction.		***17***	The solution must generate an audit trail that serves as proof of the transaction.	
~~16~~	The solution must support signing multiple document formats.		***18***	The solution must support signing multiple document formats.	
~~17~~	The solution must support various channels, including wed application for (Desktop and Mobile Devices), as well as mobile applications for (iOS and Android)		***19***	The solution must support various channels, including wed application for (Desktop and Mobile Devices), as well as mobile applications for (iOS and Android)	
~~18~~	The solution should include the option to import users and contacts in bulk		***20***	The solution should include the option to import users and contacts in bulk	
~~19~~	The solution must offer features that allow users to edit and upload their own signature images.		***21***	The solution must offer features that allow users to edit and upload their own signature images.	
~~20~~	The solution must offer flexible user authentication options, such as supporting SAML to accommodate varying user authentication needs.		***22***	The solution must offer flexible user authentication options, such as supporting SAML to accommodate varying user authentication needs.	
~~21~~	The solution must have the facility to support the implementation of single sign-on authentication.		***23***	The solution must have the facility to support the implementation of single sign-on authentication.	
~~22~~	The solution must support major operating systems (Windows, macOS, and Linux) platforms and commonly used web browsers.		***24***	The solution must support major operating systems (Windows, macOS, and Linux) platforms and commonly used web browsers.	
C.	**Security**		**C.**	**Security**	
~~23~~	The solution must support the Elliptic Curve Digital Signature Algorithm (ECDSA) with a minimum key size of 256 bits for signature generation and verification.		***25***	The solution must support the Elliptic Curve Digital Signature Algorithm (ECDSA) with a minimum key size of 256 bits for signature generation and verification.	

REFERENCE			AMENDMENT/CHANGE/CLARIFICATION		
~~24~~	The solution must ensure that digitally signed documents are legally binding and admissible in court during disputes. Additionally, it must undergo mandatory annual performance audits conducted by qualified auditors.		***26***	The solution must ensure that digitally signed documents are legally binding and admissible in court during disputes. Additionally, it must undergo mandatory annual performance audits conducted by qualified auditors.	
~~25~~	The solution must support the hashing algorithm SHA-256 or higher.		***27***	The solution must support the hashing algorithm SHA-256 or higher.	
~~26~~	The solution must support the Asymmetric encryption Algorithm RSA with a minimum key size of 2048 bits.		***28***	The solution must support the Asymmetric encryption Algorithm RSA with a minimum key size of 2048 bits.	
~~27~~	The solution provided must include an option for eKYC for every signed document.		***29***	The solution provided must include an option for eKYC for every signed document.	
~~28~~	The solution must have secure storage.		***30***	The solution must have secure storage.	
~~29~~	The solution must be capable of facilitating long-term archiving and non-repudiation of signed documents, with Certificate Revocation List (CRL) support ensuring the validation of the certificates.		***31***	The solution must be capable of facilitating long-term archiving and non-repudiation of signed documents, with Certificate Revocation List (CRL) support ensuring the validation of the certificates.	
~~30~~	The solution must include multi-factor authentication, and it's enforced during signing of documents		***32***	The solution must include multi-factor authentication, and it's enforced during signing of documents	
~~31~~	The solution must support secure communication protocols.		***33***	The solution must support secure communication protocols.	
~~32~~	The solution must have timestamping for document integrity verification.		***34***	The solution must have timestamping for document integrity verification.	
~~33~~	The solution must have secure document viewing and annotation capabilities.		***35***	The solution must have secure document viewing and annotation capabilities.	
~~34~~	The solution should include tamper-proof documents to prevent unauthorized changes without detection, utilizing special printing methods to ensure the integrity and reliability of the information.		***36***	The solution should include tamper-proof documents to prevent unauthorized changes without detection, utilizing special printing methods to ensure the integrity and reliability of the information.	
~~35~~	The solution should check certificates in real-time using the Online Certificate Status Protocol (OCSP).		***37***	The solution should check certificates in real-time using the Online Certificate Status Protocol (OCSP).	
~~36~~	The solution should include the capability to validate hard copy documents via QR code scanning as an option.		***38***	The solution should include the capability to validate hard copy documents via QR code scanning as an option.	
D.	**Signature**		**D.**	**Signature**	
~~37~~	The solution must support various certificate types, including individual and organizational certificates.		***39***	The solution must support various certificate types, including individual and organizational certificates.	

REFERENCE			AMENDMENT/CHANGE/CLARIFICATION		
~~38~~	The solution must primarily support the Department of Information and Communication Technology (DICT) National Certification Authority (NCA) – Philippine National PKI (PNPKI), or secondary support extended to global/third party CAs.		***40***	The solution must primarily support the Department of Information and Communication Technology (DICT) National Certification Authority (NCA) – Philippine National PKI (PNPKI), or secondary support extended to global/third party CAs.	
~~39~~	The solution must support the signing of documents using a trusted Certification Authority (CA) recognized by the Philippine Government.		***41***	The solution must support the signing of documents using a trusted Certification Authority (CA) recognized by the Philippine Government.	
~~40~~	The solution must support documents using Publicly Trusted Certificates.		***42***	The solution must support documents using Publicly Trusted Certificates.	
E.	**Integration**		**E.**	**Integration**	
~~41~~	The solution should be flexible to allow API integration with commonly used applications.		***43***	The solution should be flexible to allow API integration with commonly used applications.	
~~42~~	Through user management, the solution should have the capability to perform document uploading, downloading, signing, and deleting through API calls.		***44***	Through user management, the solution should have the capability to perform document uploading, downloading, signing, and deleting through API calls.	
	<Additional>		***45***	***The solution provider must be able to assist in the integration of PNPKI with the document signing solution.***	
~~43~~	The solution must provide integration options with SharePoint, OneDrive, Google Drive, Dropbox, and Alfresco.		***46***	The solution must provide integration options with SharePoint, OneDrive, Google Drive, Dropbox, and Alfresco.	
~~44~~	The solution must have comprehensive logging and auditing capabilities for transaction and key usage.		***47***	The solution must have comprehensive logging and auditing capabilities for transaction and key usage.	
~~45~~	The solution must be scalable to accommodate future growth and digital signature adoption.		***48***	The solution must be scalable to accommodate future growth and digital signature adoption.	
	Compliance			**Compliance**	
~~46~~	The solution must comply with the Philippine Electronic Commerce Act (RA No. 8792).		***49***	The solution must comply with the Philippine Electronic Commerce Act (RA No. 8792).	
~~47~~	The solution must comply with the Philippine Data Privacy Act of 2012.		***50***	The solution must comply with the Philippine Data Privacy Act of 2012.	
~~48~~	The solution should leverage the PDF Advanced Electronic Signature (PAdES) framework.		***51***	The solution should leverage the PDF Advanced Electronic Signature (PAdES) framework.	
~~49~~	The solution must utilize the Cryptographic Message Syntax Advanced Electronic Signature (CAdES) framework.		***52***	The solution must utilize the Cryptographic Message Syntax Advanced Electronic Signature (CAdES) framework.	

REFERENCE			AMENDMENT/CHANGE/CLARIFICATION		
~~50~~	The solution must comply with COA Circular No. 2021-006 Guidelines on the use of electronic documents, Electronic Signature, and Digital Signature in Government Transactions.		*53*	The solution must comply with COA Circular No. 2021-006 Guidelines on the use of electronic documents, Electronic Signature, and Digital Signature in Government Transactions.	
	Support			**Support**	
~~52~~	The service should include local support for online and email assistance, available 8x5 as needed.		*54*	The service should include local support for online and email assistance, available 8x5 as needed.	
~~53~~	Provide remediation based on health checks performed for signing solution, with service reports delivered upon completion of the remediation works.		*55*	Provide remediation based on health checks performed for signing solution, with service reports delivered upon completion of the remediation works.	

For guidance and information of all concerned.

DAKILA ELTEEN M. NAPAO
Assistant Secretary and BAC Chairperson