

BID BULLETIN NO. 1
For LBP-HOBAC-ITB-GS-20180215-02

PROJECT : **Supply, Delivery and Installation of Two-Factor (2FA) Authentication Server**


IMPLEMENTOR : **Procurement Department**

DATE : **March 22, 2018**

This Bid Bulletin is issued to modify, amend or clarify items in the Bid Documents. This shall form an integral part of the Bid Documents.

The modifications, amendments or clarifications are as follows:

- The Terms of Reference (Annex A), Section VII (Specifications) and Checklist of the Bidding Documents (Items 3.h & 6) have been revised. Please see attached revised Annexes A-1 to A-6 and the specified sections of the Bidding Documents.


ALWIN I. REYES, CSSP
Assistant Vice President
Head, Procurement Department and
HOBAC Secretariat

Specifications

| <p>Specifications</p> | <p>Statement of Compliance</p> <p>Bidders must state below either “Comply” or “Not Comply” against each of the individual parameters of each specification.</p> <p>Statements of “Comply” or “Not Comply” must be supported by evidence in a Bidders Bid. Evidence shall be in the form of manufacturer’s un-amended sales literature, unconditional statements of specification and compliance issued by the manufacturer, samples, independent test data etc., as appropriate. A statement that is not supported by evidence or is subsequently found to be contradicted by the evidence presented will render the Bid under evaluation liable for rejection. A statement either in the Bidders statement of compliance or the supporting evidence that is found to be false either during Bid evaluation, post-qualification or the execution of the Contract may be regarded as fraudulent and render the Bidder or supplier liable for prosecution subject to the provisions of ITB Clause 3.1(a)(ii) and/or GCC Clause 2.1(a)(ii)</p> |
|--|---|
| <p>Supply, Delivery and Installation of 2FA Authentication Server</p> <p>Minimum specifications and other requirements per attached Revised Terms of Reference (Annexes A-1 to A-6).</p> <p>The following documents shall be submitted inside the eligibility/technical envelope:</p> <ul style="list-style-type: none"> ▪ Duly filled-out Revised Terms of Reference signed in all pages by authorized representative/s. ▪ Manufacturer’s authorization or back-to-back certification to prove that the supplier is authorized to sell the offered item for the last three (3) years. ▪ Certification of at least two (2) engineers of the offered solution with | <p>Please state here either “Comply” or “Not Comply”</p> |

| | |
|--|--|
| certificate of employment. | |
| <ul style="list-style-type: none">List of at least three (3) installed bases of similar solution and/or equivalent technology such as SSL and IPSEC VPN and FTP, wherein one of which is a Bank, with addresses and contact details. | |

Conforme:

Name of Bidder

Signature over Printed Name of
Authorized Representative

Position

Checklist of Bidding Documents for Procurement of Goods and Services

Documents should be arranged as per this Checklist. Kindly provide folders or guides, dividers and ear tags with appropriate labels.

The Technical Component (First Envelope) shall contain the following:

1. Duly notarized Secretary's Certificate attesting that the signatory is the duly authorized representative of the prospective bidder, and granted full power and authority to do, execute and perform any and all acts necessary and/or to represent the prospective bidder in the bidding, if the prospective bidder is a corporation, partnership, cooperative, or joint venture (sample form - Form No.7).
2. Duly notarized Omnibus sworn statement (sample form - Form No.6).
3. Eligibility requirements

- **Legal Document**

3.a PhilGEPS Certificate of Registration (Platinum Membership). All documents enumerated in its Annex A must be updated; or

3.b Class "A" eligibility documents as follows:

- Registration Certificate from SEC, Department of Trade and Industry (DTI) for Sole Proprietorship, or CDA for Cooperatives, or any proof of such registration as stated in the Bidding Documents;
- Valid and current mayor's permit issued by the city or municipality where the principal place of business of the prospective bidder is located; and
- Tax Clearance per Executive Order 398, Series of 2005, as finally reviewed and approved by the BIR.

- **Technical / Financial Documents**

3.c Statement of the prospective bidder of all its ongoing government and private contracts, including contracts awarded but not yet started, if any, whether similar or not similar in nature and complexity to the contract to be bid, within the relevant period as provided in the Bidding Documents. The statement shall include all information required in the PBDs prescribed by the GPPB. (sample form - Form No. 3). The duly signed form shall still be submitted even if the bidder has no on-going contract.

- 3.d Statement of the prospective bidder identifying its single largest completed contract similar to the contract to be bid, equivalent to at least fifty percent (50%) of the ABC supported with contract/purchase order, end-user's acceptance or official receipt(s) issued for the contract, within the relevant period as provided in the Bidding Documents. The statement shall include all information required in the PBDs prescribed by the GPPB. (sample form - Form No. 4).
- 3.e The prospective bidder's audited financial statements, showing, among others, the prospective bidder's total and current assets and liabilities, stamped "received" by the BIR or its duly accredited and authorized institutions, for the preceding calendar year which should not be earlier than two (2) years from the date of bid submission.
- 3.f The prospective bidder's computation for its Net Financial Contracting Capacity (sample form - Form No. 5).
- 3.g Valid joint venture agreement (JVA), in case the joint venture is already in existence. In the absence of a JVA, duly notarized statements from all the potential joint venture partners stating that they will enter into and abide by the provisions of the JVA in the instance that the bid is successful shall be included in the bid. Failure to enter into a joint venture in the event of a contract award shall be ground for the forfeiture of the bid security. Each partner of the joint venture shall submit the legal eligibility documents. The submission of technical and financial eligibility documents by any of the joint venture partners constitutes compliance.
- 3.h Duly filled-out Revised Terms of Reference signed in all pages by authorized representative/s.**
- 3.i Manufacturer's authorization or back-to-back certification to prove that the supplier is authorized to sell the offered item for the last three (3) years.
- 3.j Certification of at least two (2) engineers of the offered solution with certificate of employment.
- 3.k List of at least three (3) installed bases of similar solution and/or equivalent technology such as SSL and IPSEC VPN and FTP, wherein one of which is a Bank, with addresses and contact details.
- 4. Bid security in the prescribed form, amount and validity period (ITB Clause 18.1 of the Bid Data Sheet);
- 5. Schedule VI - Schedule of Requirements with signature of bidder's authorized representative.
- 6. Revised Section VII - Specifications with response on compliance and signature of bidder's authorized representative.**

7. Post-Qualification Documents – (Non-submission of these documents during the bid opening shall not be a ground for the disqualification of the bidder):

7.a Business Tax Returns per Revenue Regulations 3-2005 (BIR No.2550 Q) VAT or Percentage Tax Returns for the last two (2) quarters filed manually or through the BIR EFPS; and

7.b Income Tax Return for 2016 filed manually or through the BIR EFPS

The Financial Component (Second Envelope) shall contain the following:

1. Duly filled out Bid Form signed by the bidder's authorized representative (sample form - Form No.1)
2. Duly filled out Schedule of Prices signed by the bidder's authorized representative (sample form - Form No.2)
3. Breakdown of cost using Annex B.

LANDBANK OF THE PHILIPPINES

TERMS OF REFERENCE - TWO-FACTOR (2FA) AUTHENTICATION

| Technical Requirements: | Compliance |
|--|------------|
| 1.0 Two-Factor (2FA) Authentication Server | |
| The 2FA authentication server must be able to support the following type of authenticators: <ul style="list-style-type: none"> * On-demand authenticator (Short Message System) * Hardware authenticator * Software authenticator | |
| The 2FA authentication server must be available in both software and appliance form. | |
| The 2FA authentication server must come with a RADIUS server with no additional cost. | |
| The solution must be a leader in the Gartner Magic Quadrant for User Authentication | |
| The management interface of the RADIUS server must be fully embedded within the same management console as the 2FA authentication server to simplify setup and on-going management. | |
| The 2FA authentication server and authenticators must be designed and manufactured by the same company. | |
| The 2FA authenticators must be built and assembled by the same company. | |
| The 2FA hardware authenticator seed used to generate the One Time Password or OTP must be created and generated only upon an order from a customer. It must not be pre injected in bulk without a genuine customer purchase. | |
| The 2FA authentication server must support Security in Depth (SID) authentication protocol out-of-the-box with no additional customization required. | |
| The 2FA authentication server must support CT-KIP (Cryptographic Token Key Initiation Protocol) protocol out-of-the-box with no additional customization required. | |
| The 2FA authentication server must provide Business Continuity Option without requiring the use of hardware authenticators for 2FA authentication. | |
| The 2FA authentication server must provide a user self-service portal out-of-the-box with no additional cost. | |
| The user self-service portal must provide the following functions: <ul style="list-style-type: none"> * Separated from the 2FA authentication server to avoid exposing the server and to facilitate the hosting of self-service portal function in the DMZ. * Report a lost or unavailable token. If a user has left his hardware token at home while travelling, for example, an on-demand token code, or set of one-time token codes, is issued to authenticate him temporarily to the network. * Report a permanently lost or damaged token. This is similar to the above, except that an extra workflow can be initiated to disable the user's lost/damaged token and, if necessary, issue a new token to the user. * Forgotten PIN. A token code can be issued to the user to authenticate before a PIN reset is initiated as an extra security precaution. * Grant Emergency Access. In the event a user forgets both login and PIN, emergency access can be granted by asking the user 'life questions' pre-populated from the database. * Request a replacement token. * Test a token. | |

| | |
|--|--|
| * Workflow provisioning for the creation of productivity saving processes that speed deployment scenarios and ease the work load of IT staff. | |
| The 2FA authentication server must support the use of an external LDAP directory without making changes to the data schema. The following external LDAP directory must be supported: * Authentication Manager internal database * Oracle Directory Server Enterprise Edition 11G * Microsoft Active Directory | |
| The administration user interface of the 2FA authentication server must be web-based and the communication channel must be encrypted. | |
| The solution must provide Microsoft Management Console Snap-in. | |
| The 2FA authentication server must provide delegated multi-level administration capability. It must enable granular administrative access control down to a user/group and policy level. | |
| The 2FA authentication solution must be able to integrate with over 350 certified third-party applications out-of-the-box with no customization required. | |
| The 2FA authentication server must be able to support software authenticators for the following platforms: 1. Smartphones a. Blackberry smartphones b. iPhone devices c. Windows Mobile devices d. Java smartphones e. Symbian OS and UIQ devices 2. Laptops and Desktops a. Microsoft Windows b. Mac OS X 3. Web Browsers a. SID Toolbar b. SID Software Token for Web SDK 4. Mobile SDK a. iOS b. Android | |
| The 2FA authentication server must provide API function calls usable by customized applications that require 2FA authentication integration. The API function calls should be able available for Java and C# programming language. | |
| The 2FA authentication server must support 15 replicas when necessary. | |
| The 2FA authentication server must provide load balancing capabilities for authentication request across all of the authentication servers including replicas. | |
| The 2FA authentication server must support propriety protocol based on strong cryptographic algorithms based on AES. | |
| The 2FA authentication server must be a leader in the Gartner's User Authentication Quadrant. | |
| The 2FA authentication server must protect authentication password stored in the server using SHA-256. | |
| Sensitive data at rest stored in the database must be encrypted with AES and SHA cryptographic algorithms. | |
| Trust between 2FA primary and secondary servers must be secured by 2 way SSL channel. | |

| | |
|--|--|
| 2.0 Authenticators | |
| 2.1 Hardware Authenticator | |
| The hardware authenticator must come with lifetime warranty and free replacement during the lifetime. | |
| The hardware authenticator must be water resistant. | |
| The hardware authenticator must not be made and assembled in China. | |
| The hardware authenticator must conform to the following standards: <ul style="list-style-type: none"> * Tamper evidence: ISO 13491-1; ISO DIS 13491-2:2005 * Product safety standards: RoHS, WEEE, CE, cRoHS * Regulatory standards: FCC Part 15 Class A and Class B, EN55022 Class A and Class B | |
| The hardware authenticator must be able to operate normally within -15C to 60C operating temperature. | |
| The hardware authenticator must provide fix battery lifespan options as follows: <ul style="list-style-type: none"> * 2 years * 3 years * 4 years * 5 years | |
| The OTP (One-Time Password) generated by the token must: <ul style="list-style-type: none"> * be random and not in running sequence * be automatically replaced by another random number every thirty or sixty seconds without having the need to press any buttons. * not be allowed to be used more than once * expire and becomes invalid after 30 or 60 seconds | |
| The OTP must be generated based on AES 128-bit ECB mode. | |
| The hardware authenticator must become unusable when being tampered or forced open. | |
| The LCD display of the hardware authenticator must provide countdown bars on the left of the display signalling when the code on the token will change to a different number. | |
| There must be a flashing dot on the bottom right of the display indicating that the token is functioning. | |
| When the hardware authenticator is going to expire within the next month, a small numerical three must be displayed above the flashing dot. | |
| When the token actually expires, the token must provide the following indication: <ul style="list-style-type: none"> * Numbers on the display disappear * The tiny three remains to indicate that the token has expired. | |
| The back of the token must contains certain token specific information such as the date of expiration, and the serial number of the token – engraved, printed and in bar code format. | |
| 2.2 Software Authenticator | |
| Software authenticator must support the following platforms out-of-the-box with no customization required: <ol style="list-style-type: none"> 1. Smartphones <ol style="list-style-type: none"> a. Blackberry smartphones b. iPhone devices c. Windows Mobile devices d. Java smartphones e. Symbian OS and UIQ devices f. Palm OS | |

| | |
|--|--|
| 2. Laptops and Desktops <ul style="list-style-type: none"> a. Microsoft Windows b. Mac OS X 3. Web Browsers <ul style="list-style-type: none"> a. SID Toolbar b. SID Software Token for Web SDK 4. Mobile SDK <ul style="list-style-type: none"> a. iOS b. Android | |
| Software authenticator must support the industry leading Security in Depth (SID) authentication protocol. | |
| Software authenticator must support CT-KIP (Cryptographic Token Key Initiation Protocol) protocol out-of-the-box with no additional customization required. | |
| Up to ten software tokens must be supported on one device. | |
| The "seed record" must be securely stored on smart card and USB devices and used in conjunction | |
| 2.3 On-Demand Authenticator | |
| The on-demand authenticator must support both sms and email as the delivery medium. | |
| 2.4 Risk-based Authentication | |
| The solution must support risk-based authentication based on device identification and user behaviour information captured by SSL VPNs, web portals, OWA and Sharepoint. | |
| The risk engine in the risk-based authentication must provide SMS OTP or challenge questions when assurance level is identified as risky. | |
| 2.5 Partner Authenticators | |
| The 2FA solution must support the following partner authenticators: <ul style="list-style-type: none"> * USB Flash Devices * Biometric Devices * Trusted Platform Modules | |
| 3.0 Authentication Agent | |
| The 2FA solution must provide authentication agents to enable 2FA authentication for different software operating platforms at no additional cost. | |
| The authentication agents must support the following platforms: <ol style="list-style-type: none"> 1. Microsoft Windows <ul style="list-style-type: none"> a. 32 Bit Platforms <ul style="list-style-type: none"> * Windows Server 2008 and up * Windows XP * Windows 7 and up b. 64 Bit Platforms <ul style="list-style-type: none"> * Windows Server 2008 and up * Windows XP * Windows 7 and up 2. Sun Java Web Server 3. Apache Web Server 4. Internet Information Server 5. Red Hat Enterprise Linux Version 4 and above 6. HP-UX 7. Sun Solaris | |

| | |
|--|--|
| <p>8. IBM AIX Version 5.3 and above</p> <p>9. SUSE Linux</p> <p>10. VMware ESX Version 6.0 and above</p> | |
| <p>Authentication agent for Microsoft Windows must provide the following functionality:</p> <ul style="list-style-type: none"> * Local Authentication Client – A component that enforces RSA SecurID authentication during logon to the Windows desktop. * RSA EAP Client – A plug-in into the Microsoft Wireless and VPN client. The plug-in enables RSA SecurID authentication over a VPN, Dial-up or wireless connection established using native Microsoft Wireless and VPN software. The component is supported on the desktop class systems. * Remote Authentication Server – A plug-in into Microsoft IAS RADIUS Server or RRAS. This server-side component enables RSA SecurID authentication using a native Microsoft RADIUS environment. The component is supported on the server class systems. * Online and Offline Authentication - Must provide offline authentication mechanism in case the authentication server is not available. | |
| <p>Authentication agent for Apache Web Server must provide the following functionality:</p> <ul style="list-style-type: none"> * Local, domain, and multi-domain access * Private SSL communication channel between user and web server * Wireless access protocol authentication * Controls user and group access privileges to protected web resources * Provides customizable activity trace/security log, exception, incident, and system usage reports * Uses tamper-evident cookies to prevent cookie alteration or forging <p>Authentication agent for Internet Information Service must provide the following functionality:</p> <ul style="list-style-type: none"> * Local, domain, and multi-domain access * Private SSL communication channel between user and web server * Wireless access protocol authentication * Single sign-on access for Microsoft Outlook Web Access on Microsoft Exchange server 2013 SP1 and 2010 SP3 * Single sign-on access for Microsoft Exchange server 2013 SP1 and 2010 SP3 * Single sign-on access for Microsoft Office Sharepoint Server 2010 and 2013 * Controls user and group access privileges to protected web resources * Provides customizable activity trace/security log, exception, incident, and system usage reports * Uses tamper-evident cookies to prevent cookie alteration or forging | |
| <p>Authentication agent for Unix/Linux must support PAM (Pluggable Authentication Module) and enable 2FA authentication for the following tools and services:</p> <ul style="list-style-type: none"> * login * rlogin * dtlogin * telnet * rsh * su * ftp * sftp | |

| | |
|---|--|
| * ssh * scp | |
| The authentication agent must be protected by a cryptographic algorithm. | |
| 4.0 Administration Module | |
| Administration module must provide the following PIN policy settings: <ul style="list-style-type: none"> * Number of failed authentication attempts before system will lock the user account. * Period of time before systems automatically unlock the user account. * PIN characters requirement. * PIN length. * PIN history (cannot use the same PIN for period of time). * PIN can be randomly generated by authentication server or created by user themselves. * Number of days for offline authentication. | |
| 5.0 Vendor Requirements | |
| The manufacturer must provide a certification that the vendor is an authorized reseller/partner of the proposed product; the manufacturer must also state that the vendor is reseller/partner for 3years. Must submit certifications | |
| Three (3) years warranty on software and must have a local helpdesk to provide a 24x7 technical assistance. Warranty shall also cover any reconfiguration/integration after successful implementation. Must submit warranty certificates and must provide detailes escalation procedure, business continuity plan and support including contact numbers and email addresses. | |
| The vendor shall provide at least two (2) certified engineers of the solution. Must submit certification of certified engineers/s and certificate of employment. | |
| The vendor must have at-least three (3) installed base of similar solution and or equivalent technology like SSL and IPSEC VPN and FTP, one of which a Bank. Must submit list of installed base with client name, contact person, address, telephone number and email address. | |
| Delivery after receipt of NTP: 60 days | |
| Installation will start 1 week after delivery and will end 90 days after. | |