

Addendum to following annexure

[A] Important Dates:

Sr. No.	Particulars	Timeline
1	Last Date & Time of Submission of bids	<b>3:00 PM on 21<sup>st</sup> November 2022</b> Mode: online on URL: <a href="https://www.tenderwizard.com/BOB">https://www.tenderwizard.com/BOB</a>
2	Eligibility Cum Technical Bid Opening Date	<b>4:00 PM on 21<sup>st</sup> November 2022</b> Mode: online on URL: <a href="https://www.tenderwizard.com/BOB">https://www.tenderwizard.com/BOB</a>

Annexure 12 of the RFP - Scope of Work with Technical Requirements Details

B. Technical Specification of Payment HSM

Sr. No.	Clause in RFP	Clarifications / Changes made
1	..... <b>Security Certification:</b> 39. Cryptographic module certified to FIPS: 140-2 Level 3 [certification is must], 46, 81, 180-3, 186-3, 198 .....	..... <b>Security Certification:</b> 39. Cryptographic module certified to FIPS: 140-2 Level 3 [certification is must], <del>46, 81,</del> 180-3, 186-3, 198 .....
2	..... <b>Security Features:</b> 61. Audit trails and 2 Factor Authentication for Auditor using USB tokens .....	..... <b>Security features:</b> 61. Audit trails and 2 Factor Authentication for Auditor using USB tokens <b>or smart cards</b> .....

Sr. No.	Clause in RFP	Clarifications / Changes made
	.....	.....
3	<p><b>Other Features:</b></p> <p>89. Asymmetric public key algorithms: RSA, Diffie Hellman, DSA, KCDSA, ECDSA, ECDH, ECOES</p> <p>.....</p>	<p><b>Other Features:</b></p> <p>89. Asymmetric public key algorithms: RSA, Diffie Hellman, DSA, <b>ECC - as defined in FIPS 186-3 (P-256, P-384 &amp; P-521)</b>, ECDSA, ECDH, ECOES</p> <p>.....</p>
4	<p><b>Other features:</b></p> <p>90. Symmetric algorithms: AES, ARIA, CAST, HMAC, SEED, Triple DES, DUKPT, BIP32</p> <p>.....</p>	<p><b>Other features:</b></p> <p>90. Symmetric algorithms: AES, ARIA, <del>CAST, HMAC, SEED</del>, Triple DES, DUKPT, BIP32</p> <p>.....</p>
5	<p><b>Other features:</b></p> <p>93. Syslog diagnostics support</p> <p>.....</p>	<p><b>Other features:</b></p> <p>93. Syslog <b>or SNMP</b> diagnostics support</p> <p>.....</p>
6	<p><b>Other features:</b></p> <p>103. Should adhere to all major industry standards, including FIPS-140-2 level 3, PCI-DSS, Qualified Signature or Seal Creation Device (QSCD) listing for eIDAS, Common Criteria EAL4+ (AVA_VAN.5 and</p>	<p><b>Other features:</b></p> <p>103. Should adhere to <b>the</b> all-major industry standards, including FIPS-140-2 level 3, PCI-DSS, <del>Qualified Signature or Seal Creation Device (QSCD)</del> listing for eIDAS, <del>Common Criteria EAL4+</del></p>

**Addendum 01 – dated 11<sup>th</sup> November 2022**

<b>Sr. No.</b>	<b>Clause in RFP</b>	<b>Clarifications / Changes made</b>
	ALC-FLR.2) against the protection profile EN 419 221-5 etc. .....	( <del>AVA_VAN.5 and ALC-FLR.2</del> ) against the protection profile EN 419 221-5 etc. .....

All other Terms & Conditions are same as per our Tender No. BCC:IT:PROC:114:41 dated 21<sup>st</sup> October 2022 for Supply, Implementation and Maintenance of Payment Hardware Security Modules (HSM).