भारतीय राष्ट्रीय भुगतान निगम
NATIONAL PAYMENTS CORPORATION OF INDIA

Registered Office - 1001A, B Wing, 10th Floor, 'The Capital', Bandra Kurla Complex, Bandra (E), Mumbai - 400 051

Corrigendum-1

This is with reference to NPCI's RFP no. NPCI/RFP/2021-22/IT/12 dated 17.11.2021- RFP for procurement of Web Application Firewall. The prospective bidders may please note the following changes:

Sr. No.	Document Reference	Description	Existing RFP Clause	Amended clause vide this note
1	Section 1 - Bid Schedule and Address, Sr. no. 6, Page no. 8	Last date and time for Bid Submission	10.12.2021 5.30 pm	**17.12.2021 5.30 pm**
2	Section 8 - Terms and Conditions, Clause No. 8.4, Page No 23	Performance Bank Guarantee	The Successful bidder shall, within 14 working days of receipt of Purchase Order, submit a Performance Bank Guarantee (PBG) equal to 10% of total value of the Purchase order (exclusive of taxes), valid for **1 year**, with a claim period of 12 (twelve) months from the date of expiry of the validity period of the Bank Guarantee (BG), as per statutory provisions in force. In case the successful bidder does not submit the PBG, NPCI shall be entitled to withhold an amount equal to the value of the PBG from the payments due to the successful bidder. PBG may be invoked in case of violation of any of the Terms and Conditions of this Purchase Order and also in case of deficiency of the services provided by successful bidder.	The Successful bidder shall, within 14 working days of receipt of Purchase Order, submit a Performance Bank Guarantee (PBG) equal to 10% of total value of the Purchase order (exclusive of taxes), valid for **3 years**, with a claim period of 12 (twelve) months from the date of expiry of the validity period of the Bank Guarantee (BG), as per statutory provisions in force. In case the successful bidder does not submit the PBG, NPCI shall be entitled to withhold an amount equal to the value of the PBG from the payments due to the successful bidder. PBG may be invoked in case of violation of any of the Terms and Conditions of this Purchase Order and also in case of deficiency of the services provided by successful bidder.
3	Section 9 - Technical Specifications,	SSL/TLS Handling	The solution must support minimum ECC†: 18K TPS (ECDSA P-256) / RSA:18K TPS (2K keys) scalable to ECC†: 34K TPS (ECDSA P-256) / RSA: 34KTPS (2K keys) in	The solution must support minimum ECC†: 18K TPS (ECDSA P-256) / RSA: 18K TPS (2K keys) **per instance** scalable to ECC†: 34K TPS

	Clause 2.9, Page no.37		future. SSL TPS means new SSL handshakes per second without reuse of session key.	(ECDSA P-256) / RSA: 34K TPS (2K keys) in future. SSL TPS means new SSL handshakes per second without reuse of session key.
4	Section 9 - Technical Specifications, Clause 3.51, Page no.40	Web Application Firewall	The solution must be able to decrypt SSL web traffic that are using Diffie-Hellman key exchange protocols with the monitoring appliance deployed in transparent layer-2 mode	Requirement Changed to **Good to Have**
5	Section 9 - Technical Specifications, Clause 3.52, Page no.40	Web Application Firewall	The solution must be able to decrypt SSL web traffic for inspection without terminating or changing the HTTPS connection	Requirement Changed to **Good to Have**
6	Section 9 - Technical Specifications, Clause 3.7, Page no.37	Web Application Firewall	Both Positive and Negative security model should continuously learn the application. Learning should be a continuous process and should not stop after a certain stage. Should provide facility to configure time for staging of policy and policy should move to blocking once staging time is over	Both Positive and Negative security model should continuously learn the application. Learning should be a continuous process and should not stop after a certain stage. Should provide facility to configure time for **staging/simulation** of policy and policy should move to blocking once **staging/simulation** time is over."
7	Section 9 - Technical Specifications, Clause 4.4, Page no.42	Automated threat attacks/BOT Attacks/Application DDOS - Protection, Detection & mitigation	The Solution have below flexible attack mitigation options, a. Blocking of User/session b. Feed Fake Data to Bots c. Captcha Challenge d. Filter the traffic. e. Throttle/Rate based Blocking. f. Session termination g. Redirect loop to the Bad Bot h. Custom business logic	The Solution have below flexible attack mitigation options, a. Blocking of User/session b. Feed Fake Data to Bots c. Captcha Challenge d. Filter the traffic. e. Throttle/Rate based Blocking. f. Session termination g. Redirect loop to the Bad Bot