Request for Proposal (RFP) for Revamping of Load Balancer {LB} with WAF in DC & DR.

Date: 26th Aug 2021

SBICAP Securities Limited (SSL)

Marathon Futurex, 12th Floor, B –Wing,
N M Joshi Marg, Lower Parel,
Mumbai - 400013

SBICAP Securities Limited (SSL)

Marathon Futurex, 12th Floor, B –Wing, N M Joshi Marg,
Lower Parel, Mumbai - 400013

RFP NO. SSL/ITINFRA/RFP-001/2021-22
Date: 26th Aug 2021

Request for Proposal (RFP) for Procurement of LB with WAF

ACTIVITY SCHEDULE

Sr No	Activity	Details
1.	RFP Number	SSL/ITINFRA/RFP-001/2021-22
2.	Bid Document Availability including changes/amendments, if any to be issued	RFP may be downloaded from Company's website https://www.sbisecurities.in/procurement-news
3.	Release of RFP	26th August, 2021
4.	Pre Bid	Queries on email
4.	Technical & Commercial Bid submission	13th Sep, 2021 - 16:00 Hrs
5.	Technical Bid Opening	14th Sep, 2021 - 16:00 Hrs (Tentative Date)
6	Technical Bid Evaluation and Presentation of shortlisted Service Providers	14th Sep, 2021 - 16:00 Hrs (Tentative Date)
7.	Opening of Commercial Bids	15th Sep, 2021 - 16:00 Hrs (Tentative Date)
8.	Method of Selection	The method of selection is Techno-Commercial.
9.	Reverse Auction	17th Sep, 2021 - 16:00 Hrs (Tentative Date)
10.	Bid Submission Contact Details	**IT Department** SBICAP Securities Limited Marathon Futurex, 12th Floor, B Wing, N. M. Joshi Marg, Lower Parel, Mumbai – 400 013. Maharashtra, India. Email ID: SSLIT-Procurement@sbicapsec.com
11	SSL - Contact Details	Mr. Jagjit Singh (Manager- IT) M - 9920253834 email – jagjit.sian@sbicapsec.com Mr. Vishal Singh (AVP- IT) M- 9922001173 email – vishal.singh@sbicapsec.com

Contents

Introduction

1.1 Background

SBICAP Securities Ltd (SSL) is inviting bids from eligible Bidders for Supply, Installation, Configuration, Commissioning and Maintenance of LB & WAF appliances for SSL's Infrastructure at its Primary Site (PR) and Disaster Recovery (DR) Site and various routing and access rules are proposed to be hosted on it. The Bidder should be an authorized partner and competent enough to install, configure, maintain and support the proposed LB & WAF solution setup.

1.2 Invitation of Tender Bids

This RFP is an invitation for bidder responses, No contractual obligation on behalf of the SSL whatsoever shall arise from the RFP process unless and until a formal contract is signed & executed by duly authorized officers of the SSL and the successful bidder. However, until a formal contract is prepared and executed, this offer together with SSL's written acceptance & notification of award shall constitute a binding contract with the successful bidder.

Bidders are expected to examine all instructions, forms, terms, specifications, and other information in the RFP document. Failure to furnish any information required by the RFP document or to submit a bid not substantially responsive to the RFP document in every respect will be at the Bidder's risk and shall result in the rejection of its bid. The procedure and terms & conditions for submission of bid are enumerated in this RFP.

All offers of the bidders shall be unconditional and once accepted whether with or without modifications by SSL shall be binding between the SSL and such Bidder.

2. Eligibility Criteria:

Only those Bidders who fulfill the following criteria are eligible to respond to the RFP. Document/s in support of eligibility criteria are required to be submitted along with the Technical Bid. Offers received from the bidders who do not fulfill any of the following eligibility criteria are liable to be rejected.

1. The bidder should be a company registered in India as per Company Act 1956 /2013 or a partnership firm / a Limited Liability Partnership company under the Limited Liability Partnership Act 2008 in India for last 2 years from the date of RFP. (Certificate of incorporation/Registration is to be submitted).

2. Bidder should have minimum annual turnover of Rs. 50 Crore each during last three financial years (2018-2019, 2019-2020 & 2020-21). This must be the individual company turnover and not that of any group of companies. (Copies of the audited balance sheet and P&L Statement of the company showing the same is to be submitted).

3. The bidder should have positive operating Profit (as EBITDA i.e. Earnings, Before Interest, Tax, Depreciation & Amortization) in the last three financial years, (2018-19, 2019-20, and 2020-21). (Copies of the audited balance sheet and Profit/Loss statement of the firm is to be submitted.)

4. The bidder should be the Authorized Partner / Reseller of the Proposed Solution on the date of RFP, with an authority to sell, upgrade, supply, service and maintain the proposed Solution.

5. The bidder must submit a letter from the OEM confirming the "Back-to-Back" agreement / arrangement for next 3 years to SBICAP Securities Limited, if the contract is awarded to the bidder.

6. The Bidder should be OEM/OSD for Proposed Solution or their authorized channel partners or Service Provider (SP) or System Integrator (SI) in India with an authority to do customization/up-gradation during the period of contract. Bidder needs to provide Manufacturer Authorization Form (MAF) from OEM stating that bidder is authorized partner of OEM and authorized to participate in this tender and in case the bidder is not able to perform obligations as per contract during the contract period, contracted services will be provided by OEM within the stipulated time. Either OEM/OSD or their authorized partner should participate in the RFP. In case, both OEM & his authorized partner participate, only bid of the OEM/OSD will be considered.

7. The bidder must have own/Rented/Registered support offices in India.(Address and Contact details should be submitted)

8. Bidder/OEM must have supplied & implemented the Proposed Solution in Two (2) BFSI during the past 3 years in India. (The bidder has to submit Purchase Order/Satisfactory Certificate from the organization as supporting documents for the same.)

9. The companies or firms, bidding for the above tender, should have not been black listed by any of Government Authority or Public Sector Undertaking (PSUs). The bidder shall give an undertaking (on their letter head) that they have not been black listed by any of the Govt. Authority or PSUs. In case, in the past, the name of their Company was black listed by any of the Govt. Authority or PSUs, the same must have been removed from the black list as on date of submission of the tender, otherwise the bid will not be considered.

Note: Vendor must comply with the above mentioned criteria. Non-compliance to any of the criteria can entail rejection of the offer. Photocopies of relevant documents/certificates should be submitted as proof in support of the claims made for each of the above mentioned criteria. SSL reserves the right to verify/evaluate the claims made by the vendor independently. Any misrepresentation will entail rejection of the offer.

3. Broad Scope of Work

SSL proposes to procure Physical LB & WAF with various security and features as per Annexure –A for DC and movement of existing Physical LB from DC to DR – Hyderabad site with renewal of AMC 1 to 5 years.

The scope of work includes the following but is not limited to:

1. The scope of the work is supply, install, configuration and integration of LB & WAF procured under this RFP with security and it's features to secure & application load balance with existing infrastructure at SSL's DC, Mumbai and DR Hyderabad. The bidder will provide support and maintenance of the LB & WAF during the support period of 3 to 5 year with back to back arrangements with the respective OEMs. Necessary proof for the tie-up arrangements with the OEMs to be provided to SSL.

2. The bidder has to ensure support (24x7 with 30 minutes response & replacement of the appliance within same day)as and when required for resolving all LB & WAF related issues and other required features procured in this RFP, during warranty and ATS (Annual Technical Support) period (or such other extended period as per the contract terms and paid maintenance will commence only thereafter).

3. The warranty & support cost of the LB & WAF will be included in capital cost of the products. The product support period will commence after installation, configuration and sign-off of the project with agreed warranty period.

4. The bidder should be the Premium Business Partner for the last 3 years on the date of RFP, with an authority to sell, upgrade, supply, service and maintain the proposed products.

5. The Bidder will provide the support & service as per **Annexure-A** and Technical Specification for LB & WAF **(Annexure–B)** of the RFP.

6. All the LB & WAF items delivered under this RFP should be covered under comprehensive warranty / ATS except consumables.

7. The major responsibility of the bidder is Supplying, installing, commissioning and maintenance of LB & WAF Solution at SSL's Primary site (Mumbai) and Disaster Recovery Site (Hyderabad). The detail scope covers end to end installation of whole setup and making them operational, imparting training on the same to SSL officials by OEMs.

8. Technical and functional documentation of the entire project should be submitted to SSL in Printed / Digital Book Format.

9. The bidder shall provide perpetual licenses for all LB & WAF components proposed in the solution and should be in name of SSL. The Software licenses proposed for all the components –LB & WAF solution should be independent of hardware.

10. The bidder shall ensure Support & Subscription services from the OEM with unlimited number of support requests, remote support, access to product updates/upgrades and 24x7 supports for all Severity Level issues.

11. The entire LB & WAF supplied under this RFP must be installed and configured by **OEM only**. The bidder to make necessary arrangement for the same and SSL will not pay any additional cost for implementation by OEM.

12. Detailed process documentation, SOP's and management of solution should be created and submitted before project signoff.

4. Locations to be covered

The Proposed solution being procured will be delivered & installed on PR (Primary Data Center) site in Mumbai and Disaster Recovery (DR) Site, Hyderabad. However, SSL reserves the right to change locations/add new locations as per SSL's requirement.

5. Prize Freezing

The prices finalized shall remain valid for 6 months from the date of reverse auction. SSL may place purchase order for additional requirements at the discovered license price through this RFP process within one year from the date of purchase order. However, ATS prices of Software/Hardware etc. will remain valid for 3 years from the date of purchase order.

6. Cost of Bidding

The Bidder shall bear all the costs associated with the preparation and submission of its bid and SSL will in no case be responsible or liable for these costs, regardless of the conduct or outcome of the bidding process.

7. Training

The Bidder will be responsible for training the SSL's employees in the areas of parameterization, implementation, migration, operations, management, error handling, system administration, etc. The training should at least cover the following areas:

1. Functionality available in the solution,
2. New functionality customized (if any),
3. Parameterization,
4. Impact Analysis,
5. Generating various MIS/EIS reports from the solution provided,
6. System and Application administration,
7. Log analysis and monitoring

All the trainings would be held at the appropriate sites (Bidder and SSL premises as identified at the time of training) and the Bidder has to organize the trainer from OEM.

8. Instructions for Bid Submission

8.1 Bid Security/EMD(Refundable)

8.1.1 The bidder should deposit bid security of Rs. 50,000/-(Rupees Fifty Thousand Only) in the form of a demand draft favoring SBICap Securities Limited, payable at Mumbai or Bank Guarantee issued from Scheduled Commercial Bank. Bank Guarantee should be valid for minimum 6 months from the date of issuance of RFP with claim period of 45 days.

8.1.2 EMD should be submitted with Mr. Paren Shah (9892418313) of Procurement Department, IT along with tender documents.

8.1.3 In case of bidders registered with NSIC/MSME, they are eligible for waiver of EMD. However, they need to provide valid NSIC/MSME Certificate clearly mentioning that they are registered with NSIC under single point registration scheme. Other terms & conditions relating to Bid security is as under:

8.1.3.1.1 No interest will be payable on the Bid Security amount.

8.1.3.1.2 Unsuccessful Bidder's Bid security will be returned after completion of tender process.

8.1.4 Bid Security will be forfeited in the following cases:

8.1.4.1.1 If a bidder withdraws its bid during the period of bid validity; or

8.1.4.1.2 If a Bidder makes any statement or encloses any form which turns out to be false / incorrect at any time prior to signing of Contract.

8.1.4.2 In case of any technical issues during reverse auction, if SSL decides to re-conduct reverse auction and any of the shortlisted bidder does not participate in the re-reverse auction at least by way of log in.

8.1.4.3 In case of a successful Bidder, if the Bidder fails:

8.1.4.3.1 To execute Contract within the stipulated time or

8.1.4.3.2 If the bidder refuses to accept the corrections of errors calculated in accordance with the terms of RFP.

8.1.5 The successful Bidders Bid security will be discharged upon the Bidder on Project Signoff.

9. RFP Process

- The technical and commercial proposal with the relevant information/documents/acceptance of all terms and conditions as described in this RFP document will be submitted at the below mentioned Address clearly Mentioning **"Technical Bid for Procurement of LB & WAF"** and Second Envelope Clearly Mentioning **"Commercial Bid for Procurement of LB & WAF".**

IT Department,
SBICAP Securities Limited,
Marathon Futurex, 12th Floor, B Wing, N. M. Joshi Marg, Lower Parel, Mumbai – 400 013. Maharashtra, India.
Email ID: SSLIT-Procurement@sbicapsec.com

- The Bidders will have to submit the duly signed tender documents and all Annexure Forms as part of technical bid.
- Please find below the RFP schedule for submissions and evaluations.

1.	Release of RFP	26th August, 2021
2.	Pre-Bid	Queries on email
3.	Technical Bid submission	13th Sep, 2021 - 16:00 Hrs
4.	Technical Bid Opening	14th Sep, 2021 - 16:00 Hrs (Tentative Date)
4.	Technical Bid Evaluation and Presentation of shortlisted Service Providers	14th Sep, 2021 - 16:00 Hrs (Tentative Date)
5.	Opening of Commercial Bids	15th Sep, 2021 - 16:00 Hrs (Tentative Date)
7.	Reverse Auction	17th Sep, 2021 - 16:00 Hrs (Tentative Date)

- The bidders are requested to note that:

a) They cannot make their submission after the time stipulated above and no extension of time will normally be permitted for submission of bids.
b) It is mandatory to have a valid digital certificate issued by any of the valid Certifying Authority approved by Government of India to participate in the online Reverse Auction. The bidders are requested to ensure that they have the same, well in advance or if any assistance is required for the purpose, Bidders can contact our service provider (M/s e-Procurement Technologies Ltd.).

9.1 List of the Annexures to be submitted online as mentioned below :

S/N	Particulars	Annexure	To be submitted with
1	Bill of Material for LB & WAF	Annexure-A	Technical Bid
2	Technical Specification	Annexure-B	Technical Bid
3	Eligibility Criteria	Annexure-C	Technical Bid
4	Commercial Bid	Annexure-D	Commercial Bid
5	Reverse Auction	Annexure-E	Online
6	Final Price Break-up by L1 vendor	Annexure-F	L1 Bidder
7	Non-Disclosure Agreement (NDA)	Annexure-G	L1 Bidder

9.2 Terms & Conditions :

9.2.1 SSL reserves the right to accept in part or in full or reject the entire quotation and cancel the entire tender, without assigning any reason there for at any stage.

9.2.2 Any terms and conditions from the Vendors are not acceptable to the SSL.

9.2.3 SSL reserves the right to impose and recover penalty from the vendors who violate the terms & conditions of the tender including refusal to execute the order placed on them for any reasons.

9.2.4 Not with standing approximate quantity mentioned in the Tender the quantities are liable to alteration by omission, deduction or addition. Payment shall be regulated on the actual work done at the accepted rates and payment schedule.

9.2.5 The L1 rates finalized discovered will be valid for 06 months and the L1 vendor is bound to execute the orders placed at L1 rates during the duration of the contract.

9.2.6 The prices should be exclusive of all taxes, the vendor should arrange for obtaining of permits wherever applicable.

9.2.7 During the validity period of tender quotes, any upward change in the exchange rate/ excise duty and customs duty are to be borne by the vendor. In the event of any downward revision of levies/duties etc., the same should be passed on to SSL, notwithstanding what has been stated in the quotation or in the Purchase Order.

9.2.8 The Vendor should attach all the related product literature, data sheets, handouts, evaluation reports, Bill of Material etc., pertaining to the Product for which the Vendor has quoted.

9.2.9 SSL may changes the bid evaluation criteria at its own discretion after receipt of bids from competent bidder. SSL also reserves the rights to remove components from Commercial bid for evaluation purpose and for releasing the work order for partial scope.

9.2.10 SSL will notify successful Bidder in writing by way of issuance of purchase order through letter or email that its Bid has been accepted. The selected Bidder has to acknowledge by return email/letter in token of acceptance.

9.2.11 Penalties for Delayed Implementation - The Implementation should be started immediately from the date of Delivery of the Software licenses and/or hardware. If delayed, SSL will charge a penalty of 1% of order value for every week of delay, subject to a maximum of 5% of the order value or will lead to cancellation of the purchase order itself.

9.2.12 Copy of board resolution and power of attorney (POA wherever applicable) showing that the signatory has been duly authorized to sign the acceptance letter, contract and NDA should be submitted.

9.3 Payment Terms:

Payment term	Percent of Overall
60% of PO values for new Hardware, Implementation and 3 Years Warranty	Within 30 days after submission of Invoice with Delivery Challan singed copy.
20% of PO Values for new Hardware, Implementation and 3 Years Warranty	Within 30 Days after submission on Invoice with singed Installation Report
10% of PO Values for new Hardware, Implementation and 3 Years Warranty	Within 30 Days after submission of singed-Off at DC.
10% of PO Values for new Hardware, Implementation and 3 Years Warranty	After Commissioning of 2 no existing LB in DR site and submission of PBG for 3 or 5 years (PBG 10% of PO Values) basis on the Order with 3 or 5 years.
4th and 5th Year AMC cost for new Device and All year AMC cost for existing devices.	Quarterly Arear for each year with fresh renewal of AMC basis on satisfactory of service and support from bidder.

10. Submission of Bids

A two-stage bidding process will be followed for evaluating the bids. The bidders should submit their responses to this RFP in two parts, i.e., first Technical Bid and Commercial Bid and second after techno-commercial evaluation the short-listed bidders will be called for Reverse Auction.

10.1 **Bill of Material for LB & WAF** as detailed in **Annexure - A**

10.2 **Technical Specification** is detailed at **Annexure-B.**

10.3 Bidders Organization Profile Eligibility criteria along with supporting documents as per **Annexure – C**.

10.4 Commercial Bid as per **Annexure - D**.

11. Bid Evaluation Process

11.1 Bidder Eligibility Criteria

11.1.1. Bidder Profile and experience in the industry.

11.1.2. Manufacturer Authorization Form (MAF) from OEM stating that bidder is authorized partner of OEM and authorized to participate in the RFP.

11.1.3. During evaluation and comparison of bids, SSL may, at its discretion ask the bidders for clarification of its bid. The request for clarification shall be in writing and no change in prices or substance of the bid shall be sought, offered or permitted. No post bid clarification at the initiative of the bidder shall be entertained.

11.1.4. SSL reserves the right to evaluate the bids on technical & functional parameters including factory visit, client site visit and witness demos of the system and verify functionalities, response times, public documents, Market Share, OEM establishment blogs. Group Company experience with product etc.

11.2 Commercial evaluation

11.2.1. Technical bids will be opened for eligibility criteria by SSL IT Team.

11.2.2. Technical evaluation will include technical information submitted as per technical Bid format.

11.2.3. Only the bidders who have complied with all the points of Technical Bid shall qualify for Commercial Bid evaluation, accordingly Commercial bids will be opened for Commercial Evaluation. Based on the Commercial Bids, The TPNC will shortlist the bidders for Reverse Auction round.

11.3 Reverse Auction :

11.3.1. All the Bidders who qualify in the techno-commercial evaluation process shall have to participate in the online reverse auction to be conducted by the Authorized service provider on behalf of SSL.

11.3.2. Shortlisted Bidders shall be willing to participate in the reverse auction process and must have a valid digital signature certificate. Bidders shall also be willing to abide by the e-business rules for reverse auction framed by the Authorised service provider. The details of e-business rules, processes and procedures will be provided by the Authorised service provider.

11.3.3. The Bidder will be selected as L1 on the basis of overall price package as quoted in the Reverse Auction.

11.3.4. Final Price Break-up details as per Annexure – F, should be submitted by the successful Bidder by next day of Reverse Auction.

11.3.5. Prices quoted must be "**All Inclusive**" except taxes as applicable.

11.3.6. SSL reserve the complete rights to issue a full or partial purchase order or to subtract any component from the proposed solution/ BILL OF MATERIAL at its own discretion.

12. General Terms & Conditions

12.1 Confidentiality

This document contains information confidential and proprietary to SSL. Additionally, the Bidder will be exposed by virtue of the contracted activities to internal business information of SSL, the Associates, Subsidiaries and/or business partners. The Bidders agree and undertakes that they shall keep confidential all matters relating to this RFP and will not make any disclosure to any person who is under the obligation under this document, any information, data, and know-how, documents, secrets, dealings, transactions or the terms or this RFP (the “Confidential Information”). Disclosure of receipt of this RFP or any part of the aforementioned information to parties not directly involved in providing the services requested could be treated as breach of confidentiality obligations and SSL would be free to initiate any action deemed appropriate.
The restrictions on disclosure of confidential information shall not apply to any matter which is already available in the public domain; or any disclosures made under law.

No news release, public announcement, or any other reference to this RFP or any program there under shall be made without written consent from SSL. Reproduction of this RFP, without prior written consent of SSL, by photographic, electronic, or other means is strictly prohibited.

12.2 Non-Disclosure Agreement

The shortlisted bidder will be required to sign a Non-Disclosure Agreement with SSL. The Bidder shall treat all documents, information, data and communication of and with SSL as privileged and confidential and shall be bound by the terms and conditions of the Non-Disclosure Agreement.

12.3 Governing Law and Jurisdiction

All disputes and controversies arising out of this RFP and related bid documents shall be subject to the exclusive jurisdiction of the Courts in Mumbai and the parties agree to submit themselves to the jurisdiction of such court and the governing law shall be the laws of India.

12.4 Arbitration

All disputes and differences of any kind whatsoever shall be settled by Arbitration in accordance with the provisions of Arbitration and Conciliation Act, 1996 or any statutory amendment thereof. The dispute shall be referred to the sole arbitrator who shall be appointed by SSL. The venue of Arbitration proceedings shall be at Mumbai. The Arbitration proceedings shall be conducted in English Language. The award of the Arbitration shall be final and binding on both the Parties and shall be delivered in Mumbai in the English language. The fees of the Arbitrator and the cost of the Arbitration proceedings shall be equally borne by both the Parties.

12.5 Indemnification

The Bidder shall, at its own cost and expenses, defend and indemnify SSL against all losses, judgments, statutory and regulatory penalties, fines, damages, third-party claims on account of the any misrepresentation, infringement of intellectual property rights, fraud and breach of terms of this RFP/ violation by the Bidder of any or all national/international trade laws, norms, standards, procedures etc.

The Bidder shall expeditiously meet any such claims and shall have full rights to defend itself there from. If SSL is required to pay compensation to a third party on account of the Bidder or association with the Bidder, then the Bidder shall be fully responsible for the same, including all expenses and court and legal fees.

12.6 Force Majeure

In case of delay in implementation of the Project on account of conditions which are beyond the control of the shortlisted bidder such as war, floods, earthquakes, strikes, lockouts, epidemics, pandemic, riots, fire or Governmental regulations superimposed after the date of order/ contract, the Parties shall be permitted to terminate the contract / bid document, if such delay extends for a period beyond 15 days. SSL shall not be liable to make any payments in this case.

12.7 Termination

SSL reserves the right to abandon the current tender process and restart the bidding process at any point of time without assigning any reason whatsoever. SSL can cancel the award granted to the elected Bidder at any point of time and restart the bid process completely or select another Bidder. The Elected Bidders understands and agrees that SSL shall not be obligated in any manner whatsoever and is free to stop / modify the bidding process at any stage without any liability.

12.8 Data Protection

The Bidders authorizes the release from time to time to SSL (and any of its Subsidiaries or Affiliates) all personal or professional data that is necessary or desirable for the administration of the RFP (the “Relevant Information”). Without limiting the above, the bidders permit SSL to collect, process, register and transfer to and aforementioned entities all Relevant Information. The Relevant Information will only be used in accordance with applicable law.

12.9 Intellectual Property

SSL shall have sole exclusive ownership to all its Intellectual property including and not limited to its trademarks, logos etc. This RFP shall in no way be considered as a transfer or assignment of the respective rights over any intellectual property owned, developed or being developed by SSL.

13. Annexure-A : Bill of Material for LB & WAF

Sr. No.	Required Minimum Specification	Compliance (Yes / No)	Remarks
	Platform Architecture & Specifications		
1	The proposed Load Balancer OEM should be in the Gartner's Leaders Magic Quadrant for "Application Delivery Controllers" in all the last three published reports.		
2	The proposed solution shall be dedicated, Purpose built & appliances based Solution from the same OEM. Should be high performance multi-tenant hardware with multicore CPU support. Platform should support multiple network functions including application load balancing, SSL VPN and Web application Firewall. The appliance should capable to upgrade N+1, and the product end of support should not be declare in next 5 years from the date of installation.		
3	The appliance should be populated with 4*10G SFP+ and 4*1G SFP on day 1. Appliance should support 40G QSFP+.		
4	Appliance should support 35 Gbps L7 Throughput.		
5	Appliance should support 15 Gbps bulk SSL encryption scalable to 20 Gbps in future with software license upgrade.		
6	Appliance should support ECC†: 13K TPS (ECDSA P-256) / RSA: 20K TPS (2K keys) scalable to ECC†: 20K TPS (ECDSA P-256) / RSA: 35K TPS (2K keys) in future with software license upgrade.		
7	Appliance should support compression throughput of 12 Gbps & Hardware DDOS protection of 25M SYN cookies/sec scalable to compression throughput of 20 Gbps & Hardware DDOS protection of 50M SYN cookies/sec.		
8	Appliance should support Virtualization or partition upto 8 instances (administrators should be able to run multiple instances of WAF/LB OS, each isolated from the other on purpose built hypervisor) with software license upgrade in future.		
9	Appliance should have integrated redundant hot swappable power supply.		
10	The product should comply and support Dual Stack IPv4 and IPv6 both.		
11	The solution should have support for multiple VLANs with tagging capability.		
12	The device should have support for bonding links to prevent network interfaces from becoming a single point of failure (e.g LACP).		
13	Appliance should support SSL VPN functionality on the same device with license Add-on in future if required.		
	Server Load Balancing features		
14	Solution should support various deployed mode like one-arm mode, routed mode or DSR mode.		
15	Should able to load balance both TCP and UDP based applications with layer 2 to layer 7 load balancing including WebSocket and WebSocket Secure.		
16	The appliance should support server load balancing algorithms i.e. round robin, weighted round robin, least connection, Persistent IP, Hash IP, Hash Cookie, consistent hash IP, shortest response, proximity, SIP session ID, hash header etc.		
17	The proposed solution must support global server load balancing between DC and on premise/cloud based DR and should support following DNS Record type - All (A, AAAA, A6 ,CNAME, DNAME, HINFO, KEY, MX, NS, NXT, PTR, SIG, SOA, SRV, TXR). This feature should be available with license upgrade in future as required.		
18	The appliance should support global server load balancing algorithms including - Weighted round robin, Weighted Least Connections, Administrative Priority, Geography, Proximity.		
19	The Solution should have Dedicated SSL Chipset for SSL Offloading which ensures SSL offloading should be done by dedicated hardware instead of shared CPU. SSL hardware should support both 2048 and 4096 bit keys for encrypted application access.		
20	Should support certificate parser and solution should integrate with client certificates to maintain end to end security and non-repudiation.		
21	The appliance should support Certificate format as "*.PEM", "*.PFX", "*.CER".		
22	Solution shall provide advance health checks based on HTTP, HTTPS and TCP/UDP protocols.		
23	Should support advance ACL's to protect against network base flooding attacks. Administrator should able to define ACL's rules based on connections per second (CPS) and concurrent connections (CC), cookie value. Load balancer should also support Global SYN Check Threshold setting to protect the system against SYN flood attack.		
24	The proposed Load balancer should support ICAP integration with AV and other third party solutions.		
25	The proposed solution must support TCP multiplexing, TCP optimization and dynamic Service chaining for SSL Offload.		
26	It should natively support Geolocation data base without any additional licenses and provide regular updates on OEM's website.		

27	System should support Standard HTTP, Explicit HTTP, and Transparent HTTP profiles natively without need of scripting.		
28	Load balancer should support NodeJS which can be used with native scripting language to give better control on the network traffic.		
29	Load balancer should support creation of Virtual servers which can be categorically offloaded to hardware chipsets. The level of offload to chipset function should also be customizable. This feature should be available with license upgrade in future as required.		
30	Load Balancer should have native MQTT, SIP, Diameter routing agent for optimum control on traffic.		
31	Proposed Solution should support of TLS 1.2 & TLS 1.3.		
32	Proposed Solution should support SSL VPN for Providing secure access to intranet applications from Internet to authorized officials. SSL VPN Client support should be available for IOS, Windows, Android, and Mac.		
Web Application Firewall			
33	The Device should Support below WAF Features with Software License Upgrade/Add-on.		
34	The WAF solution should be in the Gartner's Leaders Magic Quadrant for "Web Application Firewall" for any one year in the last five published reports or should be in the Challengers Magic quadrant of Latest Gartner Report for "Web Application Firewall"		
35	The Solution should meet PCI DSS Compliance as per PCI DSS requirement and should provide reports for PCI DSS compliance.		
36	The solution should address and mitigate the OWASP Top 10 web application/ mobile application security vulnerabilities. (The bidder should describe how each of the OWASP Top 10 vulnerability is addressed by the solution).		
37	The solution should provide OWASP Compliance Dashboard which provides holistic and interactive interface that clearly measures app's compliancy against the OWASP Application Security Top 10 and also provide suggestions/shortcuts to address the compliances and configure policies for it.		
38	When deployed as a proxy (either a transparent proxy or a reverse proxy), the Web application firewall should be able to digitally sign cookies, encrypt cookies, and to rewrite URLs.		
39	The Proposed WAF Solution should support both a Positive Security Model and a Negative Security Model and also should provide regular update for CVE signatures.		
40	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.		
41	The solution must support and integrate with the following web application vulnerability assessment tools (Web application scanners) at minimum to virtually patch web application vulnerabilities: White hat Sentinel, IBM Appscan, Rapid7 and QualysGuard, for rapid virtual patching.		
42	The solution must support user tracking using both form-based and certificate-based user authentication. Solution should support API security including support for uploading swagger file.		
43	The solution must be able to validate encoded data in the HTTP traffic		
44	The solution must be able to identify Web Socket connections and provide security for WebSocket including exploid against Server abuse, login enforcement, XSS and SQL injection.		
45	The solution must support the configuration to allow some pages in a web application to be in blocking mode and some pages to be in detection\learning mode.		
46	The XML protection offered by the solution must be similar to the web application protection provided with automated profiling/learning capability.		
47	The solution must be able to perform profiling of JSON. HTTP requests in the JSON format must be learnt by the WAF with the parameters and values.		
48	The solution must allow the re-learning of an application profile on a per-URL or per-page basis. The administrator should not be required to relearn the entire application when only a few pages have changed.		
49	The Proposed WAF Solution should have capability to mitigate, learn and adapt to unique application layer user interaction patterns to enable dynamic defences based on changing conditions		
50	The Proposed WAF Solution should have Correlated Attack Validation capability or Correlation features which examines multiple attributes such as HTTP protocol conformance, profile violations, signatures, special characters, and user reputation, to accurately alert on or block attacks and also to eliminate false positives.		
51	The Proposed WAF Solution should support custom security rules. Administrators should be able to define rules for the positive or negative security model and to create correlation rules with multiple criteria.		
52	The Proposed WAF Solution Should support ICAP integration with other security devices for file scanning.		

53	The Proposed WAF Solution should accurately distinguish incoming traffic between human and bot traffic, identify “good” and “bad” bots; classify traffic by browser type, etc. It should have capability of BOT detection and Protection beyond signatures and reputation to accurately detect malicious and benign bots using client behavioural analysis, server performance monitoring, and escalating using JavaScript, Image and Sound CAPTCHA challenges. This information should drive WAF policy enforcement decisions, including handling bad and suspected bots. Administrators should also receive an alert (e.g. for monitoring purposes), or have capability to block the bot.		
54	It should provide advanced BOT detection mechanism based on smart combination of signature-based and heuristic behaviour analysis, reverse DNS lookup.		
55	The Web Application Firewall should have "Anti-Automation" protection which can block the automated attacks using hacking tools, scripts, frame work etc.		
56	The Proposed WAF Solution should have Threat Intelligence to Identify New Attack Vectors.		
57	The Proposed WAF Solution should provide built-in L7 layer DDoS detection and mitigation features based on machine learning and behavioural analytics and dynamic signatures. It should have CAPTCHA support or other mechanism to avoid distributed attack.		
58	Solution should support Behavioural L7 DDoS mitigation to detect attacks without human intervention.		
59	Proposed solution should have capability to redirect Brute force attack traffic to Honey Pot page.		
60	The Proposed WAF solution must provide capabilities to obfuscate sensitive field names to defeat Man-in-The-Browser Attacks		
61	The Proposed WAF Solution must have an option to receive Spam IP Feed to Block IPs to reduce spam messages.		
62	The Proposed WAF Solution should Identify and limit / block suspicious clients, headless browsers and also mitigate client-side malwares		
63	The Proposed WAF Solution should protect API based communication between client & servers using all the relevant WAF signatures.		
64	Should provide encryption for user input fields to protect from browser based malwares stealing users credentials		
65	Solution should have the ability to build a base policy and inherit child policies from the same. Inheritance should support restricting modifications to the base policy settings		
66	On detecting an attack or any other unauthorized activity, the Web application firewall must be able to take the appropriate action. Supported actions should include the ability to drop requests and responses, block the TCP session, block the application user, or block the IP address. For particularly destructive attacks, the Web application firewall should be able to block the user or the IP address for a configurable period of time.		
67	The solution must allow administrators to add and modify signatures.		
68	Proposed Solution should have ability of HTTP response logging.		
69	Proposed Solution should have ability dynamically generate signatures for L7 DoS attacks.		
70	Proposed solution should be able to track unused elements in the policy and suggest to remove them after a specified period of time		
71	Proposed Solution should have ability to automatically detect software technology used on backend side to define signature sets required for defined Proposed Solution policy.		
72	Proposed Solution should have ability to configure way to analyse request payload based on custom rules for each URL entry configured in the security policy		
73	Proposed Solution should be able to track application changes over time and adjust config elements and rules based on that data.		
74	The solution must support regular expressions for the following purposes: Signatures definition, Sensitive data definition, Parameter type definition, Host names and URL prefixes definition, Fine tuning of parameters that are dynamically learnt from the web application profile.		
75	The WAF instance should have option to enable x-forwarder option per service to log actual client IP in webserver logs even deployed in Reverse Proxy mode.		
76	Separate policies should be applied for different applications configured on the same WAF		
77	The solution should have pre-built templates for well-known applications eg, ActiveSync, SAP, Oracle Applications/Portal . Solution should have the ability to build a base policy and inherit child policies from the same. Inheritance should support restricting modifications to the base policy settings		
78	The solution should also support sending of logs in CEF (Common Event Format) standard		

79	Proposed solution should support multiple administration domains (or partitions) to configure and administer the system. This would include support for using remote authentication servers (e.g. LDAP, Windows AD, RADIUS and TACACS+) to store system user accounts.		
80	Proposed Solution should have Role-based management with user authentication. There should be web application security administrator whom has access to web security policy objects in web profile, modify web profiles but cannot create or delete those profiles, and web application security editor (similar) whom configure or view most parts of the web security policy object in specific controlled partition holding the policy and profile objects.		
81	Organization should be able to deploy or remove the Web application firewall from the network with minimal impact on the existing Web applications or the network architecture.		
82	Native support for Geolocation data base without need of additional licenses		
83	Proposed WAF Solution should have capability to automatic learning should include Directories, URLs, Form Field Values, Whether the field values is numeric/alphanumeric/alphabets, length of the field etc.		
84	Proposed WAF Solution should have functionality to showcase how many URLs in the application have been completely learned & move them into Protection Mode automatically i.e. some URLs to be in learning mode & some URLs in the Protection Mode of the same Application		
85	Proposed WAF Solution should have capability to learn changes in the already integrated Web Application & protect it at the same time i.e. solution should be able to learn changes in the application in the Protection Mode		
86	Proposed WAF Solution should have capability to allow / deny access to specific Applications / URLs to Specific Country. Application specific geo-based policies should be allowed to be configured		
87	Proposed WAF Solution should have BOT Protection & it should not be limited to reputation-based/ signature-based controls		
88	Proposed WAF Solution should be able to provide a threat intelligence feed and service for bots protection & should be able to carry out Bot Classification of traffic into humans, Trusted Bot, Bad Bot, General Bot and Unknown new bot - Bot Type: Click Bot, Comment Spammer Bot, Crawler, Feed Fetcher, Hacking Tool, Masking Proxy, Search Bot, Spam Bot, Vulnerability Scanner, Worm, Site Helper and DDoS Tool		
High Availability			
89	The Proposed Solution should be able to work in High Availability (HA) mode and should be deployable in an Active-Standby & Active-Active in both DC & DR.		
90	Should support transparent failover between 2 devices, the failover should be transparent to other networking devices with SSL session mirroring.		
91	Should support network based failover for session mirroring, connection mirroring and heartbeat check		
92	Device level HA should support automatic and manual synchronization of configuration from primary device to secondary device.		
Monitoring & Logging			
93	Solution must support SNMPv3, Syslog.		
94	System must support external authentication including LDAP, TACACS+, RADIUS.		
95	Easy-to-use graphical user interface for visualization and top-level management, also the device console or CLI should be easily accessible if needed.		
96	Should support SSHv3 and HTTPS access.		
97	Should have ability to upgrade/downgrade device software Images.		
98	Proposed solution should also integrate with SIEM solutions.		
Support			
99	The OEM should have a Technical Assistance Center (TAC) which Follow the Sun Model with India Toll Free Numbers.		
100	The OEM should have Support Centers / Service Center or 24x7x365 TAC Support.		
101	The Proposed WAF Solution should be provided with hardware replacement warranty and Ongoing Software Upgrades for all major and minor releases during the completion of project.		
102	OEM should have Local Stocking of Spares within the Country to ensure that the SLA is not breached.		
103	RMA 4 hours and 24*7 TAC Premium Support for 3 Years for DC and DR both.		
104	RMA 4 hours and 24*7 TAC Premium Support for 4th and 5th Years for DC and DR both.		
105	Movement of existing 2 nos load balancer appliances to DR-Hyderabad, installation and Warraty pack with new LB & WAF 3+2 years		
106	Training from the OEM for 3 Persons		

Note: The commercials for the above Bill of Material shall be "**Inclusive of All**" except applicable Taxes and government levies.

14. Annexure-B: Technical Specification.

For New Appliance (LB & WAF) and AMC of Existing 2 nos Appliance					
Sr. No.	Product Code	Product Description	Qty	Cost	Remarks

15. Annexure – C: Compliance for Eligibility Criteria

(to be printed on Bidder's Letter Head and included with the Technical Bid Envelope)

#	Eligibility Criteria	Compliance (Compliant/Not Compliant)	Supporting Evidence
1.	The Bidder should be a current legal entity with a minimum 3 years of experience in India.	Y/N	Certificate of Incorporation or Appropriate Supporting Document
2.	Bidder/OEM must have supplied & implemented ITSM Tool suite Solutions in Two (2) BFSI during the past 3 years in India.	Y/N	Customer references to be provided & Copies of Purchase Orders
3.	The Bidder should be OEM/OSD for proposed solution or their authorized channel partners or Service Provider (SP) or System Integrator (SI) in India with an authority to do customization/up-gradation during the period of contract. Bidder needs to provide Manufacturer Authorization Form (MAF) from OEM stating that bidder is authorized partner of OEM and authorized to participate in this RFP	Y/N	Manufacturer Authorization Form (**MAF**) from OEM
4.	The service provider shall not assign or sub-contract the assignment or any part thereof to any other person/firm.	Y/N	Self-Declaration
5.	The bidder should be a company registered in India as per Company ACT 1956. The bidder should have experience of minimum two years in Supply of proposed solution in India.	Y/N	Incorporation Certificate
6.	The Bidder's Account should not have been declared as a Non-Performing Asset (NPA) in the Books of any bank or financial institution as on 31.03.2020.	Y/N	Certificate from Bank/ Auditor
7.	The bidder must submit an undertaking that no Government / undertaking organizations have blacklisted the bidder for any reason. Past/present litigations, disputes, if any (Adverse litigations could result in disqualification, at the sole discretion of the SSL)	Y/N	Undertaking by Bidder.
8	Minimum Annual Turnover should be INR 50 Crores in each of the Preceding three financial years.	Y/N	Auditors Certificate or CA certificate
9	Financial statements i.e. Audited Balance sheet and Profit & Loss accounts for last three years (FY2017-18, FY2018-19 and FY2019- 20)	Y/N	Auditors Certificate or CA certificate
10	The participant should be a profit-making entity for minimum of Preceding Three years. It should not have incurred / reported losses during any of the last Three financial years.	Y/N	Appropriate Supporting Document
11	An undertaking that, no penalties/fines have been imposed on their entities by any Regulator or Govt Agency or any Authority for breach of any Regulations or Laws.	Y/N	Supporting Document
13	The Bidder should have permanent office in India	Y/N	Appropriate Supporting Document

16. Annexure D: Commercial Bid (Mentioned amount are only for example) the Proportion should be define into pre-bid quotation for each line items.

Sr. No	Detailed Description	Indicative Price BID Quote (INR)	Proportion to total Cost in % of indicative price BID
	A	B	C
1	Product Cost	12518400	33.56%
2	First year warranty	2443680	6.55%
3	Second Year Warranty	2443680	6.55%
4	Third Year Warranty	2443680	6.55%
5	One time Implementation cost	350000	0.94%
6	4th Year AMC	2443680	6.55%
7	5th Year AMC	2443680	6.55%
8	Existing Device AMC From 2021 - 2022	2443680	6.55%
9	Existing Device AMC From 2021 - 2022	2443680	6.55%
10	AMC From 2023 - 2024	2443680	6.55%
11	AMC From 2024 - 2025	2443680	6.55%
12	AMC From 2025 - 2026	2443680	6.55%
Pre-Bid Total		**37305200**	**100.00%**

Note: The commercials for the above Bill of Material shall be “**Inclusive of All**” except applicable Taxes and government levies.

17. Annexure E: Reverse Auction – Overall Package Price (Mentioned amount are only for example) Post bid final price. The percentage will be same from per-bid quotation for each line items.

To arrive at L-1 bidder, Revers Auction will be conducted for the overall package price as shown below:

Sr. No	Detailed Description	Final Price BID Quote (INR)	Proportion to total Cost in % of price after BID
	A	B	C
1	Product Cost	3356000	33.56%
2	First year warranty	655000	6.55%
3	Second Year Warranty	655000	6.55%
4	Third Year Warranty	655000	6.55%
5	One time Implementation cost	94000	0.94%
6	4th Year AMC	655000	6.55%
7	5th Year AMC	655000	6.55%
8	Existing Device AMC From 2021 - 2022	655000	6.55%
9	Existing Device AMC From 2021 - 2022	655000	6.55%
10	Existing Device AMC From 2021 - 2022	655000	6.55%
11	Existing Device AMC From 2021 - 2022	655000	6.55%
12	Existing Device AMC From 2021 - 2022	655000	6.55%
Post Bid final cost		**10000000**	**100.00%**

Note: The commercials for the above overall package shall be “**Inclusive of All**” except applicable Taxes and government levies.

18. Annexure F: Final Price Break-up: To be submitted by the L1 Vendor (Post Bidding) – Bidder have flexibility to modify the line item price with +/- 5% in post bid cost.

Sr. No	Detailed Description	Price post BID Quote (INR)
	A	B
1	Product Cost	
2	First year warranty	
3	Second Year Warranty	
4	Third Year Warranty	
5	One time Implementation cost	
6	4th Year AMC	
7	5th Year AMC	
8	Existing Device AMC From 2021 - 2022	
9	Existing Device AMC From 2021 - 2022	
10	Existing Device AMC From 2021 - 2022	
11	Existing Device AMC From 2021 - 2022	
12	Existing Device AMC From 2021 - 2022	
Total Cost for New Product, Warranty and implementation and AMC of existing 2 no Load Balancer		

Note: The commercials for the above Bill of Material shall be “**Inclusive of All**” except applicable Taxes and government levies.

19. Annexure – G: Non-Disclosure Agreement (NDA)

(to be printed on Bidder's Letter Head and included with the Technical Bid Envelope)

THIS AGREEMENT ("**the Agreement**") is made on this _____day of __________, 2020.

BETWEEN

SBICAP Securities Limited, an Indian company duly incorporated under the Companies Act, 1956, having its registered office at Marathon Futurex, 12th Floor, A & B Wing, Mafatlal Mill Compound, N. M. Joshi Marg, Lower Parel, Mumbai – 400 013 (hereinafter for the purposes of this agreement, referred to as **"SSL"/ "Disclosing Party"**), which expression shall, unless repugnant to the context or meaning thereof, be deemed to mean and include its successors and permitted assigns;

AND

________________________LIMITED, a company incorporated Registered under the Companies Act, 1956 and having its registered office at ____ ____________ in (hereinafter referred to as the "Receiving Party"), which expression shall, unless repugnant to the context or meaning thereof, be deemed to include its successors and permitted assigns)

WHEREAS:

1. SSL is registered with SEBI as a Stock Broker and a Depository Participant and distributing third party financial products including mutual funds/Tax Free bonds and is registered with Association of Mutual Funds in India (AMFI).
2. **The Receiving Party** is engaged in the business of ______________________________.
3. **SSL** and **the Receiving Party** are in the process of discussion and negotiation wherein **SSL** will provide its Information related to Systems, Device, Applications, logs, etc. ("Information") to the **Receiving Party** and may in the course of discussion, negotiation and/or performance of the said Services, disclose, provide or make available to **the Receiving Party** certain Confidential Information as defined herein below; and
4. **SSL** desires to restrict use and disclosure of such Confidential Information as set out herein below.

NOW THEREFORE in consideration of the mutual promises and covenants contained in this Agreement, and the mutual disclosure of Confidential Information to each other, the Parties hereto agree as follows:

1. Confidential Information and Confidential Materials

(a) "Confidential Information" means non-public information that **SSL** designates as being confidential or which under the Confidential Information circumstances surrounding disclosure ought to be treated as confidential. "Confidential Information" includes, without limitation, information relating to released or unreleased SSL's services or products, the marketing or promotion of any **SSL** Product, SSL's business policy, Confidential Information or practices, and information received from others that **SSL** is obligated to treat as confidential. Confidential Information disclosed to the Receiving Party by any parent or agent of **SSL**, or by any subsidiary of parent of **SSL,** is covered by this Agreement.

(b) Confidential Information shall not include any information that: (i) is or subsequently becomes publicly available without the Receiving Party's breach of any obligation owed to **SSL**; (ii) became known to the Receiving Party prior to **SSL**'s disclosure of such information to the Receiving Party; (iii) became known to the Receiving Party from a source other than the breach of an obligation of confidentiality owed to SSL; (iv) is independently developed by the Receiving Party.

(c) "Confidential Materials" shall mean all tangible materials containing Confidential Information, including without limitation, written or printed documents and computer disks or tapes, whether machine or user readable, the Software being licensed including any manual and documents relating to the Software, its Source Code, etc.

2. Restrictions

(a) Except as provided below, the Receiving Party shall not disclose any Confidential Information to third parties. However, the Receiving Party may disclose Confidential Information in accordance with judicial or other governmental order, provided the Receiving Party shall give SSL reasonable notice prior to such disclosure and shall comply with any applicable protective order or equivalent. This restriction on disclosure of Confidential Information shall apply to all the Confidential Information disclosed before entering the service agreement and shall continue to have effect during the subsistence of the Service Agreement. It shall also survive the termination of such agreement for provision of the services, as set out in the recitals hereinabove.

(b) The Receiving Party shall take reasonable security precautions, at least as great as the precautions it takes to protect its own confidential information, to keep confidential the Confidential Information. The Receiving Party may disclose Confidential Information or Confidential Material only to the Receiving Party's employees or consultants on a need-to-know basis. The Receiving Party will have executed or shall execute appropriate written agreements with its employees and consultants sufficient to enable it to comply with all the provisions of this Agreement

(c) Confidential Information and Confidential Materials may be disclosed, reproduced, summarized or distributed only in pursuance of the Receiving Party's business relationship with SSL, and only as otherwise provided hereunder. The Receiving Party agrees to segregate all such Confidential Materials from the confidential materials of others in order to prevent commingling.

(d) Publications: the Receiving Party shall not make any news releases, public announcements, give interviews, issue or publish advertisements or publicize in any other manner whatsoever in connection with this Agreement, the contents / provisions thereof, other information relating to this Agreement, the Purpose, the Confidential Information or other matter of this Agreement, without the prior written approval of the SSL.

3. Rights and Remedies

(a) The Receiving Party shall notify SSL immediately upon discovery of any unauthorized use or disclosure of Confidential Information and/or Confidential materials, or any other breach of this Agreement by the Receiving Party, and will co-operate with SSL in every reasonable way to help SSL to regain possession of the Confidential Information and/or Confidential Materials and prevent its further unauthorized use.

(b) The Receiving Party shall return all originals, copies, reproductions and summaries of Confidential Information or Confidential Materials at SSL's request, or at SSL's option, certify destruction of the same.

(c) The Receiving Party acknowledges that monetary damages may not be a sufficient remedy for unauthorized disclosure of Confidential Information or Confidential Materials and that SSL shall be entitled, without waiving any other rights or remedies, to such injunctive or equitable relief as may be deemed proper by a court of competent jurisdiction.

4. Miscellaneous

(a) All Confidential Information and Confidential Materials are and shall remain the property of SSL or any affiliate thereof. By disclosing information to the Receiving Party, SSL and/or its affiliate(s) do not grant any express or implied right to the Receiving Party to or under any patents, copyrights, trademarks, or trade secret information.

(b) Any software, product, service and documentation provided under this Agreement is provided with RESTRICTED RIGHTS.

(c) Terms of confidentiality under this Agreement shall not be construed to limit either party's right to independently develop or acquire products without use of other party's Confidential Information. Further, either party shall be free to use for any purpose the residuals resulting from access to or work with such Confidential Information, provided that such party shall maintain the confidentiality of the Confidential Information as provided herein. The term "residuals" means information in non-tangible form, which may be retained by persons who have had access to the Confidential Information, including the ideas, concepts, know-how or techniques contained therein. Neither party shall have any obligation to limit or restrict the assignment of such persons or to pay royalties for any work resulting from the use of residuals. However, the foregoing shall not be deemed to grant to either party a license under the other party's copyrights or patents.

(d) This Agreement constitutes the entire agreement between the parties with respect to the subject matter hereof. It shall not be modified except by written agreement dated subsequent to the date of this Agreement and signed by both Parties. None of the provisions of this Agreement shall be deemed to have been waived by any act or acquiescence on the part of SSL, its agents, or employees, but only by an instrument in writing signed by an authorized officer of SSL. No waiver of any provision of this Agreement shall constitute a waiver of any other provision(s) or of the same provision on another occasion.

(e) This Agreement shall be governed by and construed in accordance with the laws of India and shall be subject to the exclusive jurisdiction of the courts of Mumbai.

(f) Subject to the limitations set forth in this Agreement, this Agreement will inure to the benefit of and be binding upon the Parties, their successors and assigns.

(g) If any provision of this Agreement shall be held by a court of competent jurisdiction to be illegal, invalid or unenforceable, the remaining provisions shall remain in full force and effect.

(h) All obligations created by this Agreement shall survive change or termination of the parties' business relationship.

(i) In the event this Agreement (including any schedules, exhibits or attachments hereto) is signed in both the English language and in any another language, any conflict or inconsistency between the different language versions shall be resolved solely by reference to the English language version.

5. Arbitration

All the disputes in connection with this Agreement, the construction of any provision of this agreement or the rights, duties or liabilities of the parties hereto under this Agreement shall be amicably settled. However, in the event of any such disputes are not settled amicably between the Parties, reference shall be to three arbitrators. Each party shall appoint its Arbitrator and the two respective Arbitrators appointed by each party shall appoint a presiding Arbitrator to adjudicate the dispute, difference, claim, etc. between the parties. A Party wishing to refer a dispute to arbitration shall appoint its arbitrator and send notice of such appointment in writing to the other party requiring the other party to appoint its own arbitrator within 30 calendar days of that notice and stating that it will appoint its arbitrator as sole arbitrator unless the other party appoints its own arbitrator and gives notice that it has done so within the 30 days specified above. If the other party does not appoint its own arbitrator and give notice that it has done so within the 30 days specified, the Party referring a dispute to the arbitration may, without the requirement of any further prior notice to the other party, appoint its arbitrator as sole arbitrator and shall advise the other party accordingly. The award of such sole arbitrator shall be binding on both parties as if he had been appointed by agreement.

The arbitration will be held **in Mumbai, India** and will be conducted in the English language.

IN WITNESS WHEREOF, THE PARTIES HERETO HAVE CAUSED THIS AGREEMENT TO BE EXECUTED AS OF THE DAY AND YEAR FIRST ABOVE WRITTEN

SIGNED AND DELIVERED)
For SBICAP Securities Limited)

)
in the presence of:)
)

1.
2.)
SIGNED AND DELIVERED)
For ________________________________Limited)
in the presence of:)

1.)
2.)