

**IT DEPARTMENT
CORPORATE OFFICE,
DHANLAXMI BANK LIMITED
NAICKANAL, THRISSUR - 680001**

REQUEST FOR PROPOSAL

**NETWORK ADMISSION CONTROL (NAC) SOLUTION IMPLEMENTATION AND
SUPPORT**

RFP No: DLB_IT/ RFP/ 2018-19/ 001

Version 1.03

29th Dec, 2018

Corrections and Modifications
Version 1.03
Page 14 - Section 11 - WARRANTY & SUPPORT
60 Months i.e. Five Year (5)

RFP Details in Brief.

RFP No. and date	RFP No: DLB_IT/ RFP/ 2018-19/ 001
Brief Description of the RFP	Network Admission Control (NAC) Solution Implementation and Support
Bank’s Address for Communication	Head-IT & Digital Banking IT Department 4th Floor, Corporate Office Dhanlaxmi Bank Naickanal, Thrissur Kerala – 680001
e-mail for Submission of Tender	biju.kf@dhanbank.co.in
Contact Details	Biju KF IT Department 4th Floor, Corporate Office Dhanlaxmi Bank Naickanal, Thrissur Kerala - 680001 Ph: +91 487 6627067 e-mail:biju.kf@dhanbank.co.in
Date of Issue	29/12/2018
Last date of submission of any queries, clarifications etc.	09/01/2019, 05:00 PM
Last Date of submission of RFP response as soft copy	23/01/2019, 05:00 PM

DISCLAIMER

The information contained in this Request for Proposal (“RFP Document”) or information provided subsequently to bidder(s) or applicants whether verbally or in documentary form by or on behalf of Dhanlaxmi Bank Limited, is provided to the bidder(s) on the terms and conditions set out in this RFP document and all other terms and conditions subject to which such information is provided.

This RFP document is not an agreement and is neither an offer. The purpose of this RFP is to provide applicants who are qualified to submit the bids (“Bidders”) with information to assist them in formulation of their proposals (“Bids”). This RFP does not claim to contain all the information each Bidder may require. Each Bidder may conduct its own independent investigations and analysis and is free to check the accuracy, reliability and completeness of the information in this RFP. Bank makes no representation or warranty, express or implied, and shall incur no liability whatsoever under any law, statute, rules or regulations as to the accuracy, reliability or completeness of this RFP. Bank may in its absolute discretion, but without being under any obligation to do so, update, amend or supplement the information in this RFP.

The information contained in the RFP document is selective and is subject to update, expansion, revision and amendment. Dhanlaxmi Bank does not undertake to provide any Bidder with access to any additional information or to update the information in this RFP or to correct any inaccuracies therein, which may become apparent. Dhanlaxmi Bank reserves the right of discretion to change, modify, add to or alters any or all of the provisions of this RFP and/or the bidding process, without assigning any reasons whatsoever. Such change will be intimated or made accessible to all Bidders. Any information contained in this document will be superseded by any later written information on the same subject made available/accessible to all recipients by Dhanlaxmi Bank.

Information provided in this RFP is on a wide range of matters, some of which may depend upon interpretation of law. The information given is not intended to be an exhaustive account of statutory requirements and should not be regarded as a complete or authoritative statement of law. Dhanlaxmi Bank does not own any responsibility for the accuracy or otherwise for any interpretation or opinion on law expressed herein. Further, Dhanlaxmi Bank also does not accept liability of any nature whether resulting from negligence or otherwise howsoever caused arising from reliance of any Bidder upon the statements contained in this RFP

Dhanlaxmi Bank reserves the right to reject any or all the responses to RFPs / Bids received in response to this RFP at any stage without assigning any reason whatsoever and without being liable for any loss/injury that Bidder might suffer due to such reason. The decision of Dhanlaxmi Bank shall be final, conclusive and binding on all the parties directly or indirectly connected with the bidding process.

It may be noted that notice regarding corrigenda, addendums, amendments, time-extensions, clarifications, response to bidders' queries etc., if any to RFP, will not be published through any advertisement in newspapers or any other media. Prospective bidders shall regularly visit Bank's website for any changes / development in relation to this RFP.

Table of Contents

1. INTRODUCTION	7
2. REQUIREMENT	8
3. SCOPE OF WORK AND SOLUTION	8
4. IT SYSTEM CONFIGURATION AND IMPLEMENTATION SERVICES	11
5. TRAINING SERVICES	11
6. PROJECT MANAGEMENT SERVICES	11
7. SUPPORT –TERMS AND CONDITIONS.....	12
8. SERVICE LEVEL EXPECTATIONS.....	13
9. SCHEDULE.....	13
10. RESPONSIBILITIES OF BIDDER.....	14
11. WARRANTY & SUPPORT.....	14
12. PENALTIES	14
13. COMMISSIONING TIME	15
14. ACCEPTANCE TEST.....	15
15. OBSOLESCENCE.....	15
16. INSTRUCTION TO BIDDERS.....	15
17. BIDDING PROCESS	16
18. MODIFICATION OF BIDS & CONTACTING THE DLB	16
19. TERMS & CONDITIONS OF THE BIDDING FIRMS	16
20. SYSTEM DEMONSTRATION/PROOF OF CONCEPT	16
21. DOCUMENTATION	17
22. ELIGIBILITY CRITERIA FOR BIDDER/OEM	17
23. DLB’S RIGHT TO ACCEPT OR REJECT ANY BID OR ALL BIDS.....	18
24. EVALUATION, AWARD CRITERIA & INSTRUCTIONS	18
25. CONFIDENTIALITY.....	21
26. PATENT RIGHTS.....	22
27. SIGNING OF CONTRACT.....	22

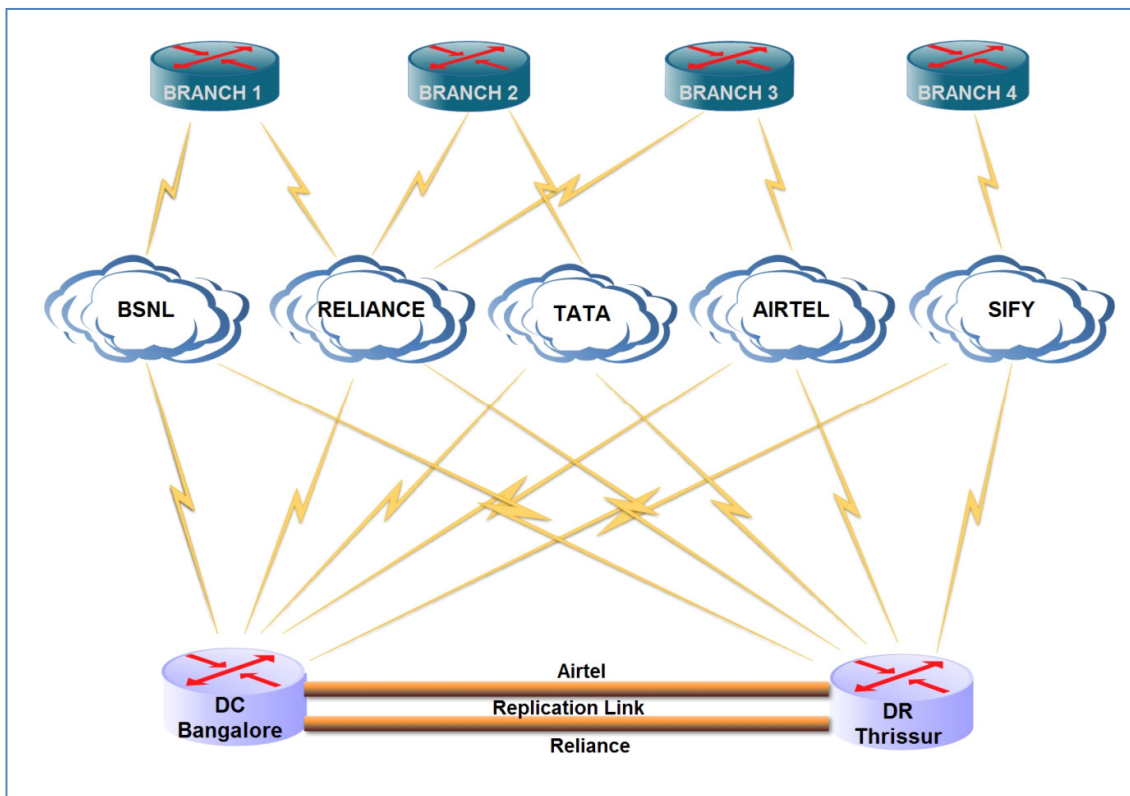
28.	PAYMENT TERMS.....	22
29.	SUBMISSION OF BID	24
30.	CLARIFICATIONS REGARDING RFP DOCUMENT.....	24
31.	IMPORTANT DATES	24
32.	EXECUTION OF AGREEMENT	25
33.	ANNEXURES	25

1. INTRODUCTION

Incorporated in November 1927 , Dhanlaxmi Bank (here in after known as “DLB”) headquartered at Thrissur in Kerala, Became a Scheduled Commercial Bank in the year 1977. DLB currently having more than 260 branches spread across India, which are connected by MPLS . Most of these locations are connected with more than one MPLS link from different service provider and network routing established with BGP. Branch locations are having the bandwidth capacity form 256 Kbps to 2Mbps depends upon the size of the particular branch and bandwidth availability.

DLB has state of the art Data Centre (DC) hosted at Nxtra Data Ltd (Bharthi Data Centre Managed Services) Bangalore and disaster Recovery (DR) site at Thrissur, Kerala. DLB has implemented Flexcube Core Banking Solution (CBS) in all the branches in India.

Below shows DLB high level WAN diagram.



2. REQUIREMENT

The purpose of this RFP is to invite bids from vendors for procurement and implement Network Access Control (NAC) Solution for DLB as per Scope of work and Technical Specifications given in this document.

3. SCOPE OF WORK AND SOLUTION

The Bidder shall supply, install, customize, implement, integrate and support the Network Access Control Solution (NAC) at DLB's DC at Bangalore, DRC at Thrissur and NAC agents across all remote locations of the DLB. Successful bidder will supply and install the solution as per the broad objectives as given in this RFP. The support for the solutions shall be for a period of 5 years from the date of completion to successful Go Live, with 3 years of warranty and 2 years of additional AMC.

1. Providing the solution would cover supply, installation and operationalisation of the NAC hardware, all necessary application software and maintenance of the equipment supplied for a period of Five year warranty/support (including hardware, system and application software etc.) with back to back support from the OEM. The new systems provided should integrate well with the existing IT and Network facility at the DLB
2. Successful bidder will take total responsibility for supply and delivery, transportation, transit insurance, storage, insurance up to acceptance by the DLB, installation and commissioning of the devices at sites including integration, acceptance testing, configuration of supplied equipment in DLBs existing environment. Integration involves changes need to be made in configuration of the supplied equipment to enable all the functional features to work in tandem with the existing devices
3. All necessary connecting cables and other accessories need to be provided by the bidder at their own cost. The bidder shall also be responsible for other related activities such as unpacking, operation, inspection etc.
4. During the installation the bidder shall check physical availability of items as per the packing list. If any of the items are not delivered/not as per the specification/are damaged etc., the bidder or their engineer/s at the site shall take immediate steps and ensure all the items are delivered so that the installation is not hampered.
5. The successful bidder should handle all matters including the configuration, operation, monitoring, management and maintenance of the NAC solution including but not limited to application, system interfaces etc.
6. The successful bidder needs to coordinate with the respective Branches/Regional office/Administrative office in respect of installation and operation of the solution under the scope of this RFP
7. The successful bidder needs to ensure that all DLB authorized devices including but not limited to PCs, laptops, ATMs, printers, scanners, VC devices, IP phones, passbook

kiosks, cash recycler machines, IP cameras are brought into purview of NAC before the installation is deemed to be complete.

8. Bidder must submit along with the technical bid the list of Ports and Services required to be opened on the Network equipment like Firewall, Router etc. at all the locations for implementing the solution
9. The OEM should provide 24x7 technical support through phone and Web for Support, Product Updates, Patches, Signatures and access to Technical Library and Product Documentation during the entire contract period with no additional cost to the DLB. It will be the responsibility of the successful bidder to ensure this
10. The successful bidder should participate and provide necessary support during the DC-DR Drill and during real disaster.
11. The successful bidder to work closely with the existing System Integrators (SIs) of the DLB to achieve minimum downtime. The DLB also expects direct OEM support during the various phases of implementation, which should be provided on demand without any additional cost. During the implementation, the performance or security of the existing network setup should not be compromised.
12. The successful bidder has to ensure installation of the updates, patches, signatures and upgrades for the solution as and when released by the OEM during the contract period with no additional cost to the DLB
13. System hardening for the solution to the satisfaction of the DLB will be under the scope of the successful bidder
14. The successful bidder has to provide onsite support to bring the devices/ endpoints under NAC control at locations, where the same could not be done from central location
15. The successful bidder will ensure onsite availability of experienced engineers in case of any urgent requirement of the DLB in addition to the existing onsite engineer without any extra cost to the DLB, till the time the issue is resolved or the DLB feels so.
16. The processing requirements, house-keeping requirements, operational requirements and future capabilities, implementation requirements, interfaces with other systems and issues relating to Security and Controls have to be comprehensively taken care of and provided for, in the solution

NAC SOLUTION SHALL BROADLY COVERS THE FOLLOWING

1	Onsite Installation and implementation of the solution at DC (Bangalore) and DR (Thrissur).
2	The proposed solution should be a physical appliance deployed in a cluster environment with redundancy, with 2200 agent based end user devices and 800 MAC based Devices(Printer, Scanners, Cameras . . etc) IP devices (With perpetual licensing) and capable to scale up 7000 devices in future .

3	Vendor's expert team will be onsite till complete installation, implementation and project signoff. Vendor shall engage their own persons under own payroll for the DLB NAC project and shall not out source partially or fully to any other third party.
4	A solution must not be a "point of failure" in network traffic flow; the failure of one or more components of the solution should not affect the organizational network's functionality .i.e. Solution should work in offline Mode /SPAN/ Mirror Traffic.
5	Solution shall monitor, detect, block, alert and provide remediation and recommendation for any unauthorized access using cascade, SPAN, mirror, hotspot hooking etc . . . methods.
6	Solution shall use agent and agent less approach for detection of unauthorized access via network activities analysis from the endpoints.
7	Solution should support all the industry standard protocols for detection.
8	Solution should have centralized architecture with web or GUI based dashboard console to monitor, reporting, notification, maintaining and policy push for the registered users centrally.
9	Solution shall support the following remote access capabilities on its management interface via HTTPS or SSH access.
10	Solution shall support role-based administration such as Administrator, Power users and Read-only access users.
11	Solution shall provide forensic evidence on any unauthorized access activity within the network as follow: Event timestamp, network events in sequence, packet capture of suspicious communication, malware behaviours, malware type, severity, source and destination of attack.
12	The proposed solution should support to monitor traffic from multiple segments like WAN, DMZ, Server Farm, Wi-Fi network, MPLS links etc. simultaneously on a single appliance.
13	Solution should have built in capabilities to add exceptions for detections
14	Solution should have built in various reports and can create custom reports like Executive report, detection life cycle report, Top 10 reports for various category and Health reports etc.
15	Solution should provide reports with (but not limited to) HTML/CSV/PDF/Excel formats
16	Solution should be able to schedule reports and also provide the flexibility to generate on-demand reports in daily/weekly/monthly/yearly or specific range (by day and time)
17	Solution shall support NTP server time synchronization.
18	Licenses should be considered based on registered asset to console at any given point of time if applicable.
19	The bidder should have back to back arrangement with the OEM so that DLB will be able to log a call with the OEM directly.
20	The bidder should have a 24x7 365 days support contact centre in order to log the calls. The contact centre numbers should be provided to the DLB along with the escalation matrix mentioning the contact person's name, number and designation in the company.

21	The selected bidder has to supply, install and configure the hardware and software provided as per the timelines and SLA levels prescribed in the RFP.
22	Technical support shall be for 5 (Five) years. (from deployment day till end of 5th year)
23	OEM/ Bidder to provide hardware replacement within 1 day's time if failed as part of RMA replacement policy
24	The solution should be capable of being bypassed in the event of any failure.

4. IT SYSTEM CONFIGURATION AND IMPLEMENTATION SERVICES

The Bidder shall provide the technical design document including .

- Product details
- System Performance benchmarks (data sheet for the hardware used, etc.)
- Architecture (diagram)

5. TRAINING SERVICES

The Bidder shall provide training at DLB Head office, or any other location as specified by DLB to the number of personnel identified by DLB on functional, operational and reporting aspects of the entire NAC solution

The Bidder/ Vendor shall provide training to DLB officials on following type.

- User Training.
- System Administration training.

Training shall be at least 2 days with a batch size as mutually agreed by the DLB and Bidder.

6. PROJECT MANAGEMENT SERVICES

Project Planning, Monitoring and Control

- The Bidder shall develop a Project Management Plan. The plan shall also detail all milestones and indicate when the required deliverable will be available to DLB
- The progress of the implementation shall be monitored on regular basis and the deviations, exceptions shall be analysed and corrective actions to be recommended / suggested.

The Deliverables shall be

- Project Management Plan
- Progress Reports at key milestones

Project Reporting

- Weekly progress report shall be submitted in project execution phase. Also the Bidder shall report on items by exception or that require urgent action.
- Monthly Project Execution Committee meetings will be held at DLB premises in Thrissur. The Bidder is required to provide a report on the following:
 - Progress against the Project Management Plan
 - Status of all open issues

7. SUPPORT –TERMS AND CONDITIONS

System Maintenance & Support services will include the following activities. The vendor is required to deploy NAC solution & execute support services with DLB covering all terms and conditions of this tender/RFP document. System Maintenance & Support services will include the following activities

- 24 x 7 online support
- Issue resolution / Onsite Visits within 8 hrs for level 0 issues
- Issue resolution / remote desktop support within 4 hrs for level 1 issues
- Issue resolution / telephonic support within 1hrs for level 2 issues

Any problems/Issues due to NAC appliance and console malfunctioning issue and virus outbreak issue identified and reported to the Bidder should be categorized based on level as Follows.

Severity Levels	NAC Solution
Level 0	>8 hrs
Level 1	>4 hrs
Level 2	1 hrs

- The maintenance support should be (24x7 365days) including product (major or minor) upgrades and updates. The support should be for unlimited requests. It may be provided on email /Telephone /Remote/Onsite.
- OEM Service and support should be covered under with dedicated TAM (Technical Account Manager) and onsite support

8. SERVICE LEVEL EXPECTATIONS

The bidder is required to adhere to the Service Level Agreements as mentioned below for the support phase.

Sl. No.	Service Area	Service Level	Penalty
	NAC Gateway Solution Appliance /server Affected	Onsite Visits next day for level 0 issues Remote/Webex session same day of issue for level 1 issues Telephonic support at same time issue faced for level 2 issues	Penalty as XX% will be calculated yearly while Support Payments would be made annually max 10% of the invoice value.
1	>8 hrs	Level 0	7%
2	>4 hrs	Level 1	5%
3	>1 hrs	Level 2	2%

Notes:

Response Time shall commence from the time a call is logged.

For the purpose of SLA, a day means the period from the commencement of business hours to close of business hours at a particular location/Branch. (Normally 10.00 AM to 6.00 PM on all weekdays excluding 2nd & 4th Saturdays and holidays)

- Bidder will provide on-site support for addressing Hardware/Software/application related issues.
- The new releases (minor / major), versions, bug fixes etc. for the system software will be supplied to the DLB at no extra charge, with necessary documentation.
- The Bidders should submit a list of support centre addresses, contact person & the resolution/response matrix for these locations.

Reports:- Reports of availability, performance, incident of Network Access Control (NAC) solutions if any, shall be submitted on monthly basis to DLB. Quarterly review shall be conducted for all Service Level requirements.

9. SCHEDULE

The Bidder shall implement the solution/Service(s) as per the schedule specified below:

- Technical Support services period will be for 5 years. (from deployment day till end of 5th year)
- The period of contract shall be extendable, based on mutually agreed terms and conditions.

10. RESPONSIBILITIES OF BIDDER

- The Vender has to supply, install, integrate and commission the solution across various locations mentioned in the technical details.
- The Bidder shall make arrangements to provide maintenance support, problem fixes & upgrades.
- System/Solution health check-up twice a year by vendor.
- System/Solution gap analysis once a year by vendor.
- Next Business Day (NBD) replacement support for hardware if any of failures.

11. WARRANTY & SUPPORT

- The Bidder further represents and warrants that all licenses delivered /rendered under and in accordance with this Contract shall have no defect, arising from design or from any act, error/defect or omission of the Bidder.
- The minimum warranty/AMC period shall be the period of 60 Months i.e. Five Year (5) from date of installation of NAC Solution. The Warranty will start after completion of installation at all sites as mentioned in Scope of Work. The Bidder shall, in addition to this, comply with the performance guarantees specified under and in accordance with the Contract.
- Product licenses should be perpetual and AMC cost to decide by OEM/Bidder accordingly.
- Upon receipt of notice of such defect / error or deficiency, the Bidder shall, with all reasonable speed, repair or replace the defective equipment/software or parts thereof, without cost to Purchaser.

If the Bidder having been notified fails to remedy the defect(s) within the period specified in ‘SUPPORT –TERMS AND CONDITIONS’, purchaser may proceed to take such remedial action as may be necessary, at the Bidder’s risk and expense and without prejudice to any other rights, which Purchaser may have against the Bidder under and in accordance with the Contract.

12. PENALTIES

PENALTY DURING SUPPORT/WARRANTY PERIOD

- If, the Bidder fails to deliver and / or install any or all of the Licenses/ Software’s mentioned in the Purchase order (PO), Purchaser shall, levy a penalty of a sum equivalent to 0.5% percent per week or part thereof of the value of purchase order subject to maximum of 10% of the purchase order value of the delayed equipment or unperformed

services for that particular location. In case of undue delay beyond a period of 15 days unless otherwise waived by the Purchaser, Purchaser at its discretion may consider the delay as termination of the Contract.

- The DLB reserves the right to impose / waive any such penalty.
- The purchaser may without prejudice to its right to effect recovery by any other method, deduct the amount of penalty from any money belonging to the bidder in its hands or which may become due to the Bidder. Any such recovery of penalty shall not in any way relieve the Bidder from any of its obligations to complete the works/services or from any other obligations and liabilities under the Contract .
- Penalty for the failure of service levels are mentioned in the table ‘SERVICE LEVEL EXPECTATIONS’ and will be calculated yearly while Support Payments would be made annually (max 10% of the invoice value).

13. COMMISSIONING TIME

Delivery and Commissioning of the NAC solution component will be at DC-Bangalore & DR-Thrissur within 12 (Twelve) weeks from the date of release of PO.

14. ACCEPTANCE TEST

Power On Self Test (POST) will be conducted by Bidder at the site in presence of DLB officials and /or nominated person. Installation report (IR) should be submitted after complete implementation of systems. DLB will take over the system on successful completion of above acceptance test.

15. OBSOLESCENCE

The bidder will ensure that the stipulated Support and maintenance facilities on the hardware / software will be available for a minimum period of 6 years. The proposed product should not be under “End of Sale” for the next three year from the date of purchase order and should not be under “ End of Support” for the next 6 years from the date of Purchase Order. The vendor will constantly update DLB on new technologies that could prove cost effective.

16. INSTRUCTION TO BIDDERS

- The Bidder shall bear all the costs associated with the preparation and submission of their bid.
- Bidder should submit the bid strictly as per RFP failing which bid will be rejected as non-responsive.
- At any time prior to the Time for submission of bids, the DLB may, for any reason, modify the Bidding Documents through amendments at the sole discretion of the DLB. In

order to provide prospective Bidders a reasonable time to take the amendment if any, into account in preparing their bid, the DLB may, at its discretion, extend the deadline for submission of bids.

- Bid shall remain valid for 3 months from last date of submission of bid prescribed by DLB.

17. BIDDING PROCESS

A two stage bidding process will be followed. The response to the present tender will be submitted in two parts:

- a) Technical bid
- b) Commercial bid.

Technical Bid shall contain all the supporting documents regarding eligibility criteria, scope of work, Technical aspects, Compliance statement and Terms & Conditions etc. mentioned in the RFP. Only those bidders confirming compliance to all the terms & conditions of RFP document shall be short-listed for commercial stage.

18. MODIFICATION OF BIDS & CONTACTING THE DLB

- Bids once submitted will be treated as final and no further correspondence will be entertained on this. No bid will be modified after the deadline for submission of bids. No bidder shall be allowed to withdraw the bid, if bidder happens to be successful bidder.
- Any effort by a bidder to influence the DLB in evaluation of the bid, bid comparison or contract award decision may result in the rejection of the bidders bid. DLB decision will be final and without prejudice and will be binding on all parties.
- No Bidder shall contact the DLB on any matter relating to its Bid, once after technical evaluation is over.

19. TERMS & CONDITIONS OF THE BIDDING FIRMS

The bidding firms are not allowed to impose their own terms and conditions to the bid and if submitted will not be considered as forming part of their bids. The bidders are advised to clearly specify the deviations, in case terms and conditions of the contract applicable to this invitation of tender are not acceptable to them.

20. SYSTEM DEMONSTRATION/PROOF OF CONCEPT

Bidder shall conduct Proof of Concept / System Demonstration wherein the Bidder has to demonstrate the implementation of the solution as per the requirement of the DLB. The Bidder shall submit detailed reports of the test outcomes to the DLB. Bidder may highlight

the noteworthy/superior features of their solution by reference calls and site visits. The Bidder will demonstrate/substantiate all or a few of the claims made in the Technical Bid to the satisfaction of the DLB, the capability of the solution to support all the required functionalities at their cost in their lab/office/in any other organization where solution is in use. The Bidder should use their own tools/utilities/simulators to demonstrate the features laid in the RFP/evaluation criteria.

21. DOCUMENTATION

The Bidder is required to provide the complete documentation of NAC solution which must include but not limited to: System Requirement Specification, Business Requirement Specifications, Installation and Implementation Guide, User Manual, Administration Guide, Hardening Document, System and Application Architecture, Operations Guide and Standard Operating Procedure.

22. ELIGIBILITY CRITERIA FOR BIDDER/OEM

Sl.	Eligibility	Documents need to be submitted
1	The bidder must be a company registered in India under the Companies Act 1956/2013.	Supporting documents.
2	The bidder may be either an OEM or an Authorized Partner or System Integrator of the OEM (Original Equipment Manufacturer) whose product they are proposing. In case the OEM does not deal directly then an OEM may bid through their Authorized Service Partners or System Integrator	Manufacturers Authorization letter from OEM in favor of Bidder. (Template available in Annexure- 5)
3	The Bidder should have a minimum annual turnover of at least Rs. 10 Crores in each of the last three financial years (i.e. 2015-16, 2016-17 & 2017-18). 4. The Bidder should have made net profit in each of the last three financial years (i.e. 2015-16, 2016-17 & 2017-18).	Audited Balance Sheet of the last three financial.
4	The proposed solution must have been implemented by Bidder in a BFSI environment with minimum 3000 IP enabled desktops in India during last five years.	List of installations with clients contact details for verification .
5	The bidder must be Platinum/Gold or Tier-1 /Tier-2 of the OEM for the proposed product.	Relevant certificate from OEM.
6	The Proposed NAC OEM should have a presence in India for the last 3 years.	Declaration from OEM.
7	The bidder should have support offices in Bangalore and Kerala.	Self-declaration with office location addresses.

8	The bidder should not have been blacklisted by Government, any govt. department, PSU or PSB during the last three years.	Self-declaration. (Template available in Annexure- 6)
9	The bidder should have minimum 3 skilled OEM certified staff in own payroll for the product which is proposed.	Details of Certified staff along with their certifications (Bidder should assign persons from these list for the NAC project in DLB).

Note: All eligibility requirements mentioned above should be complied by the bidders as applicable and relevant support documents should be submitted for the fulfillment of eligibility criteria failing which the Bids may be summarily rejected. Non-compliance of any of the criteria can entail rejection of the offer. Copies of relevant documents / certificates should be submitted as proof in support of the claims made for each of the above-mentioned criteria and as and when the DLB decides, originals / certified copies should be shown for verification purpose. The DLB reserves the right to verify / evaluate the claims made by the Bidder independently. Any deliberate misrepresentation will entail rejection of the bid/proposal.

23. DLB’S RIGHT TO ACCEPT OR REJECT ANY BID OR ALL BIDS

The DLB reserves the right to accept or reject any bid and annual the bidding process or even reject all bids at any time prior to award of contract, without thereby incurring any liability to the affected bidder or bidders or without any obligation to inform the affected bier or bidders about the grounds for the DLBs action.

24. EVALUATION, AWARD CRITERIA & INSTRUCTIONS

The Technical Bid should necessarily contain all Technical details and other terms and condition of RFP. Bidder’s proposal should conform to the contents and format of the technical bid listed out Annexure – 2 of the RFP. Proposals not conforming to the specifications may be rejected summarily. Any incomplete or ambiguous terms/conditions will disqualify the offer.

The Technical Bid / Scope of the Work submitted by the Bidder will be evaluated based on the terms and conditions of the RFP. Detailed technical evaluation will include, scrutiny of company profile, technical and functional information of proposed software/service solution, system demonstration of proposed solution, reference calls and site visits.

The functional and technical specification is in a form of a table as provided in Annexure2, which contains the required functionality features in the second column. Bidder’s responses

against each functionality as detailed therein would be evaluated for the selection. The Bidder may highlight the noteworthy/superior features of their solution and same may be specified on Annexure – 3.

1. To meet DLB's requirements, as spelt out in this Bid Document, the selected Bidder must have the requisite experience and expertise in providing services in the field of information and communication technology, the technical know-how, and the financial ability that would be required to successfully set-up the required infrastructure and provide the services sought by DLB.
2. A screening committee constituted by DLB for the purpose of selection of the successful Bidder, would evaluate Bids.
3. The proposals will be evaluated in stages. In the first stage, i.e. Technical Evaluation of the Bidders will be done and in the second stage. Indicative commercial bids would be evaluated and commercial negotiation/RA will be conducted for the technically qualified bidders in this stage .
4. The Technical Bid should necessarily contain all Technical details and other terms and condition of RFP. Bidder's proposal should conform to the contents and format of the technical bid listed out Annexure - 2 of the RFP .Proposals not conforming to the specifications may be rejected summarily. Any incomplete or ambiguous terms/conditions will disqualify the offer.
5. The Technical Bid submitted by the Bidder will be evaluated based on the terms and conditions of the RFP. Detailed technical evaluation will include, scrutiny of company profile, technical and functional information of proposed software/service solution, system demonstration of proposed solution, reference calls and site visits.
6. The functional and technical specification is in a form of a table as provided in Annexure - 2, which contains the required functionality features in the second column. Bidder's responses against each functionality as detailed therein would be evaluated for the selection. The Bidder

may highlight the noteworthy/superior features of their solution and same may be specify on Annexure - 3.
7. Each Bidder acknowledges and accepts that DLB may, in its absolute discretion, apply whatever criteria it deems appropriate in the selection of vendor, not limited to those selection criteria set out in this RFP document.
8. The Bidders shall be short listed after the evaluation of their Technical Bids and will be informed. Only the short listed bidders will be permitted to participate further process.

9. DLB reserves the right to modify / amend the evaluation process at any time during the Bid process, without assigning any reason, whatsoever, and without any requirement of intimating the Bidders of any such change. At any time during the process of Bid evaluation, DLB may seek specific clarifications from any or all Bidders.
10. DLB reserves the right to modify the total quantities subject to a variation of $\pm 25\%$ on either side of the projected requirements during the rate contract i.e. five years (5) from the date of award of the contract. The Bidder shall not and hereby waive any or all objections that it might have at the relevant point of time.
11. Bidder will not be invited for opening of Indicative commercial bid after qualifying in the Technical Bids.
12. DLB reserves the right to accept or reject in part or full any or all the Bids without assigning any reason whatsoever. Any decision of DLB in this regard shall be final, conclusive and binding on the Bidder.
13. DLB reserves the right to re-issue / re-commence the entire bid process in case of any anomaly, irregularity or discrepancy in regard thereof. Any decision of the DLB in this regard shall be final, conclusive and binding on the Bidder.
14. Modification to the RFP Document, amendments, time-extension, clarification etc. . if any, will be made available as an addendum on the DLB's website and / or emailed to the prospective Bidders.
15. The Bidder should confirm in writing its obligation to supply upgraded model of the product in case of technological obsolescence / non-availability of contracted product/model. The supply of upgraded product, subject to the DLB's approval, will be at the same contracted price as the obsolete model.
16. In case of reduction of prices due to technological obsolescence / change of product model, the Bidder should pass on the price benefit to the DLB.
17. Successful Bidder would sign the Contract/SLA and other forms specified in RFP Document with Dhanlaxmi Bank at Thrissur only.
18. The Bidder shall bear all costs and expenses for the execution, stamp duty and submission of the contract and agreements. DLB shall not be responsible or liable for reimbursing/compensating these costs and expenses.
19. To complete the work at the site within stipulated timeframe, Bidder's employees/workmen may have to visit the site multiple times, at no extra cost to the DLB.

20. Quotations contained in the Bids shall remain valid for a period of 60 (sixty) days from the date of submission of the Bid in response to the RFP.
21. Prices quoted should be EXCLUSIVE of all applicable taxes and applicable taxes would be deducted at source, if any, as per prevailing rates.
22. The price (“Bid Price”) quoted by the Bidder cannot be altered or changed due to escalation on account of any variation due currency exchange rates or cost of material.
23. The DLB will not be obliged to meet and have discussions with any Bidder and/ or to entertain any representations in this regard.
24. During the period of evaluation, Bidders may be asked to provide more details and explanations about information they have provided in the proposals. Bidders should respond to such requests within the time frame indicated in the letter/e-mail seeking the explanation.
25. The DLB’s decision in respect to evaluation methodology and short-listing Bidders will be final and no claims whatsoever in this respect will be entertained.
26. The Bids received and accepted will be evaluated by the DLB to ascertain the best and lowest bid in the interest of the DLB. However, the DLB does not bind itself to accept any Bid, lowest or otherwise, and reserves the right to reject any or all bids at any point of time prior to the order without assigning any reasons whatsoever.
27. Apart from the above, the company profile, past experience and performance track record of the Bidder in the area of the assignment, methodology to be adopted to carry out the assignment, delivery schedule, service support, price, etc. shall be some of the important criteria in selecting the bidder.
28. The Bids will be evaluated both on the Technical and Commercial merits and the DLB’s decision in this regard shall be binding, final and conclusive.

25. CONFIDENTIALITY

The bidder shall not, without the written consent of the DLB, disclose the contract or any provision thereof, any specification, or information furnished by or on behalf of the DLB in connection therewith, to any person(s). The bidder shall not, without the prior written consent of the DLB, make use of any document or information except for purposes of performing this agreement.

26. PATENT RIGHTS

- The supplier shall indemnify the purchaser against all third party claims of infringement of patent, trademark or industrial design rights arising from use of the Goods, or any part thereof in India.
- The supplier shall, at their own expense, defend and indemnify the DLB against all third party claims or infringement of intellectual Property Right, including Patent, trademark, copyright, trade secret or industrial design rights arising from use of the products or any part thereof in India or abroad.
- The supplier shall expeditiously extinguish any such claims and shall have full rights to defend itself there from. If the DLB is required to pay compensation to a third party resulting from such infringement, the supplier shall be fully responsible therefore, including all expenses and court and legal fees.

27. SIGNING OF CONTRACT.

The successful bidder(s) shall mandatorily enter into a Service Level Agreement (SLA), Non-Disclosure Agreement (NDA) and integrity Pact (IP) with DLB, within 30 days of the award of the tender or within such extended period as may be permitted by the DLB. The letter of acceptance and such other terms and conditions as may be determined by the DLB to be necessary for the due performance of the work in accordance with the Bid and the acceptance thereof, with terms and conditions shall be contained in a Memorandum of Understanding to be signed at the time of execution of the Form of Contract.

28. PAYMENT TERMS.

No advance payment will be made on award of the contract.

Hardware, Support and AMC payments would be made on Production of invoices as per below terms:

Hardware and Licenses -

- 50% on delivery, installation of the Solution including all licenses at Central Location within 10 weeks from the date of release of PO as per the timelines specified in the RFP.
- 30% on deployment and user acceptance for 10 locations for manageable switch environment and 10 locations for unmanageable switch locations and submission of the Contract, PBG, Deed of Indemnity, NDA and SLA. The 10 manageable switch locations and 10 unmanageable switch locations should be covered within 14 weeks from the date of release of PO.
- 20% on deployment and user acceptance for the remaining manageable and unmanageable switch locations.

1. Locations refer to any branches, head-offices, central and regional offices belonging to the DLB.
2. Support and AMC payments would be made annually in advance on Production of invoice and delivery of satisfactory services in the previous year.
3. Payment for procurement of hardware and licenses would be made on submission of invoices and report of delivery/commissioning of licenses. The warranty, if any for the procured licenses will start after commissioning/installation of hardware and licenses at server end.
4. All payments shall be subject to TDS, if any, as per the tax rules at the time of Payment.
5. Payments may be withheld in case all the deliverables are not met and will be based on SLA terms.
6. All out of pocket expenses, travelling, boarding and lodging expenses for the entire Term of this RFP and subsequent agreement is included in the amounts quoted and the Bidder shall not be entitled to charge any additional costs on account of any items or services or by way of any out of pocket expenses, including travel, boarding and lodging.
7. All the payments to the Successful Bidder shall be subject to the performance/ delivery of the Services to the satisfaction of DLB for this purpose.
8. Penalties / liquidated damages, if any, shall be deducted from the invoice value.

Notwithstanding anything contained in this RFP/ the Contract or in any other document(s) under no circumstances DLB shall be liable to the Successful Bidder and/or its employees/personnel/representatives/agent etc. for direct, indirect, incidental, consequential, special or exemplary damages arising from termination of the Contract;

- DLB shall not have any liability whatsoever in case of any third party claims, demands, suit, actions or other proceedings against the Successful Bidder or any other person engaged by the Successful Bidder in the course of performance of the Service.
- DLB reserves the rights to dispute/deduct payment/withhold payments/further payment due to the Successful Bidder under the Contract, if the Successful Bidder has not performed or rendered the Services in accordance with the provisions of the Contract which the DLB at its sole discretion adjudge.
- Successful Bidder shall permit DLB to hold or deduct the amount from invoices, for non-performance or part performance or failure to discharge obligations under the Contract.

- It is clarified that the any payments of the charges made to and received by authorised Successful Bidder personnel shall be considered as a full discharge of DLB’s obligations for payment under the Agreement.

Three copies of Bidder’s invoice showing contract number, Services description, quantity, unit price and total amount. Prior to preparing invoice copy and delivery challan before delivering the equipments, the bidder should check, verify and confirm the location address, user name, contact details with our purchase order. Bidder should ensure that proper delivery of equipment address, Name of end user, and contact details are mentioned on the invoice copy / delivery .

29. SUBMISSION OF BID

Bid shall be submitted in Hard/Soft Copies. The bid should contain following:

1. Technical Bid.
2. Commercial Bid.

Address for Communication:

Head-IT & Digital Banking
 IT Department
 4th Floor, Corporate Office,
 Dhanalakshmi Buildings
 Dhanlaxmi Bank Limited
 Naickanal, Thrissur,
 Kerala – 680 001

30. CLARIFICATIONS REGARDING RFP DOCUMENT

Before bidding, the bidders are requested to carefully examine the RFP Document and the terms and conditions specified therein. In case the bidders require any clarification on this RFP, the query may be sent to e-mail addresses: biju.kf@dhanbank.co.in or Phone: +91 487 6627067

31. IMPORTANT DATES

Sl no	Particulars	Date and Time
1	Issuance of RFP document by the Bank	29th Dec 2018
2	Last date of submission of any queries, clarifications etc.	09th Jan 2019
3	Last Date of submission of RFP response as soft copy	23rd Jan 2019

- Bid submitted after the last date will be rejected.

32. EXECUTION OF AGREEMENT

On awarding the contract, the successful bidder and Bank should execute an agreement, which states the responsibilities and obligations of each party with the other, as per DLB's outsourcing policy. The Bidder should sign and execute this Non-Disclosure Agreement before the execution of this Contract. The contract will be for a period of Five year.

33. ANNEXURES

Annexure-1

Below is the list of documents to be submitted for with Bid.

Technical Bid.

- 1, Supporting documents and evidence listed in '14 - ELIGIBILITY CRITERIA FOR BIDDER/OEM' table on page 13
- 2, Technical Specification conformation list. Bidder has to submit as specified in given format in Annexure – 2.
- 3, Important Unique/Additional technical feature available in the solution which are not listed in DLB Technical Specification Bidder has to submit in format specified as Annexure – 3.

Commercial Bid

Bidder has to submit the commercial bid with indicative pricing specified in given format in Annexure – 4.

Annexure-2

Sl.	Solution features/requirement - Description	Compliance Y/N	Remarks
General			
1	The proposed solution shall meet the below minimum specifications. Any hardware or software or licenses required to enable the functionality shall be provided from Day 1		
2	The following is a list of functions that should encompass a NAC solution:		
	I. Element Detection - detecting new elements as they are introduced to the network.		
	II. Authentication – authenticating each user accessing the network no matter where they are authenticating from and/or which device they are using.		
	III. Endpoint Security Assessment – assessing whether a newly introduced network element complies with the security policy of the organization. These checks may include the ability to gather knowledge regarding an element’s operating system, the list of installed patches, the presence of anti-virus software and its virus signature date, etc.		
	IV. Remediation– quarantining an element that does not comply with the defined security policy until the issues causing it to be non-compliant are fixed. When quarantined, the element may be able to access a defined set of remediation servers allowing the user fixing the non-compliant issues and to be reintroduced, now successfully, to the network.		
	V. Enforcement – restricting the access of an element to the network if the element does not comply with the defined security policy.		
	VI. Authorization – verifying access by users to network resources according to an authorization scheme defined in an existing authorization system, such as Active Directory, RADIUS servers, etc., allowing the enforcement of identity-based policies after an element is allowed on the network.		

	VII. Post-Admission Protection – continuously monitoring users, elements and their sessions for suspicious activity (i.e. worms, viruses, malware, etc.). If detected, the action taken by a NAC solution may vary from isolating the offending system to dropping the session.		
3	The Network Access Control (NAC) solution should be an automated security control platform that can monitor and control everything on the network—all devices, all operating systems, all users. The solution shall let employees and guests remain productive on the network while critical network resources and sensitive data remain protected.		
4	Solution should Maintain an up-to-date/centralized inventory of authorized devices connected to DLB’s network (within/outside DLB’s premises) and authorized devices enabling the DLB’s network.		
5	The proposed solution must possess an architecture that should works in offline Mode /SPAN/ Mirror Traffic i.e. out-of-band mode.		
Deployment			
6	Network Access Control solution (NAC/NAC Solution/Solution) should do exactly what the name implies—control access to the network with policies, including pre-admission endpoint security policy checks and post-admission controls over where users and devices can go on a network and what they can do.		
7	The solution should be deployed in high availability architecture for ensuring system availability in the event of component failure.		
Hardware			
8	The proposed solution must have RAID redundancy (for hard drives), network redundancy (for network interfaces) and Power-Supply redundancy.		
9	The proposed solution must have minimum 2 x 1000 GB Ethernet Copper Ports		
10	Scalability-The proposed solution must be easily scalable to support monitoring 7000 devices but should initially support health-check / integration of minimum 2200 End User /Desktops and 800 MAC based devices		
11	The proposed solution must be a purpose built 1RU or		

	2RU rack-mountable appliance.		
12	The proposed solution must support onboard retention of traffic logs for a period of minimum 3 months.		
13	The Physical Appliance proposed for the NAC solution should have a longitivity of 6 years from the date of release of PO.		
Management			
14	The proposed solution should have a Centralized Management Console with customizable dashboard and role-based admin		
15	The solution should offer a built-in monitoring, reporting, and troubleshooting console to assist helpdesk operators and administrators streamline operations		
16	The solution should enable administrators to centrally configure and manage profiler, posture, guest, authentication, and authorization services in a single web-based GUI console, simplifying administration by providing consistency in managing all these services.		
Reporting			
17	The proposed solution must be able to generate report on different parameters. i.e Compliance , Non-Compliance , corporate , Guest , BYOD , Mobile Devices , IOT's etc.		
18	The proposed solution should have ability to generate reports in different formats, such as HTML, Excel, CSV and PDF		
19	Reports should automatically be generated on a scheduled basis and should be available in real time on demand		
20	The proposed solution should come with predefined, out-of-the-box reports.		
21	Administrators should update or define custom reports and should have ability to run certain reports based on security role		
22	Should support scheduled reports be delivered via e-mail		

23	The proposed solution must incorporate a complete set of tools for reporting (Audit trailing, customizable reporting and data export capabilities), analysis, and troubleshooting. Data from access transactions can be organized by customizable data elements and used to generate graphs, tables, and reports. Must correlate and organize user, authentication, and device information together		
24	The solution should provide a Registered Endpoints Report. The report should provide the following details: Specify Details. <ul style="list-style-type: none"> • Logged in Date and Time • Portal User (who registered the device) • MAC Address • Identity Group • Endpoint Policy • Static Assignment • Static Group Assignment • Device Registration Status 		
Functional Requirement			
25	The proposed solution should operate within a heterogeneous network with switches from multiple vendors (e.g. - Cisco, Juniper, HP/Auruba, DEL, Linksys, Extreme Networks and Dlink etc. and legacy switches). NAC appliance should support vendor agnostic switch infrastructure.		
26	The proposed solution shall be based on agent based and but also support non-agent based end user devices.		
27	The solution should provide separate access solution for guests and visitors. The solution should support Captive portal based solution for these classes of users. These users should get a message if the compliance check on their machines fails.		
28	Automatically configure and provision personal/mobile devices such as iOS, Android, Chromebook, and Ubuntu, enabling them to securely connect to enterprise network		
29	The solution should have a provision to support non-NAC capable hosts (i.e., printers, IP phones, IOT's etc.) based on Mac address or other parameter and it should support exception lists for non-NAC capable hosts.		

30	The solution should support the backup and recovery of policies/configuration.		
31	For forensic and faster network troubleshooting, the solution should log each & every session/ all important events that pass through and provide simple graphical and statistical reports. & Logs should be exportable to external log server.		
32	The proposed solution able to support IPv6-IPv4 dual stack deployments		
33	Solution should be licensed wherein all supported features should be available for all IP devices		
34	Solution must be vendor & OS agnostic to existing wired, wireless and VPN network.		
35	Solution shall have capabilities to identify and block the endpoint which are connected on Network Infrastructure.		
36	Solution must be able to automatically classify the detected devices in to different categories according to their functions such as Windows, Apple MAC , Printers, Network Devices, Linux, Unix & IOT's etc.		
37	Should provide detailed information regarding the endpoint connected to the network.		
38	Should provide information regarding the endpoint connected to the network, such as IP Address, MAC Address, NetBIOS Name, NetBIOS Domain, Domain User, Domain Member, OS-Class, IP of the connected switch, Switch Port, Switch Port VLAN, Switch Port Status, Switch Vendor, Access status ets . .		
39	Auto-Remediation or Should guide users through a self-remediation process.		
40	The solution should discover any new network device entering the network and permit network access based upon the policy for this network device.		
41	The solution should have a provision to support non-NAC capable hosts (i.e., printers, IP phones, IOT's etc.) based on MAC address or other parameter and it should support exception lists for non-NAC capable hosts.		

42	<p>Device authentication & network access control- The solution must support the following authentication methods</p> <ol style="list-style-type: none"> 1. 802.1X Authentication. 2. Agent-less Authentication. 3. MAC Address based Authentication by type 4. MAC Address based Authentication by pre-defined list 5. AD - LDAP 6. RADIUS 		
43	<p>The solution should address vulnerabilities on user machines through periodic evaluation and remediation to help proactively mitigate network threats such as viruses, worms, and spyware</p>		
44	<p>The solution should enforce security policies by blocking, isolating, and repairing noncompliant machines in a quarantine area without requiring administrator attention</p>		
45	<p>The solution should offer a rules-based, attribute-driven policy model for creating flexible and business-relevant access control policies. Provides the ability to create fine-grained policies by pulling attributes from predefined dictionaries.</p>		
46	<p>The solution should have the capability to collect endpoint attribute data via passive network telemetry, querying the actual endpoints, or alternatively from the infrastructure</p>		
47	<p>The solution should verify endpoint posture assessment for PCs connecting to the network The solution should provide the ability to create powerful policies that include but are not limited to checks for the latest OS patches, antivirus and antispymware software packages with current definition file variables (version, date, etc.), registries (key, value, etc), and applications. Solution should support auto-remediation of PC clients as well as a periodic reassessment to make sure the endpoint is not in violation of company policies.</p>		
48	<p>The solution should support importing endpoints from a comma-separated values (CSV) file in which the list of endpoints appears with the MAC address and the endpoint profiling policy details separated by a comma</p>		

49	The solution should support MAC Address Bypass (used for devices which do not support 802.1x) and can further utilize identity of the endpoint to apply the proper rules for access.		
50	The solution must allow users access to the network in a worst case scenario in case of AAA server outages or any other reasons like WAN failure.		
51	The solution shall have profiling capabilities integrated into the solution in order to detect end points. (Please specify supported protocol/features) <ul style="list-style-type: none"> • Profiling using MAC OUIs • Profiling using DHCP information • Profiling using RADIUS information • Profiling using HTTP information • Profiling using NetFlow information • Profiling using SPAN/Mirrored traffic • Profiling using MAC OUIs discovery. 		
52	The solution should be capable of being bypassed in the event of any failure of the solution.		
53	The proposed solution should support the mechanism to send customized message to specified recipients/end users when a certain policy is triggered. For eg. If firewall violation exceed certain threshold limit for certain users, then the user should receive a message		
54	The proposed solution should detect known/friend or unknown/rogue devices on specific VLAN depending on device type, MAC address, or other criteria		
55	The proposed solution should be able to Detect infected or otherwise compromised/malicious devices on specific VLAN depending on threat information from desktop anti-virus, vulnerability assessment tool, SIEM alerts or other criteria.		
56	The proposed solution should support Manual/administrative override of default action		
57	The propose solution should support Guest on-boarding flexibility and should include delegation to guest sponsors, as well as the option for guests to self-register their own devices		
Integration Capability			
58	Solution should integrate seamlessly with DLB's existing IT infrastructure comprising of routers, switches, firewalls, IPS, various types of WAN links and computers, devices, Operating Systems etc.		

59	For forensic and faster network troubleshooting, the solution should log each & every session/ all important events that pass through and provide simple graphical and statistical reports. & Logs should be exportable to external log server.		
60	The proposed NAC solution should integrate with leading Firewall brands such as (Checkpoint, Palo Alto Networks, Fortinet, Cisco, etc.) to respond rapidly to compromised devices on network to prevent threat propagation.		
61	The proposed NAC solution should integrate with Enterprise level SIEM solutions i.e. Alien Volt and Syslog server. The Solution should be able to share information to leading SIEM vendors using standard protocols(Syslog, CEF) and should allow the SIEM system to send syslog messages to the NAC solution to automatically respond to any endpoint security issues		
62	The proposed NAC solution should support, verify authentication and integrate with Microsoft LDAP & Active Directory server.		
63	The proposed solution must able to integrate with existing Antivirus solution such as Symantec End point protection for Auto- Remediation.		
64	The proposed NAC solution should integrate with MDM vendors such as Airwatch. The solution should be able to integrate with leading EMM/MDM vendors to provide real-time visibility of unmanaged/agentless mobile devices. In addition, it should also deliver comprehensive information about the managed mobile devices that are connected to the enterprise network. Automatic detection, enrollment, compliance check and policy based access rules regardless of device type.		
65	Solution should integrate with the leading vulnerability assessment tools & ATD security vendors, allowing it to receive threat information and apply policy-based mitigation actions depending on the severity or priority of the threat.		
66	The proposed solution should include any software license or plug-in module required to meet the above integrations from Day 1. Also It should be possible to plug in new security features in future.		

Licensing

67	Licensing should cover all the features required to deploy the NAC solution.		
Endpoint Posture Checking			
68	Perform advanced endpoint posture assessments to ensure organization's compliance is met before devices connect.		
69	End point Posture Checking support the following operating systems and versions: Microsoft Windows 7 and above, Apple macOS 10.10 and above.		
70	Endpoint posture and health checks should include Winows and Installed Applications, Antivirus, Firewall, Network Connections, Processes, Patch Management, Peer to Peer applications, Virtual Machines, USB Devices etc.		
71	Users of unhealthy endpoints that do not meet compliance requirements, should receive a message about the endpoint status and instructions on how to achieve compliance		
Remediation, quarantine and captive portals			
72	Quarantine (A quarantine network is a restricted IP network that provides users with routed access only to certain hosts and applications)		
	Captive portals (A captive portal intercepts HTTP access to web pages, redirecting users to a web application that provides instructions and tools for updating their computer. Until their computer passes automated inspection, no network usage besides the captive portal is allowed)		
73	The proposed solution should enforces security policies by blocking, isolating, and repairing noncompliant machines in a quarantine area without requiring administrator attention		
74	The proposed solution allow administrators to quickly take corrective action (Quarantine, Un-Quarantine, or Shutdown) on risk-compromised endpoints within the network. This will help to reduce risk and increase security in the network.		

75	The proposed solution should support automated remediation system including starting process, killing process, setting registry keys, starting antivirus, update anti-virus, starting windows updates and running custom scripts. • Help desk and self-service remediation allowing for load reduction through end user self-support and automatic remediation.		
76	Solution should include a guest networking application		
77	Solution should provide below mentioned mechanism for notification of user credentials to Guest Users - 1)Web Page redirect 2)SMS integration 3)Email		
78	Perform advanced endpoint posture assessments to ensure organization's compliance is met before devices connect, Endpoint posture and health checks should include Windows and Installed Applications, Antivirus, Firewall, Network Connections, Processes, Patch Management, Peer to Peer applications, Virtual Machines, USB Devices etc.		
79	The solution should allow administrators to quickly take corrective action (Quarantine, Un-quarantine, or Shutdown) on risk-compromised endpoints within the network. This helps to reduce risk and increase security in the network.		
Case Studies			
The proposed solution should cover the below mentioned case studies out of the box. These case studies are not exhaustive.			
80	Asset Classification-The proposed solution can detect both new and existing endpoints and categorizes them based upon the type of endpoint (Ex: Windows, Printer, Network Device, etc...).		
81	Guest Identification and Control-The proposed solution can detect a new connection to the network and assess that it is not a device belonging to the corporate network or domain, and handles the device as specified within the rule		
82	The proposed solution can properly detect whether a device is running an Antivirus application, determine if the signature files are current within a specified date range, and handle the device as specified within the policy		

83	The proposed solution can check to see if any Windows endpoints contain any known vulnerabilities and remediate or handle the device as specified within the rule		
84	The proposed solution can identify applications installed on the endpoints. Policies can be written to categorize these applications and determine their current status based upon attributes of these applications.		
85	The proposed solution enforcement options should remain the same regardless of switch manufacturer. The solution can enforce policies at the switch port, including moving a device from one VLAN to another, blocking the switch port, and applying dynamic ACL		
86	Continuous Policy Enforcement-The proposed solution can ensure devices are compliant with policies as long as they are connected to the network. If a device becomes non compliant after it has already been inspected, solution will identify non-compliance and handle it as specified within the policy		
87	The proposed solution can determine if any endpoints are running any P2P applications and handle the situation as specified within the rule		
Software and Support Maintenance			
88	The proposed solution must provide the options of RTF (Return to Factory), ND (Next Day) be supported from the manufacturer as part of OEM's general support offerings.		
89	The proposed solution must include at least five years maintenance contract with back to back support from OEM.		
90	The SI of the proposed solution should have support offices located at Bangalore and Kochi locations.		
Deployment Locations			
91	The proposed solution will be deployed for DLB centrally at two locations:- Datacenter Site – Bangalore Disaster Recovery Site - Thrissur		

Annexure – 3

Bidders/Vendors may highlight the important Unique/Additional technical feature providing to DLB in the solution which are not listed in Technical Specification in below format.

Sl.	Unique/Additional technical feature not listed in Technical Specification.	Remarks
1		
2		
3		
4		
5		
6		
7		
8		

Annexure – 4

Commercial offer

NAC Gateway Solution for Dhanlaxmi Bank				
Sr. No.	Description	Qty	Indicative Price	Indicative total Price
1	NAC Gateway Solution for DC (2 Numbers in Cluster) and 1 in DR	3		
2	License cost for 2200 Agent based end devices and 800 Non-agent-less MAC based devices (Perpetual model licensing)	1		
3	AMC and Support cost for 3 Years	1		
4	AMC and Support cost for 4th Year (Advance Payment on 3 rd Year)	1		
5	AMC and Support cost for 5th Year(Advance Payment on 4 th Year)	1		

All prices are exclusive of taxes

NAC Gateway Solution for Dhanlaxmi Bank (Additional Components)				
Sr. No.	Description	Qty	Indicative Price	Indicative total Price
1	Additional license cost for 500 Agent based end devices (Perpetual model licensing)	1		
2	Additional License cost for 500 Non-agentless MAC based IP devices (Perpetual model licensing)	1		

All prices are exclusive of taxes

All prices quoted shall based on the services, specification, terms and conditions specified by the DLB in the RFP

Annexure - 5**OEM/Manufacturer Authorization Format (On OEM's letter head)**

Ref: Date:

To

DGM (IT & Digital Banking)
IT Department
Dhanlaxmi Bank
Corporate Office
Thrissur

Dear Sir,

Sub: Manufacturer Authorization for RFP No. dated xx/xx/xxxx

We <OEM Name>having our registered office at <OEM Address> are an established and reputed manufacturer of <hardware details> do hereby authorize M/s _____ (Name and address of the Partner) to offer their quotation, negotiate and conclude the contract with you against the above invitation for tender offer.

We hereby extend our full guarantee and warranty as per terms and conditions of the tender and the contract for the solution, products/equipment and services offered against this invitation for tender offer by the above firm and will extend technical support and updates / upgrades if contracted by the bidder.

We also confirm that we will ensure all product upgrades (including management software upgrades and new product feature releases) are provided by M/s for all the products quoted for and supplied to Dhanlaxmi Bank during the Five year product warranty/Support period.

<OEM Name>

<Authorized Signatory>

Name:

Designation:

Note: This letter of authority should be on the letterhead of the OEM and should be signed by a person competent and having the power of attorney to bind the manufacturer. It should be included by the bidder in its bid.

Annexure - 6

Non Blacklisting Declaration Format (*On OEM's letter head*)

Ref: Date:

To

DGM (IT & Digital Banking)
IT Department
DhanlaxmiBank
Corporate Office
Thrissur

Dear Sir,

Sub: Non Blacklisting Declaration by *<OEM Name>* for RFP No. Dated *<xx/xx/xxxx>*

We *<OEM Name>* having our registered office at *<OEM Address>* are an established and reputed manufacturer of *<Name of Product>*, do hereby declare and confirm that we are not currently blacklisted by any Central/State Govt. or any Dept/Bank.

<OEM Name>

<Authorized Signatory>

Name:

Designation:

Note: This letter of authority should be on the letterhead of the OEM and should be signed by a person competent and having the power of attorney to bind the manufacturer. It should be included by the bidder in its bid.