Section-E: Revised (2nd) SCOPE OF WORK

The scope of work includes understanding the requirement, customizing and providing the deployment architecture of proposed solution. Supply, install and commission solution at LIC data centers. Configure for high availability, tune up the appliances with LIC Security requirement; document the solution, train the candidates nominated by LIC. This is not an all-inclusive list. The Bidder is expected to provide the end to end solution and vendor is expected to absorb any other cost of material / services if any not particularly listed below.

Based on the contents of the RFP, the Bidder shall be required to propose a solution, which is suitable for LIC, after taking into consideration the effort estimated for implementation of the same and the resource and the equipment requirements. LIC expressly stipulates that Bidder's selection under this RFP is on the express understanding that this RFP contains only the broad provisions for the entire assignment and that the deliverables and the services in connection therewith are only a part of the assignment. The Bidder shall be required to undertake to perform all such tasks, render requisite services and make available all such resources as may be required for the successful completion of the entire assignment at no additional cost to the LIC notwithstanding what is stated here and what is not stated.

A Minimum 10,000 licenses for concurrent users will be procured by LIC. However, if the number of users exceeds 10,000 the bidder will not deny access to the additional users, but bring it to the notice of LIC. If the number of concurrent users continues to exceed 10,000 for period of seven days. LIC will place additional purchase order for the same.

The Bidder must envisage all necessary services to be provided and ensure the same is delivered to LIC. LIC will not accept any plea of the Bidder later for omission of critical services on the pretext that the same was not explicitly mentioned in the RFP.

General

- Supply of the solution/products along with the licenses with provision for version upgrades/patches.
- Installation and implementation of the solution as per the technical specifications and requirements of LIC.
- In case there is a cost incurred to LIC due the wrong BoM/Specification/feature-set of the solution at any location, the same will have to be replaced by vendor at no extra cost to LIC.
- Prepare test-plan, migration plan and rollback strategies
- Monitoring, onsite support and offsite support
- The successful bidder shall co-ordinate and co-operate with the other vendors appointed by the LIC so that the work shall proceed smoothly without any delay and to the satisfaction of LIC.
- No extra claim shall be entertained on account of all/part of any job redone on account of bidder's negligence which results into damages/losses during execution of the job. Also, any component(s) required to deliver the solution after release of Purchase Order shall have to be provided by the successful bidder. All such cost shall be borne by the bidder.
- The vendor has to provide complete escalation matrix which should be updated and sent to LIC as and when there is a change.
- No extra claim shall be entertained on account of all/part of any job redone on account of bidder's negligence which results into damages/losses during execution of the job. Also, any component(s) required to deliver the solution after release of Purchase Order shall have to be provided by the successful bidder. All such cost shall be borne by the bidder.
- The bidder has to perform an OEM/OSD/OSO audit immediately after the deployment of the solution. The OEM/OSD/OSO audit has to provide a detailed report on the hardening, best practices to be adopted and compliance to IRDAI guidelines. All aspects of technical specifications should be verified for the implementation. IS Audit requirements as per the IRDAI/other regulatory guidelines should be complied with. The audit should also cover compliance with any legal, regulatory or industry requirements.
- After the first OEM/OSD/OSO audit, immediately after deployment the bidder has to perform a half yearly OEM/OSD/OSO audit and provide a detailed report on the hardening and best practices to be adopted. All aspects of technical specifications should be verified for the implementation. IS Audit requirements as per the IRDAI/other regulatory guidelines should be

complied with. The audit should also cover compliance with any legal, regulatory or industry requirements and should provide recommendations on the latest security posture to be adopted in view of the evolving threat landscape.

- The OEM/OSD/OSO Audit report should be made available within seven days of conducting the OEM/OSD/OSO Audit. The System Integrator has to ensure that all the shortcomings pointed out in the OEM Audit report are rectified and all the recommendations are complied with within fifteen working days at no additional cost to LIC.
- The Bidder has to formulate the BCP processes in line with the IRDAI guidelines and conduct DR Drill twice a year. The DR drill conducted has to be evaluated by a third party (CERT-In empanelled).

1.1) Details of Work

- ➢ Total solution will cover supply, installation, implementation, testing, training, supporting the MFA and Contextual Access solution (including the licenses and hardware), management and reporting during the contract period.
- ➢ The hardware has to be sized in such a manner to ensure no latency, no malfunctioning or any adverse impact on the system even at the peak load.
- ➢ Prepare HLD and LLD in consultation with OEM/OSD/OSO and LIC for rollout. The design should be OEM/OSD/OSO certified.
- ➢ Design and document a Project implementation plan with significant milestones marked on it.
- ➢ The selected bidder needs to configure the solution in High Availability (HA) mode (Active-standby) and configure management and reporting as deemed fit to address the LICs requirement .
- ➢ The successful bidder need to implement the solution as per the technical specification described in this tender.
- ➢ Bidder needs to study the existing Client, Server, LAN & WAN network environment of LIC and suggest suitable changes for deployment of proposed solution.
- ➢ The solution needs to be integrated with LIC's existing Local Area Network, Wide Area Network, Server and Security infrastructure etc.
- ➢ The bidder shall be responsible to provide within scope of work all facilities like labour, transportation, tool Kits, testing equipment etc. which is necessary for successful deployment of solution.
- ➢ Transportation to & fro, lodging and boarding of manpower shall be in vendors scope. (Present Locations are Vile-Parle (S.V. Road, Mumbai 400054), IDC (Prabhadevi, Mumbai) and Bangalore.

1.2) Details of MFA requirement

- ➢ The bidder shall provide the MFA and Contextual Access solution as per the requirements mentioned in the technical specifications.
- ➢ The provided solution shall be of the latest versions and should not be end of support for the next six years.
- ➢ The initial requirement is for 10000 users (concurrent licenses) which may be scaled up to 50,500 users. These users will be using the Multi-Factor Authentication, Contextual Access Solution and Remote connectivity solution.
- ➢ The successful bidder shall provide all necessary hardware, software licenses, tools, deploy, implement, train and handover the solution to LIC.
- ➢ In case of any regulatory changes the bidder has to make the necessary modifications in the solution so as to comply with the regulatory changes.
- ➢ LIC intends to integrate the offered solution with multiple applications/server/network devices.
- ➢ "User" should be able to access all MFA and Contextual Access integration application/systems with single license.
- ➢ There should not be any restriction on the number of devices.
- ➢ The effective start date of the licenses shall be Go-live and acceptance by LIC.
- ➢ License subscription cost shall also include product support. Product support shall include updates, upgrades, patches/bug fixes, problem resolution etc. If, any new version of the software is released during the subscription period, then the same shall be made available to LIC without

any additional cost. 24 x 7 problem resolution support shall be provided through telephone/ e-mail during the subscription period.

➢ The proposed solution should support both IPv4 and IPv6.
➢ Bidder shall submit the manufacturer/OEM/OSD/OSO authorization letter to confirm that product/solution is delivered from Manufacturer/OEM/OSD/OSO and Bidder is partner with OEM/OSD/OSO for the above scope of work and submit the same as part of the bid. This agreement should include but not limited to the ownership of the activities, timelines and resources associated to the activities.

1.3) Hardware requirements

The successful bidder must provide all necessary hardware (for both DC and DR) for supporting 50,000 concurrent users from day one with full hardware warranty and support for the complete contract duration. Bidders must include all required compute, storage, network components, OS, database license and any other software licenses required for the solution to work.

LIC shall provide the required SSL/TLS certificates, SMS gateway, data center rack space and other datacenter components.

SSL/TLS certificate quality, LAN IP, Public IP must be given in advance.

The bidder should provide all the required hardware details along with detailed configuration (refer below) required for hosting the Multifactor Authentication and Contextual Access Solution in LIC while submitting the Technical Bid.

1. Bidder must provide enterprise grade rack mounted servers of data center class or OEM appliances.
2. Bidder must ensure high availability and load balancing at SW and HW level with hardware at least at n+1 failure.
3. The overall hardware must be able to support 50,000 concurrent users from day 1.
4. All hardware components like Server with computer, storage, network switch for interconnectivity, network cables should be supplied.
5. All required software components like OS license, database license, any other software licenses must be supplied
6. Installation and configuration of hardware solution must be done by the bidder
7. Complete onsite warranty for all hardware components must be included in the solution for entire contract period
8. The bidder will be responsible for maintenance of the hardware during the entire contract period.
9. The hardware sizing has to be certified by the OSD (MFA solution provider and the hardware OEM)

Exclusion: Following components shall be provided by LIC
1. Rack space
2. Power
3. SMS gateway
4. email gateway

1.4) Process and System Study

The Bidder is expected to study the RFP to gain an understanding of the current and proposed business processes in the LIC. The Bidder is expected to identify business process areas where the Bidder may need to obtain further understanding. The Bidder is expected to identify further process improvement opportunities.

The successful Bidder will be required to create a detailed System Requirement Specification (SRS) document with the understanding. The SRS preparation team of the successful Bidder should be experienced, with full functional knowledge of the software. The LIC reserves the right to ask for

replacement of any team member if the LIC feels he/ she is not adequately qualified for the same. The SRS Document shall be signed off by the LIC on acceptance of the same.

1.5) Design and Architecture

Bidder has to architect the solution deployment after understanding the following details:

- Understanding the Network in terms of Network, Server and Security appliances, LAN, WAN & Internet Links and segments etc.
- Prepare the designs and implement the solution in line with ISO27001:2013 standards as modified from time to time.
- Study of LIC's existing security environment and guidelines and recommend best practices to implement and roll out the solution.
- Study of our present architecture at Data centers.
- Bidder needs to prepare a detailed execution plan.

1.6) Preparation of System Requirement Specification Document

The Bidder is expected to create System Requirement Specification (SRS) Document under the scope of the Multifactor Authentication and Contextual Access Solution implementation including all proposed interfaces and customizations involved. The System Specification Document shall be signed off by the LIC on acceptance of the same.

The Bidder may suggest amendments to the processes that would suit the product solution offered for a seamless integration and document the same to suit the proposed "Multifactor Authentication and Contextual Access Solution" as envisaged in the Study Report. However, the objective and output of the process should not change. On acceptance of the final solution by the LIC, the Bidder cannot deviate from the agreed solution under any circumstance unless agreed by the LIC. The agreed solution shall be binding on the part of the Bidder and inability to deliver the solution may result in annulling the contract and the same being awarded to another vendor as per the decision of the LIC. The LIC shall impose financial penalties or / and invoke the PBG in such circumstances.

The Bidder is expected to prepare the System Requirement Specification Document containing the following details but not limited to:

- Overview of the Process with System/Application FAQs
- Security features
- Application deployment architecture with Hardware topology
- User manual & Run Book
- Version description document
- Application upgradation and patches management document
- Architecture & design document including Traffic flow document between the devices
- IP address allocations to various components
- Project Plan with milestones, resourcing, and deliverables
- Inventory list consisting of hostnames, make, model, serial number
- Testing cases and test results documented before and after implementation.
- Standard Operating Procedures
- Industry Best Practice Use cases and customization for LIC
- Vendor support details and escalation matrix
- OEM support details and escalation matrix
- List of reports related directly/ indirectly to module(s)/ customization/ interface
- IT Security and Backup Architecture and parameterization with relevant details
- Handling of Logs
- User Manual and on-line tutorial
- Performance Measurement Matrix.

1.7) Basic Installation of Hardware and Software

Bidder has to perform following jobs for completing the above mentioned activity:

- ➢ Installation of hardware.
- ➢ Installing the required OS and Applications on Physical Hardware.
- ➢ Configuring IP address and default gateway etc. on all devices
- ➢ Check L2 & L3 connectivity on network using "ping & trace route" commands
- ➢ Installing License for the solution.
- ➢ Enabling of features and functionality as per the technical specifications.
- ➢ Configure the solution in HA mode (either in Active-Active or Active-Standby as specified by LIC while execution)
- ➢ Integration with AD (Active Directory) to facilitate user identification.
- ➢ Configure all automated updates for all features.
- ➢ Configuration of update and upgrades as and when the latest version is released.
- ➢ Configuring backup Schedule.
- ➢ Check for failover.

1.8) Basic Deployment

- ➢ The selected bidder shall deploy Multifactor Authentication and Contextual Access Solution that complies with the technical specifications of the RFP.
- ➢ The Bidder's resources will be required onsite during the deployment phase.
- ➢ The selected Bidder shall assign project manager and associated support personnel for this project. The number of resources required deploying for MFA and Contextual Access Solution implementation shall be provided along with their skillsets (example L1, L2, L3 implementation or Operations) with LIC as part of the final project plan.
- ➢ The solution provider should be able to integrate with all the required, existing, and proposed future IT systems/tools. Solution should integrate with all the third-party endpoint agents like Firewall, DLP, Proxy, ITSM, Encryption, Backup solution clients, industry leading PIM solution, SIEM etc.
- ➢ The proposed solution should support and integrate seamlessly, without any dependency, with the existing VPN in LIC or any other VPN services procured by LIC in future.
- ➢ The proposed solution should enable remote connectivity from trusted endpoints only.
- ➢ The solution provider should provide a detailed implementation Plan of action (POA) for Multifactor Authentication and Contextual Access Solution. It should include the approach, risk, benefits, and downtime (if any). Post approval of POA, solution provider should work with LIC's internal teams and application or business owners to complete the implementation of the solution.
- ➢ LIC will perform its own Vulnerability assessment/ Penetration testing (VAPT) & Risk assessment on the entire solution before going live and the solution provider needs to fix all the vulnerabilities/risks highlighted in the reports at no extra cost to LIC.
- ➢ The Solution provider will deploy and validate all the features in the Multifactor Authentication and Contextual Access Solution including (but not limiting to) Dashboard setup, use cases, auto-remediation of security policies/patches and report customization.
- ➢ Setting up of test environment at LIC site will be Bidder's responsibility.
- ➢ The Bidder should provide the deliverables and sign off for each of the deliverables at various stages of customization and implementation.

1.9) Security Requirements

- ➢ Provide security in compliance with LIC security requirements to protect the confidentiality, integrity, and availability of the information systems.
- ➢ Develop, implement, maintain, and use best in class industry proven safeguards that prevents the misuse of information systems and appropriately protect the confidentiality, integrity, and availability of information systems.
- ➢ Maintain a security plan that complies with industry accepted security requirements. Security Plan should be embedded within the Project Plan & approved by the LIC. The security plan would be reviewed by the LIC during the implementation phase.
- ➢ The Bidder shall abide by the access level agreement to ensure safeguards of the confidentiality, integrity, and availability of the information systems.

- Selected bidder will not copy any data obtained while performing services under this RFP to any media, including hard drives, flash drives, or other electronic device, other than as expressly approved by LIC.
- Standards Benchmark – To ensure that all parties have a common understanding of any security issues uncovered, the independent organization that conducts the VAPT shall provide vulnerability rating's (preferably) based on industry standards as defined by First's Common Vulnerability Scoring System (CVSS) and MITRE's Common Weakness Enumeration (CWE).
- The vendor has to undertake remedial action for any shortcomings pointed out during the course of LICs IS Audit.

2.0) Backup, Archiving and DR

The bidder has to provide a solution for taking backups and archive the replica of the systems' database and the application as well. There should be a provision of adequate Business Continuity Management (BCM) to maintain Business continuity.

The methodology for the backing up of data and its archival has to be provided by the bidder .The methodology or strategy used should be in alignment with LIC's Backup and Archival strategy. The Application should have a capability for easy retrieval of the backed-up data (both application and the database) with least amount of manual intervention with no data Loss events.

The Bidder should provide backup solution for the proposed setup.

The bidder should configure the solution for an active DR without any additional licenses. The DR should be made functional with no manual intervention. The DR should synchronize with the DC and vice versa for any changes that are made on one setup.

2.1) Log Management and Reporting

There shall be provision for complete audit trail of all operations by the users. There shall be provision / functionality to track down all backend modifications as per assigned users' roles and responsibilities if any, by any user, which can be retrieved and analyzed to get the complete history of the issue. The vendor may take it as an input for redressal of the issue, if the same is application related. The solution should be integrated with the existing SIEM solution or any other SIEM Solution procured in future

Log Management and Reporting would involve following tasks:

- Configuring logging and reporting.
- Enable capturing of logs, log retention period and mechanism for archiving logs.
- Creating Out-of-the-box reports and customized reports templates based on the needs of LIC.
- Scheduling of backup.
- Checking up of restoration of Management hardware from backup.
- Configure Incident based alert mechanism supported by the solution like Visual Alerts, e-mail & SMS etc.
- Any reference to reporting mentioned in the tender document.

2.2) Documentation

Full documentation of the project is to be included in the deliverables by the successful bidder. LIC may provide a format for documentation to the successful bidder. Bidder should provide all documents to LIC as listed below (where applicable)

- Project Plan with milestones, resourcing, and deliverables.
- Architecture & design document including Traffic flow document between the devices.
- Infrastructure build document.
- IP address allocations to various components.
- Network Architecture/flow document.
- Inventory list consisting of hostnames, make, model, serial number.

- ➢ Contract number for raising RMA with OEM in case of hardware failure.
- ➢ Testing cases and test results documented before and after implementation.
- ➢ Standard Operating Procedures.
- ➢ Industry Best Practiced Use cases and customization for LIC.
- ➢ Vendor support details and escalation matrix.
- ➢ OEM support details and escalation matrix.

Architectural document requirements:

- ➢ Solution deployment architecture with Hardware topology
- ➢ User manual
- ➢ Version description document
- ➢ Problem reports and Issue logs
- ➢ System/Application FAQs
- ➢ Application upgradation and patches management document
- ➢ Run Book

Bidder is expected to provide user and technical documentation including Installation, Commissioning, Implementation, security check Manuals.

All the documents shall be supplied in properly bound volumes of A4 size sheets. Three sets of hardcopies as applicable and one softcopy on CD shall be supplied as final document. Documents for high level design, detailed design, configuration of individual features set on various appliances, general testing, scenario based fail-over testing, Standard Operating Procedure, best practices etc. shall form the complete set for fulfilling the documentation criteria.

Vendor shall also submit Delivery and Installation Report, Warranty certificates, License Copies for all the items supplied along with the supplies. Installation report should contain the part numbers of all the components supplied by the selected bidders.

2.3) Training

LIC expects the bidder to train the administrator/business users till the personnel gain enough expertise in the system and capable of taking over the training function. The training should include features, facilities, operations, implementation, troubleshooting, system administration, database administration, operating system administration, DR elements. All training will be hands- on training along with the trainer for the users. The Bidder should also provide e-learning facilities for users of the solution.

Training shall be provided on each of the modules to specified LIC personnel. Training shall be provided at no additional cost to LIC through OEM/OSD/OSO approved authorized agencies/faculties.

- Pre-Implementation: Provide training to the LIC personnel/ Onsite and offsite support team on the product architecture, functionality and the design for each solution under the scope of this RFP.
- Post Implementation: Provide hands-on training to the LIC personnel/ Onsite and offsite support team on the day to day operations, alert monitoring, policy configuration for all solutions etc. (this is not exhaustive and may be modified in discussion with the vendor)
- Documentation and knowledge transfer after each patch/version update.
- The bidder and OEM/OSD/OSO are required to provide training jointly as per the below table for people nominated by the LIC for each solution specified in the scope of work.
- The bidder and OEM/OSD/OSO are required to provide ad-hoc trainings to the LIC staff as required by LIC, to acquaint them with the latest features and functionalities of the solutions. LIC has the right to exercise this training option at its discretion.
- The bidder is required to provide all trainees with detailed training material and one additional copy to the LIC for each solution as per the scope of work of the LIC. This training material should cover installation, operation, integration, maintenance, troubleshooting and other necessary areas for each solution.
- All out of pocket expenses related to training shall be borne by the selected bidder.

- The vendor may utilize the OEM/OSD/OSO resources in case the bidder does not have adequately experienced resources for providing training

Solution	Pre-Implementation (Days)	Post-implementation (Days)
As per the RFP	1	2

The detailed training documents should be given to the training participants. The detailed theory & hands-on training should be imparted by the OEM/OSD/OSO Authorized personnel at LIC premises. The training facilities shall be made available by LIC, the Bidder will have to ensure that training is imparted in a professional manner through certified and experienced personnel (other than on-site Personnel) and proper course-ware is given to every person attending the training.

2.4) Acceptance by LIC

➢ A comprehensive "Acceptance Test Plan" document, containing various aspects of the 'Acceptance Test' to demonstrate all the features of the proposed Solution, shall be submitted by the bidder.

➢ Scenario based Acceptance Test shall be carried out jointly by the representatives of LIC and the Bidder after the Installation.

➢ The Bidder's resources will be required onsite during the testing phase.

➢ All security issues identified will have to be either resolved or a mutually accepted remediation should be agreed upon between the LIC and successful Bidder.

➢ The Bidder shall provide test plan, test cases and test results.

➢ The LIC shall commence the User Acceptance Testing only after a formal confirmation that the system is ready for UAT.

➢ The Bidder should provide test cases for UAT for LICs review. Upon finalization of test cases, user acceptance testing will be started by the business users.

➢ Any deviations/ discrepancies/ errors observed during the testing phase will have to be resolved by the Bidder. Any exceptions will have to be documented and signed off by the LIC.

➢ The Bidder shall first deliver the base/UAT version of the software, and the Bidder shall assist LIC to conduct a preliminary test to ascertain the extent to which the software has met business requirements as furnished in the RFP and complies with the specifications.

➢ The Bidder is expected to make all necessary modifications to the solution, customizations, interfaces, etc., if there are performance issues or errors identified during testing. The Bidder will assist LIC in preparing the test cases, including the test data. The Bidder will assist in conducting all the tests and comparing/ analyzing the results. Any bugs identified will have to be rectified and subsequent patches/ versions will also have to be tested without any additional cost to LIC.

➢ The testing also includes testing to ascertain whether the response time, the bandwidth usage & performance of the solution are as per the expectations of LIC and would involve an error free dry run of the customized solution and end-run simulation.

➢ LIC may accept the application software only after the critical or major Bugs are fixed.

➢ The Bidder shall be responsible for maintaining appropriate program change control and version control for all the modifications/ enhancements carried out during the implementation/ testing phases.

➢ The Bidder shall be responsible for providing and updating system & user documentation as per the modifications/Changes done in the MFA and Contextual Access Solution.

➢ Appliances will be considered to have been commissioned when all services as described in this tender document are able to run smoothly to the satisfaction of LIC. Mere installation of appliances with out-of-the box features will not constitute as commissioning of the proposed solution.

➢ The final acceptance will be provided by LIC after verifying all aspects as mentioned in the document have been delivered to satisfaction.

LIC has the right to the following aspects:

➢ Access Control (logical, physical, administrative etc.) of all products has to be shared with LIC officials, but vendor should implement in such a way that accountability can be fixed,

➢ To ascertain the effectiveness and efficiency of the resources deployed

- The vendor will do the necessary changes in the setup as per the changing business needs without charging any cost to LIC.
- Physical verification of Licenses, Software media, technical documentation as per purchase order.
- Registering the Hardware & Software License with OEM/OSD/OSO for validation and desired technical support.

2.5) Go Live

Go-Live is the phase in which the application is made available to all the users to carry out live transaction.

- Before the final Go-Live the Bidder must complete the development/ customization of the application as per the Functional and Technical Specifications agreed with the LIC.
- The Go-Live is an end to end responsibility of the Bidder who will manage total planning, hand holding support as per the scope of work.
- Bidder should provide 45 Days of hand holding support post Go-Live.
- On satisfactory performance of application post 45 days from Go-Live, LIC will issue Completion Certificate.
- Acceptance: A one-month test period will be used by LIC to evaluate the selected Multifactor Authentication and Contextual Access Solution. After the selected solution has been successfully tested and implemented, LIC and the selected bidder shall agree on the start date of the Go-LIVE. If any issues/problems are identified during the test period and Security assessment (VAPT) bidder must fix the same without any additional cost to LIC.
- VAPT exercise shall be conducted by the LIC; it shall be the Bidder's responsibility to rectify the gaps unearthed during the VAPT at no additional cost to the LIC during the contract period.
- The implementation phase shall be deemed as completed in all respects only after
- All applications and services are implemented as per the intent of this RFP.
- All functionalities mentioned in this RFP have gone live.
- All the related trainings are completed, and post training assessment carried out by the LIC

2.6) Guidelines for Maintenance and Support

- Certify and complete continuity planning according to LIC security requirements before moving information systems into a production status. Audits will be conducted by LIC to ensure security, any gaps identified will be remediated by the vendors.
- Vendor should develop a disaster recovery plan for restoration of the system in the event of a disaster or major incident.
- Vendor should follow LIC's Change, Patch & Incident management policies and processes.
- Vendor should maintain audit logs for all monitoring and events according to LIC policy and provide this information upon request. These audit logs must be secure and stored as per defined retention policy.
- All exceptions to be documented and signed off by appropriate LIC personnel.
- Configuration items such as computers and other devices, software contracts and licenses, third party tools and business services which are related to the application should be disclosed.
- Additional guidelines would be provided based on the support scenario that's decided between vendor and LIC.

2.7) Performance and Support Assurance

The System Integrator and OEM/OSD/OSO must provide the following performance assurances on the solution:

- The OEM/OSD/OSO and System Integrator must assure that all types of support including warranty, security, upgrade and maintenance support for hardware, software and any other component shall be available throughout the contract period. Solution/upgrade for any newly emerged threat/vulnerabilities must be provided without any additional cost to LIC.
- Stage of Product life cycle: The Software and engineering support for all the equipment/devices offered in the Total Solution must be available till the end of Contract Period (Taking into account the implementation period from the date of purchase order). During SW and Engineering

support the OEM/OSD/OSOs would continue to develop, repair, maintain, and test the product software including operating system and release appropriate bug-fixes/patches/updates. Documentary evidence for "Stage of product Life Cycle" must be from the information/documents available in public domain.

The System Integrator shall be able to provide reporting and MIS as per the detailed specifications. In case, OEM/OSD/OSO is not able to provide the same, third party software/hardware may be used. For any such third-party tool and/or tool of the OEM/OSD/OSO/s the respective OEM/OSD/OSO of the NGFW will be responsible and accountable for smooth, efficient and effective performance of such tools during the entire contract period

2.8) Compliance with IS Security Policy:

The Vendor shall have to comply with LIC's IT & IS Security policy in key concern areas relevant to the RFP, details of which will be shared with the finally selected Bidder. Some of the key areas are as under:

i. Responsibilities for data and application privacy and confidentiality;
ii. Responsibilities on system and software access control and administration;
iii. Custodial responsibilities for data, software, hardware and other assets of LIC being managed by or assigned to the Vendor;
iv. Physical Security of the facilities;
v. Physical and logical separation from other customers of the Vendor;
vi. Incident response and reporting procedures;
vii. Password Policy;
viii. Access management Policy;
ix. Acceptable usage Policy (Authentication and Identity Management, Authorization and access control);
x. Data Encryption / Protection requirements of LIC;
xi. Cyber Security Policy;
xii. Auditing;
xiii. In general, confidentiality, integrity and availability, non-repudiation, authenticity, privacy of data/information must be ensured;
xiv. Responsibilities in carrying out background verification of personnel deployed from vendor side regularly and submit the report as and when needed by LIC;

2.9) Right to Audit

i. It is agreed by and between the parties that the Service Provider shall get itself annually audited by external empanelled Auditors appointed by LIC/ inspecting official from the IRDAI or any regulatory authority, covering the risk parameters finalized by LIC/ such auditors in the areas of products (IT hardware/ software) and services etc. provided to LIC and the vendor shall submit such certification by such Auditors to LIC. The vendor and or his / their outsourced agents /sub – contractors (if allowed by LIC) shall facilitate the same. LIC can make its expert assessment on the efficiency and effectiveness of the security, control, risk management, governance system and process created by the Service Provider. The Service Provider shall, whenever required by such Auditors, furnish all relevant information, records/data to them. All costs for such audit shall be borne by LIC.
ii. Where any deficiency has been observed during audit of the Service Provider on the risk parameters finalized by LIC or in the certification submitted by the Auditors, it is agreed upon by the Service Provider that it shall correct/ resolve the same at the earliest and shall provide all necessary documents related to resolution thereof and the auditor shall further certify in respect of resolution of the deficiencies. It is also agreed that the Service Provider shall provide certification of the auditor to LIC regarding compliance of the observations made by the auditors covering the respective risk parameters against which such deficiencies observed. All costs for such audit shall be borne by the service provider/vendor.

iii. Service Provider further agrees that whenever required by LIC, it will furnish all relevant information, records/data to such auditors and/or inspecting officials of the LIC/ IRDAI and or any regulatory authority required for conducting the audit. LIC reserves the right to call and/or retain for any relevant material information / reports including audit or review reports undertaken by the Service Provider (e.g., financial, internal control and security reviews) & findings made on the Service Provider in conjunction with the services provided to LIC.

EXPECTED DELIVERABLES (from successful bidder)

➢ The Bidder has to specify the Name of the OEM/OSD/OSO with the product name in the Technical specification.
➢ The Bidder should provide backup solution for proposed setup.

SN	Description	No. of Users	Qty
1	Licenses for the Multifactor Authentication and Contextual Access and Remote connectivity solution for five years as per the RFP, for concurrent users with provision for DR. This should include the warranty, AMC and support for five years.	**10000 scalable to 70,000**	**01**
2	Hardware Requirement (As per Scope of Work)	**NA**	**NA**
3	Implementation Charges	**NA**	**NA**
4	Onsite support , as per the RFP	**NA**	**02**
5	Direct Premium Support (Highest level of support) with 24x7x365 with OEM/OSD/OSO. Vendor to provide this Support for the entire solution.	**Not Applicable**	**NA**

Service-Delivery and Project Management:

The selected vendor will have to post a full time onsite Service-Delivery Manager (SDM) immediately after the signing of the Contract. The detail of SDM should be conveyed in writing to LIC within 6 weeks of receipt of purchase order. The onsite Service-Delivery Manager will be required to be posted for the entire implementation period and has to sit on site at LIC-CO-IT, Mumbai office. The onsite SDM should have the following minimum profile:
(a) Minimum 5 years of IT experience
(b) ITIL aware and having knowledge of Service Delivery processes.
(c) Minimum 2 years of Program Management experience.
(d) 1 years' experience of similar deployments.
(e) Experience of handling/managing teams (Minimum 5 reportees).

The responsibilities of the On-site Service-Delivery Manager as a part of support are as follows (*indicative but not exhaustive*):

(a) Act as a Single Point of Contact (SPOC) for the entire project
(b) Responsibility for the entire execution & management of the project after receipt of purchase order. (ii) Overall monitoring of project
(c) Coordination for Delivery/Installation of New hardware in stipulated time frame
(d) Call flow management, Quality Service Delivery
(e) On-site Team management
(f) Overall monitoring and management of network gateway security and related services
(g) SLA management and reporting
(h) Submission of periodical Reviews and reports required by LIC.
(i) Crisis management and Emergency response procedures.
(j) Preparation and submission of detailed Project documentation to LIC (Purchase Order wise) and progress of initiatives taken by LIC.

(k) He should be placed at LIC premises during LIC's office hours. However, the hours may be extended whenever required.

The Vendor shall submit to ED (IT/BPR), CO, Mumbai the name and contact details, including address, telephone number, mobile number, FAX number/email address of the nominated Service-Delivery Manager.

It is mandatory for the concerned Service-Delivery Manager to have structured meeting with the ED(IT/BPR)/Secretary(IT)/Dy. Secretary(IT)/Assistant Secretary (IT), Security Section of Central Office once a week, preferably on Monday, during the implementation period from the date of receipt of the first Purchase Order by the vendor. Weekly meetings should be held till the project is entirely rolled out.

In short, Onsite Service-Delivery Manager shall carry out and coordinate the various tasks involved in the project like Project scheduling, tracking, monitoring, identifying risks, liasioning with all stake holders (OEM/OSD/OSO, vendors' back-end teams etc.) and reporting to LIC on the overall progress of the project, etc. No charges will be payable by LIC for the onsite Service-Delivery Manager.

Onsite Support Services:

The successful Bidder has to provide throughout the contract period, the services of an onsite L1 & L2 support personnel at Central office (IT), Mumbai with the qualifications and Experience as described below. As per the changing business needs, LIC may ask the Personnel to report for duty in different Time Windows as per the need of LIC.

The successful bidder has to submit a Background Verification Report conducted by Police of all resources deployed (L1 support, L2 support, Offsite L3 Engineer and Service Delivery Manager)

L1 onsite support personnel Qualifications:

a) Graduate in Science/Engineering with at least 1 year of Experience in implementation of the multifactor authentication and contextual access solution.
b) Should have good knowledge on implementation and management of the solution of the solution being procured .
c) Should be in the pay-roll of the vendor i.e. not outsourced.
d) For seamless integration of the entire solution, the onsite support will have to co-ordinate with the various users and projects and resolve the problem.
e) The L1 should be placed at LIC premises during LIC's office hours. However, the hours may be extended whenever required.
f) He should have the competency to educate the users of LIC at Central office with regard to daily jobs; trouble- shoot any related issues etc.
g) If the performance is not up to the mark, the Personnel may have to be changed, if LIC so requests.

L2 onsite support personnel Qualifications:
a) Graduate Engineer (B.E. / B.Tech or equivalent) with at least 2 years of Experience in implementation of the multifactor authentication and contextual access solution.
b) Should have good knowledge on implementation and its functionality
c) Should be able to do day-to-day maintenance of all security devices/appliances/equipments etc. at all locations.
d) Should help to locate, notify and resolve any issue pertaining to the solution .
e) Should be able to do required changes in configuration, policies, etc.
f) Should be in the pay-roll of the vendor i.e. not outsourced.
g) For seamless integration of the entire solution, the vendor will have to co-ordinate with the various projects and resolve the problem.
h) The L2 should be placed at LIC premises during LIC's office hours. However, the hours may be extended whenever required.
i) He should have the competency to educate the Security administrators of LIC at Central office with regard to daily jobs; trouble- shoot any related issues etc.

j) If the performance is not up to the mark, the Personnel may have to be changed, if LIC so requests.

Submission of CV, selection of the onsite Engineers by LIC, other conditions:

Following conditions shall be applicable regarding the onsite L1/L2 support:

a) Details of the concerned candidates along with his/her Curriculum Vitae (CV) are to be provided to LIC along with the photo-identity and supporting documents (duly verified and attested by vendor) within 3 weeks from the date of issue of purchase order/Letter-of-Intent.
b) If required, the candidates (for onsite support at LIC) may be interviewed by LIC officials or LIC's consultant or persons nominated by LIC; including hands on troubleshooting etc. based on which the candidate will be assessed and shortlisted.
c) If the candidate is not found to be suitable, vendor will have to provide an alternate candidate. The selected candidate has to report to the LIC, within 2 weeks of being intimated of the selection by LIC.
d) Shortlisted candidates will also form a standby pool for LIC. Engineers from this pool only will be accepted by LIC for the onsite support (including the standby resource). In case of attrition/resignation, the pool has to be updated on regular basis following the process defined above.
e) In case of a person going on leave, suitable replacement shall be provided from the pool for that leave-period failing which penalty as per the SLA conditions shall be applicable.
f) If any on-site support person leaves before expiry of one year, penalty as per SLA conditions shall be applicable. This will be cumulative in nature for each occurrence.
g) In case the on-site support person is to be changed by the vendor, minimum of one-and-half month (45 days) advance notice shall be given by the vendor to LIC. Additionally, an overlapping period of at least 21 days has to be there between the new and old engineer failing which penalty as per SLA conditions shall be applicable
h) On-site support person may have to be changed by the vendor, if LIC so desires. Notice period for the same will be of 30 days from LIC.
i) The selected vendor will also have to earmark an Offsite L3 Engineer for LIC, who will act as the advisor/consultant for issues and may have to come for meeting at LIC and work on the new initiatives that LIC may take from time-to-time. No charges will be payable by LIC for this purpose

Onsite support additional requirements:

In addition, the onsite support shall carry out and shall be responsible to do following functions for all/respective components of the total solution:

a) Overall monitoring, management, and Quality Service Delivery
b) Data Backup & Recovery
c) Software patches and updates as provided by the OEM from time to time
d) Monitoring of ports, Rules, Change in Rules and its impact analysis
e) Periodic assessments, maintenance, and health audit of individual device as well as that of the overall infrastructure
f) Resolution of both logical and physical issues/ problems relating to the solution and/or related processes.
g) Maintain Device Configuration
h) Crisis management and Emergency response procedures
i) Real time visibility to resource utilization statistics
j) Create and implement Event Management policies
k) Help identify meaningful Events by creating filtering rules
l) Implement Event correlation and filtering though Event Management policies when an Event occurs
m) Disaster Recovery
n) Proactive insights to help remediate issues quickly and also detailed drill-downs to identify the impact quickly.
o) Maintain History of critical events
p) Configuration Backups
q) Plan & Validate critical changes and prepare Change Procedure, Analyze impact of Change and execute approved
r) changes

s) Verify software releases, bug fixes, vulnerability fixes and identify recommended software.
t) Capacity and License Management
u) Log Collection and Analysis
v) Root Cause Analysis for Critical & Repetitive Incidents
w) Preparation of frequently known error datasheet
x) Support scheduled mocks and DR drills.
y) Daily Checklist and Historical Trend Analysis
z) Manage the lifecycle of Change Management Requests, as required, resulting from an Incident, Problem, Service Request
aa) Service Request, Change and Incident Tracker
bb) Audit and Compliance Readiness Support

SUPPORT PLAN:

The Bidder should provide a detailed plan on the support for the Security solution to maintain the system uptime of at least99.9%.

SUPPORT PROCESS REQUIREMENT:

(a) The vendor shall provide an escalation matrix in consultation with the IT/BPR Department, Central Office, LIC for different categories of support calls.
(b) Day-to-day maintenance of the setup.
(c) The support Personnel provided should be conversant with the regular Configuration from scratch, administration tasks, patch management, user management, backup procedures, etc.
(d) The Bidder should ensure that there will be a proper change & configuration management, backup management, security management. These procedures should be well documented, followed and maintained (copy of the same should be submitted to LIC Central Office – IT dept.)
(e) The onsite support Personnel should re-install/ reconfigure any component/ system of the security equipment supplied by the vendor, in case of crash of those components / system on problem or patch/upgrades. The on-site Support Personnel also needs to support, if any security installations done by a separate vendor.
(f) In case the problem is not being rectified by the onsite Personnel even after 1 hour, the issue should be escalated and resolved within 5Hrs from time of incident.
(g) The support Personnel should also keep track of the issues/ticket raised through the web interface help desk/telephone/mail etc. and should provide the solution for the same.
(h) Upgradation of products to the latest version at all the locations, whenever applicable by following a risk-based approach. The procedures have to be documented and submitted to LIC before carrying out any such activity.
(i) The vendor has to do necessary implementations required from business continuity perspectives with respect to network gateway security.
(j) Risk based approach has to be implemented for any change management effected in the configurations carried out.
(k) Root cause analysis of any event has to be done and proper corrective action has to be taken with information to LIC officials. Based on that, the vendor should recommend for improvement to policies, procedures, tools and other aspects.
(l) Alert LIC officials for any unusual occurrence observed.

Note:

➤ No telephone connection will be provided by LIC to the onsite support persons.
➤ The on-site support may also be required to work on Sunday/LIC holidays or beyond office hours on working days, for which an advance notice will be given.

Remote (offsite) Support

The successful Bidder has to provide throughout the contract period, the services of an offsite support beyond LIC's office hours. The roles and responsibilities of offsite support would be the same as that of onsite support as mentioned above. In addition he has to alert/escalate LIC officials (as per matrix provided) in the event of any security threat.

The offsite support has to be provided within 6 weeks of issue of PO. The details of offsite support such as name, Contact no., email ID etc. has to be provided to LIC within the same time period. The complete escalation matrix for offsite support has to be provided to LIC within 6 weeks. The offsite support has to monitor using the VPN setup at vendor end at vendors cost.