TECHNICAL SPECIFICATION

Records Integration and Upgradation

SCOPE OF WORK

S. No	Particulars	Compliance	Remarks
Introduction			
1.	The technology used and the system is obsolete as its already more than 5 years and no upgrade has happened. Newer technologies can utilize hardware resources in a more optimum way. Web technologies available have a very high IOPS compared to the existing one. Indexing for DB is a major issue and reporting happens from the same DB as Read/Write Operations. No Data security measures exist on Data Level and Application Level. No Graphical Dashboard exists. With available data, system is not performing any analysis which will make the decision ease for the management. System is also not providing any considerable analytics.		
Proposed System			
2.	The System will have an open API model to integrate all existing application such ARGIS, ARESA, CPBO and UPAO.		
3.	A centralized Data Repository will ensure that all data are synced with each other and is instantly available.		
4.	A central Repository will also enable central policy management for all functional applications.		
5.	Entry module for Units should be based on latest technologies and Web Services.		
6.	The system will be optimized for low bandwidth factor for remote locations.		
7.	Replicated DB will be provided on the locations so that reporting will be accessed with an ease.		
8.	Graphical dashboard for admin will be available for quickly visualizing details like Vacancies available and shows the people who are qualified for the respective criteria.		
9.	Graphical Dashboard will also give count of posting base don locations, period , ranks etc.		
10.	System will provide details for probable candidates for a selected vacancy based on various policies mentioned in the policy master.		
11.	System will provide analytics based on the location of a unit and also suggest how to improve strength.		

12.	System will provide suggestion where recruitment rallies should be conducted based on the previous locations where rallies have been conducted.		
13.	System will also suggest skill set available.		
Deployment in Cloud Environment and Integrating with other Applications.			
14.	Creating a cloud environment will allow optimum delivery of services and various locations. Record Cloud will enable administrators to shift Infrastructure on the fly to whichever department wherever required.		
15.	Cloud will also enable easy management of various parameters like terminals, servers, devices, signatures etc.		
16.	Integrating it with services like Data Security to keep transparently encrypted at all times, Use PKI to enable Digital Signing of All Documents using CCA India approved tokens and allow login and access privileges based on Single Sign on and Centralized identity and access management.		
17.	Integrating it with ARMS will allow auto triggering of emails to concerned departments like when a posting order is processed an email will be sent to the locations where SOS/TOS is about to occur.		
18.	Integrating Recruitment rally will enable easy generation of requirements, generation of rally locations, auto storing of records for selected candidates through ARTC&s.		
19.	A Consolidated Record Sheet can be accessed by the user from his unit using any terminal or Information Kiosk. The Document will consist of his complete record including his Part II Orders, Salary Statements etc.		
20.	UHD RFID Cards will allow individuals to login. The cards can be linked with PKI to provide digital signatures to all individuals and they can use the cards to login into terminals, access their details from kiosk, or do their day to day work based on their access rights.		
21.	Data Security in form of Authentication, Authorization, Encryption and Audit logs will be available for all transactions including that of the administrator.		

22.	A Centralized policy manager will enable creating of all policies centrally which can be used by various concerned departments like a change in pay and allowances policy, changes in subscription policy, changes in OTTB, changes in porting policy, promoting policy etc.		
23.	The System will Automatically on generation of Pension documents will transfer all details from effective to non-effective DB. This will ensure performance of functional and active DB as non-effective data will not be processed every time.		
24.	Physical documents can be stored with RFID based tags. This will enable locating the file very easy using Tag Finders and also on the system. The racks can be configured with RFID readers and will automatically detect any file available in the specified rack.		
25.	A simplified search option will be provided which will enable operators and users to find details by just typing a keywork and based on their access privileges the system will show search results.		
26.	A detailed MIS for various activities like details of individuals who retired between two dates, personnel belonging to a state, retired on a particular rank etc. will be available.		
27.	A case management module will help in keeping NE but active files in a separate active zone for example files under litigation etc.		
28.	The entire system should be deployed on ARWAN and should be accessible over ARWAN to all locations of AR. The data accessibility has to be optimized for minimum bandwidth consumption using Caching at Local Systems and server side processing.		
29.	The entire system will be deployed centrally through which each branch can utilize their computing power of their localized system and should get the benefits of the centralized Engineered Storage.		
30.	The system should store a Centralized Database which is to be used by all the modules for different branches.		
31.	The system should store all data pertaining to all automations related to records and will be accessed by various automation systems through a central console.		
32.	The system should just take one entry and the same data should be replicated to all other		

	sections of records instantly.		
33.	Data verification will be done by the one single branch or user and same verified data will also be accessible to all other branch.		
34.	The system should give alert to the user if the personnel data is not verified properly and until the process is not completed the system should not proceed to further process.		
35.	The system should check and validate duplicity of the data.		
36.	The system should validate personnel data so that the data should only be saved when the mandatory fields are filled properly.		
37.	The system should perform background audit of each and every entries or transaction made by the user. The audit reports should be available to the System Administrator as and when required and for any specific period and time.		
38.	The system should also track the login details of the user and should generate a login audit report. The Login should be configured with AR Access Key for authentication, encryption and signing if required.		
39.	The system should have common database pertaining data to Posting, Promotion so that systems can instantly use them as and when needed.		
RECORD MODULES			
40.	The system should store master unit details.		
41.	The system should store master ranks details.		
42.	The system should store master branch details.		
43.	The system should store master Qualification Types		
44.	The system should store master cast category.		
45.	The system should store master religion details.		
46.	The system should store master pay scale details.		
47.	The system should store master pay matrix details.		
48.	The system should store master leave category details.		
49.	The system should store master allowances details.		
50.	The system should store master deductions details.		
51.	The system should store master award type details.		
52.	The system should store master state details.		
53.	The system should store master nationality details.		
54.	The system should be capable of Storing the Personal Details		
55.	The system should be capable of Storing the Unit Details		
56.	The system should be capable of Storing the		

	Enrollment Details		
57.	The system should be capable of Storing the Education Details		
58.	The system should be capable of Storing the Address Details		
59.	The system should be capable of Storing the Martial Details		
60.	The system should be capable of creating a Create Level User who will be responsible for BRO Creation		
61.	The system should be capable of creating a Verify Level User who will be responsible for Verifying the BROs Created		
62.	The system should be capable of creating a Authorize Level User who will be responsible for Authorizing the BROs verified		
63.	The system should allow the Create level user to create BROs related to Desertion		
64.	The system should allow the Create level user to create BROs related to Dismiss Details		
65.	The system should allow the Create level user to create BROs related to Posting		
66.	The system should allow the Create level user to create BROs related to Separation		
67.	The system should allow the Create level user to create BROs related to Strength increase		
68.	The system should allow the Create level user to create BROs related to Strength increase		
69.	The system should allow the Create level user to create BROs related to Allowance		
70.	The system allow the Create level user to create BROs related to Awards/Medals		
71.	The system should allow the Create level user to create BROs related to Child Education		
72.	The system should allow the Create level user to create BROs related to Financial Assistance		
73.	The system should allow the Create level user to create BROs related to Hostel		
74.	The system should allow the Create level user to create BROs related to Leave entry		
75.	The system should allow the Create level user to create BROs related to Officiating Pay		
76.	The system allow the Create level user to create BROs related to Pay Fixation		
77.	The system should allow the Create level user to create BROs related to Promotion		
78.	The system should allow the Create level user to create BROs related to Family		
79.	The system should allow the Create level user to create BROs related to Family Planning		
80.	The system allow the Create level user to create BROs related to Former Service		
81.	The system allow the Create level user to create BROs related to Hospitalization		
82.	The system should allow the Create level user		

	to create BROs related to Injuries		
83.	The system should allow the Create level user to create BROs related to Medical Categorization		
84.	The system should allow the Create level user to create BROs related to Miscellaneous Details		
85.	The system should allow the Create level user to create BROs related to Punishment		
86.	The system should allow the Create level user to create BROs related to Qualification		
87.	The system should allow the Create level user to create BROs related to Review of service		
88.	The system should allow the Create level user to create BROs related to Cancellation of BROs		
89.	The system allow the Create level user to create BROs related to Casualty Amendment		
90.	The system should be capable of Uploading BROs Created on the Server Online		
91.	The system should allow the Create level user to Check BRO Details		
92.	The system should allow the Verify level user to Verify BRO Details		
CPBO INTEGRATION			
93.	The system should seamlessly gather data from record and PAO module for bill processing.		
94.	CPBO should only generate the final pay slip of the individuals after the PAO generates the credits statement.		
95.	CPBO can automatically update bill information based on new rank and location where the personnel is posted.		
96.	The system should automatically display provident fund data to CPBO instantly when the data is updated from the GPF section.		
97.	The system should have multi-layered checks to ensure that only eligible individuals pay slips are generated. The slips should have a cross reference from the PAY generated Credit Statement.		
98.	The system should automatically calculate leave encashment of the personnel when the person retires from Assam Rifles		
99.	The system should be able to verify the data entered by the CPBO.		
100.	The system should be able to credit the bill to the individual's account upon successful verification.		
101.	The system should be able to generate credit report for payment after the verification of final bills received from CPBO.		
Requirement Analysis			
102.	Analyse user requirements to arrive at a proposed solution for the system in terms of		

	Software characteristics. This Phase is initiated on approval of a project Proposal. The deliverables this Phase define the proposed System in enough details to justify the recommendations presented and to prepare an implementation plan. This Phase may include following activities: (i) Examine the current System (ii) Define System context and objectives of the proposed System (iii) Build Conceptual Data Model (iv) Build Conceptual Process Model (v) Establish basic System concepts by Conceptualizing Prototype. Prepare a User Requirement Specification and System Requirement Specification and get it approved.		
High Level Design			
103.	Define the overall functioning of the System and establish the Functional and Physical rules and design guidelines. The functional definition of the System is presented in the documentation in a manner understandable to the user as well as development Team. This Phase may include following activities: (i) Build Functional Data Model (ii) Build Functional Process Model (iii) Define System performance criteria (iv) Define Architectural Standards (v) Build Prototype Prepare Functional Specifications for Unit Process		
Low Level Design			
104.	Do the detailed design of the Software components and write specifications of various software components based on High Level Design. The Function design documentation should allow the user to approve the description of each Unit Process and contain sufficient details to allow the development Team to process with System Construction activities. The Phase includes following activities: (i) Build Physical Data Model (ii) Build Physical Process Model Write Specifications for Unit Process		
Construction, Compilation and Testing			
105.	Produce Unit tested Software components. This include following activities: (i) Program Physical Data Model (ii) Program Physical Process Model (iii) Prepare User guides and		

	documentation (iv) Conduct Unit Testing with demo data.		
Training, finalizing implementation			
106.	Providing Training on all modules as per plan and schedule provided by HQ DGAR. The phase will be the final phase which will consist of the following : (i) On Hand Training along with implementation. (ii) Once the users are confident a final phase of training will be provided. (iii) Package will be handed over in running condition.		
Documentation			
107.	Providing Detailed documentation for managing system technically and at User Level. Documentation to Include Technical Documentation & User Manual for the Entire Developed System.		
108.	The software should be platform independent and should run on Linux as well as Windows.		
109.	The system Should run on Virtualized environment.		
110.	The server should run on Linux & Windows		

Hyper Convergent Infrastructure

Sl. No.	Parameter	Specification	Compliance (Yes/ No)	Remarks
1	Make/Brand	HCI appliance OEM shall be in the Leaders category consecutively in last two published Gartner's Magic Quadrant reports on "Hyperconverged Infrastructure".		
2	Hyper Converged Appliance	Hyper converged appliance, which comes Factory Installed with various software including Software Defined Storage and hypervisor. SDS should NOT be top-up or add-on software license bundled on generic x86 server. It should be an integral part of appliance.		
3		Proposed HCI Appliance should be in all flash drive configuration using not more than 2TB capacity drives. Usable capacity per-node should be after all overheads in respect of core/memory/storage being used for deduplication, compression and optimization.		
4		Solution must be able to integrate storage, compute, networking, hypervisor, real-time deduplication, compression, and optimization along with powerful data management, data protection, and disaster recovery capabilities in a standard x86 server building block.		
5		Nodes should offer Storage Features such as De-duplication and Compression. Thin provisioning/ replication /snapshot /auto tiering/ backup license(s) should be provided for the full capacity of the system. Storage performance monitoring software should be included. Future capacity growth shall not warrant any additional software license on the storage landscape.		
6		Proposed hardware must be capable to de-duplicate, compress & optimize all data inline, in real-time with fine data granularity of minimum 8KB data blocks.		
7		Solution should ensure minimum impact to production workloads and guaranteed CPU and RAM available to user applications while doing global dedupe, compression and optimization.		
8		The Hypervisors are to be preinstalled in the nodes along with Cloud / Virtualization Management. The management node requirements, if any should be included by default and management node to be considered outside of the HCI nodes. All offered licenses for virtualization manager are to be of non-embedded type and should have no limitation of functionality.		
9		Should also have capability to use Network		

		Virtualization (SDN).		
10	Nodes Required	Minimum 4 (Four)		
11	Processor	Latest Generation Intel® (Skylake) Processors product family, >=3.00 GHz per Core. Populated with minimum 2 sockets per node.		
12	Total Physical Cores	108 Cores (Including all the Nodes)		
13	Processor Cache	Min. 22 MB L3 Cache		
14	Total Physical RAM	Min. 1 TB DDR4. Scalability to double or more of provisioned RAM		
15	Total Usable Storage	Min. 50 TB Usable capacity post Deduplication and compression for the entire cluster in HA state. The proposed solution must be able to sustain one node failure and it should in no way affect/degrade the production services & usable resources, to the end user application.		
16	Network	Minimum 2 x 10Gb SFP+ (SR) Ethernet ports (each Node) and 4 x 1Gb RJ45 Ethernet ports (Additional ports to be configured by bidders as per their solution requirement). Additionally, Minimum 1 no 1Gb RJ45 Ethernet management port.		
17	Data Protection Features	Backup functionality as an integrated feature or separate server / software license to be offered.		
18		Backup must be an independent copy of source Virtual Server and must allow restore of deleted or corrupted source Virtual Server		
19		Replication across separate datacenter with the ability to carry simultaneous out bi-directional replication between two data centers and with the ability to replicate Any-to-Any in a Mesh Data Center deployment of more than 3 DC's.		
20		The ability to define backup policy per data store, a group of VMs or specific VM		
21		Data Protection should have RPO of 10 minutes for local backups		
22		The ability to execute backup tasks during office hours without impacting to production workloads		
23		Data loss protection against single node failure in cluster		
24		The proposed solution must be able to provide backup reports for audit purpose		
25	Hypervisor	VMWare ESX Hypervisor needs to be proposed with the HCI Appliance for this requirement.		
26		Proposed solution must be able to support the following VM-Centricity and Mobility feature:		
27		i) Backups for specific VMs and Clone specific VMs		
28		ii) Ability to move specific VMs between data centers		

29		iii) VM-level backup instead of forcing protection at the data store or protection domain level		
30	Data Recovery Features	Data recovery should be independent of source Virtual Server		
31		Solution should provide a backup catalog to allow any Virtual Server to be recovered to any specific point-in-time		
32		Data recovery process should be simple with an RTO in minutes		
33	Storage Controller in Nodes	SAS RAID controller with minimum 1GB cache for RAID 0, 1 and 5		
34	Rack Unit	Minimum 2U or higher rack unit (RU) configuration Appliance with Sliding Rails and Cable Management Arm.		
35	Redundancy & Business Continuity	Dedicated non-shared Redundant platinum rated AC power supplies on each of the proposed HCI appliance nodes and should be able to sustain single power supply failure per-node.		
36		Solution should be able to sustain one node failure per cluster.		
37		Solution should be able to sustain 1 NIC port failure per node.		
38		During a single component failure of any type in any node, production services should not be affected or degraded in anyway.		
39		Solution should be able to sustain multiple points of failure with no loss of functionalities or data.		
40		Availability of Data Store with zero RPO for all VMs is to be ensured in the event up to 2 Node failure for the stretch clusters at D3 domain.		
41		In the event of a Hard drive failure, appliance should not be affected and virtual machines should continue to run on the appliance. Drive replacement should be seamless to virtual machines hosted on the appliance.		
42		Solution should be able to sustain 2 SSD Disk failure per physical node, and 1 HDD failure simultaneously in each node of cluster across all nodes in cluster.		
43	Disaster Recovery Features	The solution must provide a simple failover operation.		
44		The solution must allow changing of IP address of recovered Virtual Servers to match target data center.		
45		The solution should allow changing Virtual Server settings (example vCPU, vRAM, vSwitch) if required		
46		The solution must allow the option to test DR failover to separate network with no impact to production workloads		

47		The solution should have feature to assist in failback process to Primary data center		
48		Hyper converged solution should have a guaranteed local cluster backup time of 1 minute		
49		Data Protection should have a minimum RPO of 10 minutes for local backups		
50		Data recovery process should be simple with an RTO in minutes		
51	Manageability	The ability for a single administrator to manage all aspects of the Hyper-convergence from within the Virtualization Manager or server OEM browser based software for all sites.		
52		Globally manage Backup Policies per Data store or per VM.		
53		VM-centric management through a single pane of glass via the virtualization manager or server OEM browser based software.		
54		Programmatic/API interface to enable automated tasks like failover/failback.		
55		System remote management should support browser based graphical remote console along with Virtual Power button, remote boot using USB/CD/DVD Drive. It should be capable of offering upgrade of software and patches from a remote client using Media/image/folder.		
56		Should help provide proactive notification of actual or impending component failure alerts on critical components like CPU, Memory and HDD.		
57		System should support embedded remote support to transmit hardware events directly to OEM or an authorized partner for automated phone home support		
58	Scalability	Minimum scalability of 12 nodes in the same cluster.		
59		Hyper-converged solution must be able to allow in-box upgrade of CPU, RAM and storage capacity as well as scale-out expansion		
60		Hyper-converged solution should support addition of compute/access nodes to provide additional compute resources		
61	Server Security	Should maintain repository for firmware and drivers recipes in the flash drive associated to management port. This is to aid rollback or patching of compromised firmware. Should also store Factory Recovery recipe preloaded to rollback to factory tested secured firmware		
62		For firmware security, Hyperconverged system should support remote management chip creating a fingerprint in the silicon, preventing system from booting up unless the firmware		

		matches the fingerprint. This feature should be immutable		
63	OS Support	Windows 2012 and 2016 Standard/Data Center, SUSE Enterprise Linux, RHEL 6.x, (All latest flavors of Linux and Windows) in Virtual Machines		
64	Serviceability	Proposed Nodes shall provide insights, forecasting and recommendations for quicker problem resolutions including automating case creation or alternate solution on proactive support services with proactive parts dispatch directly from OEM.		
73	Warranty	On-site Comprehensive Warranty and Service including all spares, and service offering with NBD on-site for parts as well as telephone support 24 hours.		

High End Switch

Sr. No	Specifications	Compliance Yes / No	Remarks
1	**Architecture**		
1.1	Modular architecture, minimum four slots for interface modules		
1.2	Shall have two dedicated management module slots in addition to the interface modules		
1.3	Shall have CLOS Architecture or equivalent shared switch fabric capability with minimum four switch fabrics all supporting active switching to support high switching capacity		
1.4	Shall have fully distributed architecture (any additional hardware required for the same shall be proposed)		
1.5	Shall provide distributed Layer-2 (switching) and Layer-3 forwarding (Routing) on all line cards (any additional hardware required for the same shall be proposed)		
1.6	Shall have minimum 3.2 Tbps of switching capacity or higher		
1.8	Shall have 8 x10 G SFP+, 16 x1 G-SFP and 48x10/100/1000BaseT ports from day-1		
1.9	Shall be 19" Rack Mountable		
1.10	The Switch should have operating system with modular architecture		
2	**Advanced Service Modules support**		
2.1	The switch shall support service modules to port applications directly to the switch chassis. This shall include support VPN Firewall module		
3	**Resiliency**		
3.1	Shall have the capability to extend the control plane across multiple active switches making it a virtual switching fabric, enabling interconnected switches to perform as single Layer-2 switch and Layer-3 router		
3.2	Shall support virtual switching fabric creation across four chassis-based switches using 10G Ethernet Links		

3.3	Should support Virtualizes a physical switch into multiple logical devices, with each logical switch having its own processes, configuration, and administration		
3.4	Should support Hot-swappable Modules		
3.5	Passive backplane with no active components for increased system reliability		
3.6	IEEE 802.1D Spanning Tree Protocol, IEEE 802.1w Rapid Spanning Tree Protocol and IEEE 802.1s Multiple Spanning Tree Protocol		
3.7	IEEE 802.3ad Link Aggregation Control Protocol (LACP)		
3.8	Ring protocol support to provide sub-100 ms recovery for ring Ethernet-based topology		
3.9	Virtual Router Redundancy Protocol (VRRP) to allow a group of routers to dynamically back each other up to create highly available routed environments		
3.10	Graceful restart for OSPF, IS-IS and BGP protocols		
3.11	Bidirectional Forwarding Detection (BFD) for OSPF, IS-IS and BGP protocols		
3.12	The Switch support In-Service Software Upgrade (ISSU)		
4	**Layer 2 Features**		
4.1	Shall support up to 4,000 port or IEEE 802.1Q-based VLANs		
4.2	Shall support GARP VLAN Registration Protocol or equivalent feature to allow automatic learning and dynamic assignment of VLANs		
4.3	Shall have the capability to monitor link connectivity and shut down ports at both ends if uni-directional traffic is detected, preventing loops		
4.4	Shall support IEEE 802.1ad QinQ and Selective QinQ to increase the scalability of an Ethernet network by providing a hierarchical structure		
4.5	Shall support Jumbo frames on GbE and 10-GbE ports		
4.6	Internet Group Management Protocol (IGMP)		
4.7	Multicast Listener Discovery (MLD) snooping		
4.8	IEEE 802.1AB Link Layer Discovery Protocol (LLDP)		
4.9	Multicast VLAN to allow multiple VLANs to receive the same IPv4 or IPv6 multicast traffic		
5	**Layer 3 Features (any additional licenses required shall be included)**		
5.1	Static Routing for IPv4 and IPv6		
5.2	RIP for IPv4 (RIPv1/v2) and IPv6 (RIPng)		
5.3	OSPF for IPv4 (OSPFv2) and IPv6 (OSPFv3)		
5.4	IS-IS for IPv4 and IPv6 (IS-ISv6)		
5.5	Border Gateway Protocol 4 with support for IPv6 addressing		
5.6	Policy-based routing		
5.7	Unicast Reverse Path Forwarding (uRPF)		
5.8	IPv6 tunneling to allow IPv6 packets to traverse IPv4-only networks by encapsulating the IPv6 packet into a standard IPv4 packet		
5.9	Dynamic Host Configuration Protocol (DHCP) client, Relay and server		
5.10	PIM Dense Mode (PIM-DM), Sparse Mode (PIM-SM), and Source-Specific Mode (PIM-SSM) for IPv4 and IPv6 multicast		

	applications		
5.11	MPLS and VPLS Support		
5.12	Should support PBR, OSPF, BGP, NSF, MPLS, VPLS from day one		
5.12	Should support Virtual Extensible LAN (VXLAN) with the help of additional linecard		
6	**QoS and Security Features**		
6.1	Access Control Lists for both IPv4 and IPv6 for filtering traffic to prevent unauthorized users from accessing the network		
6.2	Port-based rate limiting and access control list (ACL) based rate limiting		
6.3	Congestion avoidance using Weighted Random Early Detection (WRED)		
6.4	Powerful QoS feature supporting strict priority (SP) queuing, weighted round robin (WRR) and weighted fair queuing (WFQ)		
6.5	IEEE 802.1x to provide port-based user authentication with multiple 802.1x authentication sessions per port		
6.6	Media access control (MAC) authentication to provide simple authentication based on a user's MAC address		
6.7	Dynamic Host Configuration Protocol (DHCP) snooping to prevent unauthorized DHCP servers		
6.8	Port security and port isolation		
7	**Management Features**		
7.1	Configuration through the CLI, console, Telnet, SSH and Web Management		
7.2	SNMPv1, v2, and v3 and Remote monitoring (RMON) support		
7.3	sFlow (RFC 3176) or equivalent for traffic analysis		
7.4	Management security through multiple privilege levels with password protection		
7.5	FTP, TFTP, and SFTP support		
7.6	Port mirroring to duplicate port traffic (ingress and egress) to a local or remote monitoring port. Shall support minimum four mirroring groups		
7.7	RADIUS/TACACS+ for switch security access administration		
7.8	Network Time Protocol (NTP) or equivalent support		
7.9	Shall have Ethernet OAM (IEEE 802.3ah) management capability		
8	**Environmental Features**		
8.1	Shall provide support for RoHS and WEEE regulations		
8.2	Shall be capable of supporting both AC and DC Power inputs		
8.3	Operating temperature of 0°C to 45°C		
8.4	Safety and Emission standards including UL 60950-1; IEC 60950-1; VCCI Class A; EN 55022 Class A		
9	**Software Defined Networking (SDN) Capability**		
9.1	The Switch should have OpenFlowOpenflow 1.3.1 protocol capability to enable software-defined networking from Day one		
9.2	The Switch should Allow the separation of data (packet forwarding) and control (routing decision) paths, to be controlled by an external SDN Controller, utilizing Openflow protocol		

Application Load Balancer

Sl No.	Description of Requirements	Compliance (Yes/No)	Remarks
	Architecture		
1.	Should be high performance purpose built hardware with multicore CPU support.		
2.	The appliance should have 8 GB RAM and 5 Gbps of system throughput to support multiple load balancing features and functions		
3.	The appliance should have minimum 4 triple speed 10/100/1000 Mbps Gigabit copper ports & option for 2 * 10G SFP+ ports		
4.	Solid state drive (SSD) for high I/O performance and dual power supply support		
5.	Hardware based SSL acceleration with 2Gbps of bulk SSL throughput and 2800 2k SSL transactions per second (TPS)		
6.	USB based fast failover support for automated configuration synchronization and improved failover time as compare to traditional cluster		
7.	In order to meet high performance requirements load balancer must support virtual grouping (not clustering) of the appliances and must appear as single system.		
8.	Multiple appliances in virtual group/domain should allow administrator to configure one or more applications application (virtual services) across both physical appliances to meet high performance requirement		
9.	**Load balancing features**		
10.	Should able to load balancer both TCP and UDP based applications with layer 2 to layer 7 load balancing support		
11.	The appliance should support server load balancing algorithms i.e. round robin, weighted round robin, least connection, Persistent IP, Hash IP, Hash Cookie, consistent hash IP, shortest response, proximity, snmp, SIP session ID, hash header etc.		
12.	Should support Multi-level virtual service policy routing – Static, default and backup policies for intelligent traffic distribution to backend servers		
13.	Support for policy nesting at layer7 and layer4, solution should able to combine layer4 and layer7 policies to address the complex application integration.		
14.	Script based functions support for content inspection, traffic matching and monitoring of HTTP, SOAP, XML, diameter, generic TCP, TCPS. Load balancer should support ePolicies to customize new features in addition to existing feature/functions of load balancer		
15.	Traffic load balancing using ePolicies should support algorithms including round robin, least connections, shortest response, persistence ip, hash ip, hash ip and port, consistent hash ip and snmp		
16.	Should provide application & server health checks for well-known protocols such as ARP, ICMP, TCP, DNS, RADIUS, HTTP/HTTPS, RTSP etc..		
17.	**IPv6 gateway and Application acceleration**		
18.	Should provide performance optimization using TCP connection multiplexing, TCP buffering and IEEE 802.3ad link aggregation. Support for TCP optimization options including windows scaling, timestamp & Selective Acknowledgement for enhanced TCP		

	transmission speed TCP optimization option configuration should be defined on per virtual service basis not globally.		
19.	Appliance should provide real time Dynamic Web Content Compression to reduce server load and solution should provide selective compression for Text, HTML, XML, DOC, Java Scripts, CSS, PDF, PPT, and XLS Mime types.		
20.	should provide advanced high performance memory/packet based reverse proxy Web cache; fully compliant with HTTP1.1 to enhance the speed and performance of web servers		
21.	Should provide support for cache rules/filters to define granular cache policies based on cache-control headers, host name, file type, max object size, TTL objects etc..		
22.	Should provide secure online application delivery using hardware-based high performance integrated SSL acceleration hardware. SSL hardware should support both 2048 and 4096 bit keys for encrypted application access.		
23.	Should support certificate parser and solution should integrate with client certificates to maintain end to end security and non-repudiation		
24.	The appliance should support Certificate format as "OpenSSL/Apache, *.PEM", "MS IIS, *.PFX", and "Netscape, *.DB".		
25.	Should support OCSP protocol to check the validity of the certificates online. Certificate bases access control, CRL's (HTTP, FTP, and LDAP) support.		
26.	Should provide full ipv6 support and OEM should be IPv6 gold-certified. OEM should be listed vendor for ipv6 phase-2 certification.		
27.	IPv6 gateway should provide compressive support for IPv6 functions to help with ipv4-to-ipv6 transition without business disruption and must provide support for dual stack, DNS64, NAT 64, DNS 46, NAT 46, IPv6 NAT		
28.	Should support various deployment modes for seamless integration including reverse proxy (IPv6 to IPv4, IPv4 to IPv6) and IPv6 to IPv6 transparent and reverse proxy mode.		
29.	**Network and application security**		
30.	Should support advance ACL's to protect against network based flooding attacks. Administrator should able to define ACL’s rules based on connections per second (CPS) and concurrent connections (CC), cookie value.		
31.	Appliance should have security features like reverse proxy firewall, Syn-flood and dos attack protection features from the day of installation.		
32.	Should support integrated network based firewall to protect against network based attacks; administrator should able to configure the security policies on per interface basis.		
33.	Proposed solution provide integrated WAF functionality to protect against layer7 attacks and should support deep packet inspection of HTTP & HTTPS traffic in reverse proxy mode		
34.	Application firewall should support built in rules to counter application attack, provision should be there to customize predefined application security rules. Should support all kind of attacks including OWASP top 10		

35.	WAF module should support both detection and prevention mode and policies should be enforced on per virtual services.		
36.	**Clustering and failover**		
37.	Should provide comprehensive and reliable support for high availability with Active-active & active standby unit redundancy mode. Should support USB based fast failover.		
38.	should support built in failover decision/health check conditions (both hardware and software based) including CPU overheated, SSL card, port health, CPU utilization, system memory, process health check and gateway health check to support the failover in complex application environment		
39.	Should have option to define customized rules for gateway health check - administrator should able to define a rule to inspect the status of the link between the unit and a gateway		
40.	Support for automated configuration synchronization support at boot time and during run time to keep consistence configuration on both units.		
41.	should support floating MAC address to avoid MAC table updates on the upstream routers/switches and to minimize the failover delay		
42.	Support for multiple communication links for real-time configuration synchronizations including HA group, gateway health check, decision rules, SSF sessions etc.. and heartbeat information		
43.	Clustering function should support IPv6 VIP's (virtual service) switchover		
44.	N+1 clustering support with active-active and active-standby configurations.		
45.	**Centralized management**		
46.	Centralized management appliance should have extensive reporting and logging with inbuilt tcpdump like tool and log collecting functionality		
47.	The appliance should have SSH CLI, Direct Console, SNMP, Single Console per Cluster with inbuilt reporting.		
48.	Should support XML-RPC for integration with 3rd party management and monitoring		

Server and Device Monitor

Ser No	PARTICULARS	COMPLIANCE (YES/NO)	REMARKS
1	Should be a comprehensive management platform that delivers integrated, modular management capabilities across fault, configuration, accounting, performance, and security (FCAPS) needs		
2	Should support minimum 50 wired devices from day 1 and the solution should be scalable up to 1500 wired devices without any hardware or software up-gradation.		
3	Should allow automatic topology discovery and creation of network maps for layer 2 as well as layer 3 networks including all the available VLANs		

4	Should have network inventory polling capability for IP network nodes, available line cards, modules, ports, physical links, VLAN interfaces and all the other SNMP capable devices in the network.		
5	Should allow extensive fault management with real time event and alarm notifications including system logs		
6	Should allow centralized creation and management of VLAN and ACL policies		
7	Should have scheduled device configuration back-up and restore functionality		
8	Should have automatic detection of configuration changes for easy trouble shooting and isolation.		
9	Should allow monitoring and management of 3rd party devices and end points.		
10	Should have the functionality of scheduled configuration roll out		
11	Should have the functionality to perform scheduled or unscheduled network wide software or firmware upgrades		
12	Should have the ability to customize NMS dash board.		
13	Should allow grouping of devices for applying any particular change/task		
15	Should have 64-bit support		
16	Should support centralized as well as distributed deployment.		
17	Should support virtualization management; management and monitoring of both physical and virtual networks. It should provide insight into and management of virtual networks and reduce migration complexity by aligning and automatic network policies with virtual images.		
18	Should support role based access control		
19	Should be with software update and upgrade assurance during the warranty period		
20	Should have support for add-on modules on the same software platform for monitoring and management of routers, wireless controller, wireless access points and wireless client devices.		
21	Should facilitate enable centralized management of proposed network elements with a variety of automated tasks, including discovery, categorization, baseline configurations, software images, configuration comparison tools, version tracking, change alerts, and more		
22	Should support centralized VLAN Management to view current VLAN configuration, VLAN topology, bulk VLAN deployment etc.		
23	(a) Should provide high-performance, scalable network log audit and analysis support with auditing online activities of internal users		
	(b) Should support various log formats such as NAT, flow, NetStream including log formats that allows audit security-sensitive operations and digest data from		

	HTTP, FTP, and SMTP packets		
	(c) Should support policy driven log filtering		
	(d) Should support log collection from devices that do not otherwise support the standard protocols such as Flow, NAT, NetStream, sFlow/Netflow etc.		
	(e) Should support user activity auditing of at least 50 users from day 1 and this should be optionally extendable up to 1500 users.		
24	Should offer following RADIUS/AAA features: (a) Shall support user identity authentication based on the access policies associated with infrastructure resources, such as routers, switches, license for 100 users from day 1. (b) Shall provide a full-featured RADIUS server that supports centralized authentication, authorization, and accounting management. (c) Network-agnostic device fingerprinting capabilities based on HTTP+MAC+DHCP device recognition for BYOD. (d) Shall support authentication modes like 802.1X, VPN, portal, and wireless access identity modes like PAP, CHAP,EAP-MD5, EAP-TLS, and PEAP to fit into applications with different security requirements. (e) Shall provide centralized policy creation to set the appropriate access rights for each type of user and device across the network.		
25	Should be a ITILv3 compliant comprehensive management platform that delivers integrated, modular management capabilities across fault, configuration, accounting, performance, and security (FCAPS) needs.		
26	Offered software should have compatibility with Microsoft Windows or Linux operating systems		
27	Offered software should be scalable up to 1500 wired devices and 1500 users.		

Unified Thread Management

S. No	Specification	Compliance (Yes/No)	Remarks
General Requirements			
(a)	Network security appliance should support "Stateful" policy inspection technology. It should also have application intelligence for commonly used TCP/IP protocols like telnet, ftp etc.		
(b)	The proposed vendor must have a track record of continuous improvement in threat detection (IPS) and must have successfully completed NSS Labs' NGFW Methodology v7.0 testing with a minimum exploit blocking rate of 99%		
(c)	OEM should be in Leaders quadrant of Gartner's – in Enterprise Firewall Magic Quadrant as per the latest report		
(d)	Appliance shall be ICSA certified for Firewall, IPS & Gateway AntiVirus functionalities		
Hardware & Interface requirements			
(a)	14 x 1GE RJ45 inbuilt interfaces, 12 x 1GE SFP interface slots from day one		
(b)	The Appliance should have USB & Console Ports		
Performance and Availability			
(a)	The Firewall should be on multiprocessor architecture with minimum 20Gbps of Firewall throughput & support of 3,500,000 concurrent sessions, and 200,000 new sessions per second from day one and Firewall Latency should not be more than 3µs		
(b)	Minimum IPS throughput of 4500 Mbps for real world traffic or enterprise mix traffic		
(c)	Minimum Threat Prevention Throughput (measured with Application Control and IPS and Anti-Malware enabled) of 3000 Mbps for real world traffic or enterprise mix traffic		
(d)	IPSec VPN throughput: minimum 10 Gbps		
(e)	Simultaneous VPN tunnels: 1000		
(f)	Proposed solution must support minimum 6 Gbps of SSL Inspection throughput		
(g)	Proposed solution must support minimum 10 virtual firewall from day one		
Routing Protocols			
(a)	Static Routing		
(b)	Policy Based Routing		
(c)	The Firewall should support dynamic routing protocol like RIP, OSPF, BGP, ISIS		
Firewall Features			

(a)	Firewall should provide application inspection for LDAP, SIP, H.323, SNMP, FTP,SMTP, HTTP, DNS, ICMP, DHCP, RPC,SNMP, IMAP, NFS etc		
(b)	IPv6-enabled inspection services for applications based on HTTP, FTP, SMTP, ICMP, TCP, and UDP		
(c)	Allows secure deployment of next-generation IPv6 networks, as well as hybrid environments that require simultaneous, dual stack support of IPv4 and IPv6		
(d)	The firewall should support transparent (Layer 2) firewall or routed (Layer 3) firewall Operation		
(e)	The Firewall should support ISP link load balancing.		
(f)	Firewall should support link aggregation functionality to group multiple ports as single port.		
(g)	Firewall should support minimum VLANS 2048		
(h)	Firewall should support static NAT, policy based NAT and PAT		
(j)	Firewall should support IPSec data encryption		
(k)	It should support the IPSec VPN for both site-site and remote access VPN		
(l)	Firewall should support IPSec NAT traversal.		
(m)	Support for standard access lists and extended access lists to provide supervision and control		
(n)	Control SNMP access through the use of SNMP and MD5 authentication.		
(o)	Firewall system should support virtual tunnel interfaces to provision route-based IPSec VPN		
(p)	The Firewall should have integrated solution for SSL VPN		
(q)	Should support LDAP, RADIUS, Windows AD, PKI based Authentication & should have integrated 2-Factor Authentication server support & this two factor authentication can be used for VPN users for accessing internal network from outside and for Local users accessing internet from inside the network and for administrative access to the appliance or all of them		
(r)	The solution should have basic server load balancing functinality as an inbuilt feature		
(s)	Licensing should be a per device and not user or IP based (should support unlimited users)		
Integrated IPS Features Set			
(a)	IPS should have DDoS and DoS anomaly detection and protection mechanism with threshold configuration.		
(b)	Support SYN detection and protection for both targets and IPS devices.		
(c)	The device shall allow administrators to create		

	Custom IPS signatures		
(d)	Should have a built-in Signature and Anomaly based IPS engine on the same unit		
(e)	Signature based detection using real time updated database & should have minimum 10000+ IPS signature database from day one		
(f)	Supports automatic security updates directly over the internet. (ie no dependency of any intermediate device)		
(g)	Signature updates do not require reboot of the unit.		
(h)	Configurable IPS filters to selectively implement signatures based on severity, target (client/server) and operating systems		
(j)	IPS Actions: Default, monitor, block, reset, or quarantine		
(k)	Should support packet capture option		
(l)	IP(s) exemption from specified IPS signatures		
(m)	Should support IDS sniffer mode		
AntiVirus & AntiBot			
(a)	Firewall should support antimalware capabilities , including antivirus, botnet traffic filter and antispyware		
(b)	Solution should be able to detect and prevent unique communication patterns used by BOTs i.e. information about botnet family		
(c)	Solution should be able to block traffic between infected host and remote operator and not to legitimate destination		
(d)	Should have antivirus protection for protocols like HTTP, HTTPS, IMAPS, POP3S, SMTPS protocols etc.		
(e)	Solution should have an option of packet capture for further analysis of the incident		
(f)	Solution should uncover threats hidden in SSL links and communications		
(g)	The AV should scan files that are passing on CIFS protocol		
(h)	The proposed system shall provide ability to allow, block attachments or downloads according to file extensions and/or file types		
(j)	The proposed system should be able to block or allow oversize file based on configurable thresholds for each protocol types and per firewall policy.		

Other support			
	Should support features like Web-Filtering, Application-Control & Gateway level DLP from day one		
(a)	The proposed system should have integrated Enterprise-class Web Content Filtering solution with database which should support over 250 million webpages in 72+ categories and 68+ languages without external solution, devices or hardware modules.		
(b)	Should support detection over 3,000+ applications in multiple Categories: Botnet, Collaboration, Email, File Sharing, Game, General Interest, Network Service, P2P, Proxy, Remote Access, Social Media, Storage Backup, Update, Video/Audio, VoIP, Industrial, Special, Web (Others)		
(c)	The product must supports Layer-7 based UTM/Firewall virtualization, and all UTM features should be supported in each virtual firewall like Threat Prevention, IPS, Web filter, Application Control, content filtering etc.		
(d)	The solution should have the flexibility to write security policies based on IP Address & User Name & Endpoint Operating System		
(e)	QoS features like traffic prioritization, differentiated services,. Should support for QoS features for defining the QoS policies.		
(f)	It should support the VOIP traffic filtering		
(g)	Appliance should have identity awareness capabilities		
(h)	The firewall must support Active-Active as well as Active-Passive redundancy.		
(j)	Solution must support VRRP clustering protocol.		
Management & Reporting functionality			
(a)	Support for Built-in Management Software for simple, secure remote management of the security appliances through integrated, Web-based GUI.		
(b)	Support accessible through variety of methods, including console port, Telnet, and SSHv2		
(c)	Support for both SNMPv2 and SNMPv2c, providing in-depth visibility into the status of appliances.		
(d)	Should have capability to import configuration and software files for rapid provisioning and deployment using Trivial File Transfer Protocol (TFTP), HTTP, HTTPS		
(e)	The solution should have option for firewall configuration audit & compliance check to be done in automated or manula process		
(f)	Should capable to provide a convenient method for alerting administrators when critical events are encountered, by sending e-mail alert messages to		

	administrator defined e-mail addresses		
(g)	Solution must allow administrator to choose to login in read only or read-write mode		

Network Traffic Manager

S No	Description of requirement		Compliance (Yes/No)	Remarks
	BANDWIDTH CONTROLLER			
1	**An additional device for bandwidth control should be provided along with the system. The features are as follows.**			
	General Features	(i) The system should ensure reliable performance for network dependent applications.		
		(ii)The system should reduce the impact of non-strategic traffic, and diagnose and resolve network problems		
		(iii) The system should identify and control bandwidth hogs so that network administrators can identify problem users, applications and websites and apply automated policies to limit or prevent bandwidth allocation.		
		(iv) The system should have the feature to easily monitor recreational traffic like video streaming and P2P sharing.		
	Technical Features	(a) **Real-time Monitoring:** The system should monitor the health of network in real time and give insight about how applications are performing, bandwidth consumed by users, applications across the network		
		(b) **Policy-Based Shaping:** The system should have the feature to prioritize how and when users, applications and websites can consume bandwidth on network.		
		(c) **Interactive Analytics:** Intuitive dashboard feature should be there to visualize activities by all users.		
		(d) **Application Acceleration:** The system should support acceleration and caching features.		
		(e) **Predictive Recommendations:** The system should have the feature to study the patterns and trends in the network and automatically make suggestions to repair and improve network performance.		

		(f) **QX Boost for Skype application:** Improve the quality of experience For voice, video and application sharing. Exinda QX Boost for Skype for Business correlates Skype® call data with network information to provide a complete end-to-end view of your call traffic, down to the Device level.		
	Hardware Features	**(a)Traffic shaping and Acceleration**		
		(i) Shaping Throughput: - 1 Gbps		
		(ii) Concurrent Flows: - 220,000		
		(iii) Packets per second: - 200,000/s		
		(iv) New Connection Rates: - 10,000/s		
		(v) Acceleration Throughout: - 30 Mbps		
		(vi) Edge Cache Throughput: - 50 Mbps		
		(vii) Optimized Connections: - 6,000		
		(viii) APS Objects 250		
		(ix) SLA Objects 250		
		(x) PDF Reports 60		
		(xi) Traffic Policies 1024		
		(b) **Interface Capability**		
		(i) The system should have 1 x RJ45 based dedicated console port for management purpose.		
		(ii) The system should have at least 3 x 1G (Copper) bypass bridge pair and 2x 1G (Fiber) bypass bridge pair. Also, the system should have one additional NIC slot for future expansion.		
		(c) **Physical Parameters**		
		(i) Form Factor: -1U rack mountable		
		(ii) Power Rating: - 17W @ 0.13A, 22W @ 0.16A (Max)		
		(iii) Environment: - 0 deg cel to 40 deg cel, 5% to 90% operating humidity.		

Two units of under mentioned device should provide with the system.

(a)		**<u>SYSTEM PARAMETERS</u>**			
		Speech band	300 to 3400 Hz		
		Modulation	Pulse Code Modulation		
		No. of channels per system	32 (30 speech channels, 1 terminal Signaling and 1 Sync. Channel)		
		Sampling frequency	8000 Hz		
		No of sample bits	8 per channel		
		Total bits per frame	256		

		Bit rate	2048 Kbps ± 50 ppm		
		Construction and Architecture	Chassis based modular multiplexer shelf capable of supporting minimum 12 slots for integration of data, voice, fax and LAN traffic		
		Universal Slots	All slots (other than for power and control) should be universal i.e. capable of accepting any type of voice/data/fax card manufactured by the same OEM.		
		Add-Drop or Drop - Insert Function	a) Should be able to add-drop/drop-insert voice and data at channel (64 kbps) multiple channel (nx64 Kbps) and at E1. b) Add-drop should be software configurable by user in the field		
		Digital Cross Connect function	a) It should have an inbuilt cross connect facility on the same equipment b) Cross Connect : It should be able to map the following voice interfaces: i) E1 to E1 ii) E&M (two wire or four wire) to e1 and vice versa iii) FXO/FXS to E1 and vice versa c) Add-drop should be achievable by software by user in the field		
		Redundancy	Dual controller, dual power with load sharing		
		Protection	1 for 1 protection , E1, T1, FOM		
			PDH ring protection, QE1, QT1, FOM, Mini QE1, 3E1 for DS0 SNCP protection		
		Management	Console, Telnet, SNMP, and In band management support		
			Craft interface port for connection to external LCD display		
			Compatible to a SNMP based GUI network management system		
		No. of Slots	Should have 16 or more hot plug-in slots with capability to support following cards.		
			Single E1/Quad E1 (G.703)/ Mini-Quad E1/3*E1 card-DS0 SNCP protection		
			X.21/V.35/RS232/EIA530		
			2W/4W E&M		
			QFXO/QFXS/12FXo/12FXS/24FXO/24FXS		
			10/100 Base-T Router Card		
			2/4 channel G.SHDSL card		
			8-channel Dry Contact I/O		
			Magneto Interface Card		

		TDMoE (TDM over Ethernet) with 2 Combo GigaBit (GbE) interface for IP uplink		
(b)	**Interface Support: - The system shall support below mentioned interfaces/Cards.**			
	Network Line Interface-E1 should comply with the following specifications:-			
	Number of ports	1E1 / 4E1 / 3E1		
	Line Rate	2.048 Mbps ± 50 ppm		
	Line Code	AMI or HDB3		
	Input Signal	ITU G.703		
	Output Signal	ITU G.703		
	Framing	ITU G.704		
	Connector	BNC/RJ48C , DB25S for Mini Quad E1		
	Electrical	120 ohm twisted pair		
	Jitter	ITU G.823		
	10/100 Ethernet Router Card with capability to handle 64 WANs should comply with the following specifications			
	Number of ports	2 LAN ports, Max. 64 WAN ports, Each WAN port has data rate n x 64K bps, 1≤ n ≤32 (≤ 4Mbps for total of all 64 WAN ports		
	Physical Interface	10/100 BaseT x 2		
	Connector	RJ45		
	Routing protocol	RIP-I, RIP-II, OSPF, Static		
	Supporting Protocols	PPP (IPCP/BCP), MLPPP, HDLC, Frame Relay, and Cisco compatible HDLC, NAT/NAPT, DHCP		
	Diagnostic	Ping, Trace route		
	QoS	Rate limit		
	10/100 Ethernet Router Card with capability to handle 64 WANs			
	Number of ports	8 LAN ports, Max. 64 WAN ports. Each WAN port has data rate n x 64K bps.		
	Physical Interface	10/100 BaseT x 8		
	Connector	RJ45		
	Routing protocol	RIP-I, RIP-II, OSPF, Static		
	Supporting Protocols	PPP (IPCP/BCP), MLPPP, HDLC, Frame Relay, and Cisco compatible HDLC, NAT/NAPT, DHCP		

	Diagnostic	Ping, Trace route		
	QoS	Rate limit		
	Voice Card (8EM) port (interfaces) should comply with the following specifications:-			
	(a) Connector: RJ45 connector (b) Alarm conditioning: CGA busy after 2.5 seconds of LOS ,LOF (c) Encoding: a low or u low user selectable together for all. (d) Impedance: balanced 600 or 900 ohms. (e) Longitudinal rejection : 55 dB (f) Loss adjustment : -21 to +10 dB/0.1dB step transmit and receive (g) Single/ distortion: >46 dB with 1004 Hz, 0 dBm input (h) Frequency response: -0.25 to-1 dB from 300 to 3400Hz (i) Signaling : Type 1,Type 2,Type 3,Type 4,Type 5 transmit only			
	Voice card (12 FXS/ 12 FXO/ 24 FXS/24 FXO) port (interfaces) should comply with the following specifications:-		-	
	(a) 12 FXS/FXO Connector : Twelve RJ11 (b) 24 FXS/FXO Connector : One RJ21X (c) Alarm conditioning : CGA busy after 2.5 seconds of LOS ,LOF (d) Encoding : A-law or μ-law, user selectable together for all (e) AC Impedance: : balanced 600 or 900 ohms (f) Longitudinal Conversion Loss : > 46dB (g) Cross talk measure : Max -70dBm0 (h) Gain Adjustment : -21 to +10 dB / 0.1dB step transmit & receive (i) Signal/ Distortion : > 25dB with 1004 Hz, 0dBm input (j) Frequency Response : - 0.25 to -1 dB from 300 to 3400 Hz, coincide with ITU-T G.712 (k) Loss adjustment: -21 to +10 dB/ 0.1 dB step transmit and receive (l) Signal / Distortion:. 46 dB with 1004 Hz , 0dBm input (m) Frequency response: - 0 .25 to -1 dB from 300 to 3400 Hz , coincide with ITU-T. (n) Ideal channel noise : Max -65 dB Mop (o) Inter- modulation : coincide with ITU-T B.712 (p) 2Wire return loss : > 2 dB echo , > 20 dB signing (q) FXS loop feed : Nominal -48 V dc with 20 mA current limit (r) Signaling : Loop Start, DTMF, pulse, PLAR,			

	Battery Reverse			
	G.SHDSL Line port (interfaces) should comply with the following specifications:-			
	Number of ports	2 or 4		
	Line Rate for 4-channel G.shdsl	n x 64Kbps (n= 3 to 31)		
	Line Rate for 2-channel G.shdsl	n x 64Kbps (n= 3 to 15)		
	Line Code	16-TCPAM, full duplex with adaptive echo cancellation		
	Connector	RJ45		
	Electrical	Unconditioned 19-26 AWG twisted pair		
	Sealing current	Max. 20 MA source current		
	Clock Source	From System, Line		
	Diagnostic Test	G.SHDSL Loopback: To-LINE, To-bus		
	TDM over Ethernet Card			
	Combo Gigabit Ethernet (GbE) Interface	Number of Ports 2 Speed 10/100/1000M bps Connector RJ45 for twisted pair GbE, LC for optical GbE, auto detection		
	Gigabit Ethernet (GbE) Interface	Number of Port 2 Speed 10/100/1000 BaseT Connector RJ45		
	Ethernet Function	MDI/MDIX for 10/100/1000M BaseT auto-sensing Ping function contained ARP Per port, programmable MAC hardware address learn limiting (max. MAC table 8192 (8k) entry)		
	Basic Features:			
	Packet Transparency	Packet transparency support for all types of packet types including IEEE 802.1q VLAN and 802.1ad (Q-in-Q)		
	QoS	User configurable 802.1p CoS, ToS in outgoing IP frame		
	Traffic Control	(a) Ingress packet Rate limiting buckets per port for Ethernet port (b) Supporting Rate-based and Priority-based rate limiting for LAN		

		port. (c) Pause frame issued when the traffic exceeding the limited rate before packet dropped following IEEE802.3X		
	Link Aggregation	WAN support link aggregation		
	Jitter & Wander	PPM: per G.823 Traffic PPB: per G.823 Synchronous*		
	Standard Compliance			
	IETF	TDMoIP (RFC5087), SAToP (RFC4553), CESoPSN (RFC5086)		
	IEEE	802.1q, 802.1p, 802.1d, 802.3, 802.3u, 802.3x, 802.3z, 802.1s, 802.1w, 802.1AX		
	Co-directional port (interfaces) should comply with the following specifications:-			
	Interface	ITU G.703 64 Kbps co-directional interface		
	Connector	120ohm, RJ48		
	Line Distance	Up to 500 meters		
	Loopack	DTE Payload Loopback, Local Loopback		
	Voice Card 12 MAG (Magneto)			
	(a) Connector : Twelve RJ11 (b) Alarm Conditioning CGA busy after 2.5 seconds of LOS, LOF. (c) Encoding A-law or μ-law, user selectable together for all. (d) Impedance Balanced 600 or magneto telephone impedance match. (e) Longitudinal Conversion Loss > 46dB. (f) Gain Adjustment -21 to +10 dB / 0.1dB step transmit & receive. (g) Signal/ Distortion > 25dB with 1004 Hz, 0dBm input. (h) Frequency Response - 0.25 to -1 dB from 300 to 3400 Hz, coincide with ITU-T G.712. (i) Idle Channel Noise Max. –65 dBm0p. (j) Min Detectable Ringing Voltage 16 Vrms. (k) Ringing Detectable Across L1 and L2 (Tip and Ring), L1 and GND (Tip and GND) (l) Single Ring Type: ring for 2 sec. and stop, or ring for 4 sec. and stop. (m) Continuous Ring Type: 1 sec on 2 sec off, or 2 sec on 4 sec off (n) Ringing Send across L1 and L2 (Tip and			

	Ring), L1 and GND (Tip and GND). (o) Signaling Magneto MRD (Ringing across Tip and Ring or Tip and Ground). (p) Signaling Bit A, B, C, D Programmable. (q) Signaling is carried transparently by the digitizing process.			
(c)	**Clock Source**	Internal, E1/T1 Line, External		
(d)	**Alarm Relay**	Alarm Relay: max. Voltage 3 Vdc/ max. current: 1A Fuse alarm, and performance alarm		
(e)	**System Configuration Parameters**	Active Configuration, Stored Configuration, and Default Configuration		
(f)	**Supervisor**			
	RS232 Console Port (VT100)	10 Base-T, Ethernet, SNMP In-band 64 Kbps supports HDLC/PPP, SSH		
(g)	**Performance Monitor**			
	Separate Registers	Network, user, and remote site		
	Performance Reports	Reports include E1 Bursty Errored Second, Severe Errored Second, and Degraded Minutes. Also available in Statistics (%)		
	Alarm Queue	To record the latest alarm type, location, and date & time		
	Threshold	Bursty Seconds, Severely Errored Second, Degraded Minutes		
(h)	**Diagnostics**			
	Loopback	E1/T1 interface (Line Loopback, Payload Loopback, Local Loopback), DTE Loopback (DTE-to-DTE, DTE to Line)		
	Test Pattern	For Controller: 221-1, 215-1, 211-1, 29-1, and 4-bye user define pattern		
(j)	**Front Panel**			
	LED	1 per V.35-interface, ACO, Power, SYNC/TEST, LOF, BPV, RAI/AIS		
(k)	**Physical /Electrical**			
	Dimensions	432.4 x 220 x 223.5 mm (W×H×D)		
	Power	Single/ Dual -48 Vdc: -36 to -75 Vdc, 100 Watts max.		
		Single/ Dual -48 Vdc: -36 to -75 Vdc, 150 Watts max.		
		Single/ Dual -24 Vdc: -18 to -36 Vdc, 150 Watts max		
	Temperat	0-55°C		

	ure			
	Humidity	0-95%RH (non-condensing)		
	Mounting	Desk-top stackable, 19" /23" rack mountable		
	Line Power supply	Available only with DC power for G.SHDSL card only		
	Power Consumption	Max 110 Watts		
	The OEM should have authorized R & D & Repair/Replacement center in India with presence in India of about 10 Years			
(l)	**Certification**	EN55022 Class A, EN50024, FCC Part 15 ,Class A, FCC Part 68, CS-03, IEC60950, UL60950, IEC 61850-3, IEEE 1613		
(m)	**Compliance**	ITU G.703, G.704, G.706, G.732, G.736, G.823, G.826, G.711, G.712, G.775, O.151, V.11, V.28, V.54		
(n)	**Card Configuration required as part of supply.**			
		Controller (CPU) card -1 no		
		48 V Dc Power Supply Card- 1 No		
		3-Port E1 card – 1 No		
		2-port Router Card – 1 No		
(p)	**DC Power Source (-48V)**	**(j)** Input 230 VAC (Range 170-264 VAC, single phase, 50 Hz).		
		(k) Output Current :- 8 Amp		
		(l) Size: - 485(W) x385(D) x165(H) mm with screw terminals at front		
		(m) Should have short circuit protection.		

Hardware Security Module

S. No.	Description of requirement	Compliance (Y/N)	Remarks
Functional Capabilities			
(a)	Must support cryptographic offloading and acceleration		
(b)	Should provide Authenticated multi-level access control		
(c)	Must have strong separation of administration and operator roles		
(d)	Capability to support client authentication		
(e)	Must have secure key wrapping, backup, replication and recovery		

(f)	Must support unlimited protected key storage		
(g)	Must support clustering and load balancing		
(h)	Should support Logical cryptographic separation of application keys		
(j)	Must support —k of n‖ multi-factor authentication		
Application Program Interfaces (APIs)			
(a)	PKCS#11, OpenSSL, Java (JCE), Microsoft CAPI and CNG		
Host connectivity.			
(a)	Dual Gigabit Ethernet ports (to service two network segments)		
Cryptography			
(a)	Asymmetric public key algorithms: RSA, Diffie-Hellman, DSA, KCDSA, ECDSA, ECDH		
(b)	Symmetric algorithms: AES, ARIA, Camellia, CAST, RIPEMD160, HMAC, SEED, Triple DES		
(c)	Hash/message digest: SHA-1, SHA-2 (224, 256, 384, 512 bit)		
(d)	Full Suite B implementation with fully licensed ECC including Brainpool and custom curves		
Security compliance			
(a)	FIPS 140-2 Level 3		
Safety and environmental compliance			
(a)	Compliance to UL, CE, FCC part 15 (for Commercial products)		
(b)	Compliance to RoHS2, WEEE		
Management and monitoring			
(a)	Support Remote Administration —including adding applications, updating firmware, and checking the status— from NoC		
(b)	Syslog diagnostics support		
(c)	Command line interface (CLI)/graphical user interface (GUI)		
(d)	Support SNMP monitoring agent		
Physical characteristics			
(a)	Standard 1U 19in. rack mount with integrated Smart Card Reader		
Performance			
(a)	RSA 2048 bit signing performance 3,000/second and RSA 2048 key generation performance min 10 keys/second		

(b)	ECC 256 bit prime curve signing performance 5000 /sec and ECC 256 bit key generation performance - 800/sec		
Custom Application			
(a)	Should enable secure execution of custom security-critical application code within the tamper resistant hardware boundary		
Key Generation and Protection			
(a)	Ability to generate RSA keys (2048 and 4096) on board on demand and shall be secured by high security module in accordance with FIPS 140-2 level 3 recommendations for Cryptographic Modules Validation.		
Key back up and restoration			
(a)	The proposed solution must include the software/hardware to - securely store the keys at DC, at DR and at one remote location and restore them in case of necessity		
No. of Keys to be protected			
(a)	The HSM must secure a minimum of 1 lakh keys in accordance with FIPS 140-2 level 3 standards. The licensing and HSM hardware must have no restriction on the number of keys to be protected		
Performance upgrade of HSM			
(a)	The performance of HSM should be upgradable on field.		
Instant Key reflection			
(a)	Multiple HSMs to be supportable for DR, key backup, key update, and key processes, load balancing and failover. Should support instant key reflection to all the HSMs in the system.		
Logical partitions			
(a)	Unlimited logical/cryptographic separation of application keys. all The licenses must be included		

Authentication Server

SL.	PARTICULARS	Complied (YES/NO)	Remarks
	Authentication Server		
1	Should support Windows server 2008 & Windows 2012		
2	Microsoft Active Directory,ADAM,MS Microsoft SQL Server,Open LDAP,Novell eDirectory		
3	Should support Microsoft CA, Check Point VPN, Entrust, Windows Logon, Single Sign-On		
4	Should support hardware and software authenticators.		
5	Should provide load balancing and failover capabilities using multiple primary and replica servers.		

6	Easy integration with applications such as Citrix, OWA, IIS, IAS		
7	Should have extensible SDK to support integrations		
8	Should have built in support for HSM with Remote PED		
9	Should have support for OTP, CBA, Context based authentication		
10	The Access Key should be under Gartner's Magic Quadrant for at least three consecutive years.		

Network Time Server

Sl No	Description of Requirements		Compliance (Yes/No)	Remarks
	Power Supply:			
1	Voltage	230 +/- 10% V AC		
2	Frequency	47-55 Hz		
	Funtions/ Features :			
3	Time Facility	Using Universal Time co-ordination(UTC)		
4	Propagation delay Compensation	Supported		
5	Accuracy	# +/- 250 Nanosecond		
6	Time Accuracy	Better than 1 PPM		
7	LCD Display	Front panel LCD display to show status, time and no. of satellites		
8	**Inputs**	GPS Antenna input through BNC connector.		
9	**Outputs**	Power Supply		
10	NTP output (2 nos. customizable) for NTP client access through RJ-45 .Both Ports shall be independent			
11	RS232 serial port output (2 Nos)			
12	Pulse output: 1 PPS, ½PPM, 1PPM (Configurable).			
13	Support Client request per Second	10,000		
	Antenna			
14	Length of GPS	50 meters		
15	Gain	Over 30 DB		
16	RECEIVER,GLOBAL POSITIONING SYSTEM,DISPLAY TYPE:LCD;DISPLAY SIZE:2 X 3.5 INCH;DISPLAY RESOLUTION:240X400 PIXELS;DATA INTERFACE:ETHERNET;PC INTERFACE:ETHERNET;;EXPANSION SLOT TYPE:USB;WAY POINTS:2; Server FREQUENCY:48-55 HZ;			

	OPERATING TEMPERATURE:0-55 DEG.C;ELECTRICAL RATING:230 VAC;ADDITIONAL INFORMATION:WITH ANTENNA and Surge Arrestor			

Authentication Tokens

Ser No	Description of Requirements		Compliance (Yes/No)	Remarks
1.	Certification	FIPS 140-2 Level 2 or as per CCA Guidelines CC / EAL 4+		
2.	Asymmetric Key Operations	• PKCS#11 compliant • RSA signature: 2048 bit or higher • Secure hash: MD5, SHA -1, SHA-256, SHA -512 ECC P-Curves		
3.	Memory	64 KB or more		
4.	Credential Storage	• X.509 V3 certificates, • secure symmetric key storage • Microsoft Windows Credentials		
5.	Platform Support	Windows7, 10, Windows Server 2012and higher server OS, Linux OS		
6.	Random Number Generator	ANSI X9.31 PRNG or NIST DRBG SP 800 90 CTR mode		
7.	Data Transfer rate	125 Kbps or more		

Lightning Protection System

Sl. No	Description of Requirement	Compliance (Yes/No)	Remarks
1.	The Lightening protection should have radius of protection of 79 meters in Zone-I at 5 mtr height.		
2.	The Lightening Arrestor Should have profiled, in alterable and good conductor structure to generate a forced air circulation at its tip and in prolonged (Venturi System) air intakes and peripheral ejectors.		
3.	The Lightening should have mechanical stimulation system, no battery or electronics is to be used.		
4.	Lightening Arrestor should be equally effective of both positive and negative lightning strikes.		
5.	The necessary fixing bracing PCC/grouting above the building/installation with testing commissioning to entire satisfaction of Engineer- in —charge		
6.	The installation of the system shall be carried out under the supervision of certified trained engineer from OEM of complete all as specified and directed.		
7.	The certified Engineer have to produce the Certificate of Certified Engineer from OEM and having knowledge of International Standards.		
8.	Supply and installation of gun metal elevation rod 2 mtrs long from OEM with necessary bracing clamps, drilling,		

	1 fixing and grouting arrangement etc complete all as specified and directed		
9.	Supply and laying underground LT cable PVC insulated, PVC sheathed copper conductor single core,70 sqmm with necessary connection, laying, clipping on insulated pads, saddles all as specified and directed		
10.	Should provide M&L for Gel compound earthing with earth enhancing compound with 25kgs including copper earth strip of size 25x3 mm with necessary clipping on insulated pads/saddles with earth pit to minimum resistance value complete all as specified and directed		

Smart Rack

Description	Paramter	Technical Requirement	Compliance (Yes/No)	Remarks
System specifications	(WxDxH)	Maximum 800x1200x2150mm(42U)		
	Power supply input	Minimum Dual Feed AC 230V/1P/50Hz.		
	IT Load	3kW		
	Minimum Usable U space for IT Equipments	34 U		
	Installation Site	Should be suitable for Elevated floor installation / general ground installation		
	Utility Entry	Should have provision for both Top/Bottom as Standard		
	System supported languages	Should support English as language for operation by default		
	Cabinet interior lighting	LED - with door limit switch		
	Exterior colors	Black or as per OEM standard		
	Front & back door	Front toughened glass, rear plain dual door		
	Local interface	Colour TouchScreen Display		
	Monitoring	Power, Cooling, Smoke, WLD, temperature and humidity, UPS, door sensor to be integrated for monitoring		
	Sensor	Minimum 1 No. Spot sensor for water leak detection		
		Minimum 1 No. Temperature and humidity sensors		
		Minimum 1 No. Smoke sensor		
		Minimum 1 No. Proximity sensors for doors		
		Minimum 1 No. Beacon- for local alarm		
Power subsystem	UPS capacity	Minimum 6 kVA UPS		
	UPS rated input	230VAC		
	Input Voltage Range	160 V - 285 V		
	Input Frequency Range	40-70Hz		
	Input Power Factor	0.98		
	Input power consumption meter	Energy meter with digital display should be installed at input to monitor		
	Output Max Power	6kVA/5.4kW		
	Efficiency	94% at 100 % Load in online & 98%in Green Mode		
	Backup Time	15 Mins - 1 Battery Pack		
	RPDU parameters	Basic Rack PDU should be provided, Zero U, 32A, 230V,		

		(20)C13 & (4)C19		
Cooling subsystem	Total air conditioning cooling Capacity	3.5kW		
	Minimum Air flow	700CMH		
	Air conditioning installation	Should be Rack mount type, not more than 5U		
	Outdoor ambient temperature	-20℃ ~ +45℃		
	Refrigerant	Environmental Friendly R410A		
	Emergency fan module	Minimum 1 No. at front (Inlet) and top (Exhaust)		
		OEM for UPS, Racks, PDU, Sensors should be same including the monitoring software. OEM should be minimum ISO 9001, ISO 14001 and ISO 50001.		