

REQUEST FOR PROPOSAL

Scope of Bid:

First Security Islami Bank Limited, Dhaka, Bangladesh wishes to receive bids for the below-mentioned Item:

Lot No.	Item Details
1	Privilege Access Management solution.
2	Total Number of Admin Users: 50
3	Total Number of Devices: Unlimited

Bidder's Qualification:

1. The bidder should be a company registered and working in Bangladesh having good business record for last 10 years.
2. The Bidder must have at least two (2) implementations of any internationally reputed (which been in the PAM leader or challenger or Visionaries quadrant of Gartner Magic Quadrant) PAM solution experience in Bangladesh which been running successfully in Banking sector for minimum of last two (2) years in production environment. Work Completion certificate/Customer letter/proof needs to be provided to understand the PAM practice experience of the bidder.
3. The bidder should have all necessary licenses, permissions, consents, no objections, approvals as required under law for carrying out its business.
4. **OEM relationship:** The bidder must be a direct partner of the offered OEM solution vendor for at least last two (2) years in Bangladesh. Manufacturer Authorization Letter from OEM needs to be provided to support it. No 3rd party letter would be accepted.
5. Bidder must provide training for proposed solution by OEM/Local Resource.
6. Solution must have a security certification on vault.
7. Implementation must be done by Local PAM certified engineer.
8. Local Implementation engineer should have any certification on Linux (RHCSA/RHCE), certification on security solutions like VM, WAF, email security, load balance and must be PAM certified.
9. The bidder must provide local + OEM support for the product, with direct support ticket opening facility for easy support and maintenance.
10. The proposed solution can be Linux/Windows based and must be hardened by OEM.



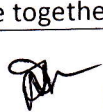

Technical specifications for RFP

Lot 01: Privilege Access Management Solution

Type		Privilege Access Management Solution	
OEM Name			
SN	Requirements	Compliance (Yes/No)	Response
	Market Recognition		
1	Proposed solution must be recognized as <ul style="list-style-type: none"> a) Leader or Challenger in the Gartner Magic Quadrant b) Leader or Visionaries in the Gartner Magic Quadrant NOTE: OEM solution must meet both above criteria to be qualified for evaluation/ proposal submission.		
2	Proposed PAM Solution must have high ranking (above 4.5) in Gartner Peer Insights reviews. NOTE: OEM solution must meet above criteria to be qualified for evaluation/proposal submission.		
	Mandatory Features		
3	The solution shall secure and manage privileged passwords and session of systems and applications effectively.		
4	The solution shall support the ability to manage passwords and perform session recording for the privileged accounts on multiple platforms.		
5	The solution should be able to assess privileged account security risks.		
6	The solution shall provide all the components, including the vault, the central policy administration, the behavior management, and the database in the same OVA or in Appliance.		
7	Secured platform - main password storage repository should be highly secured (built-in firewall, hardened machine, limited and controlled remote access etc.) where the super administrator user should not be accessible via web interface/remote client.		
8	Solution must send alerts when attempts are made to execute critical or dangerous commands (this is a mandatory requirement).		
9	Solution must not require any external database that needs to be licensed separately.		
10	The solution shall have the capability to search across both text and windows-based recording by keywords, time, users, and target address.		



11	The system should allow users to copy and paste the passwords without seeing it.		
12	The system must have the capability of executing privilege commands without giving the access to the network operator.		
13	The solution shall be able to provide intelligence-driven analytics to identify suspicious and malicious privileged user behavior.		
14	Solution must have task manager which will help to execute any privilege task without any human intervention.		
15	The solution must have the capability to save session instance file into local drive for security & flexibility.		
16	The solution must have its own clustering technology which reduces the burden of configuration, managing and operating a Highly Available solution.		
17	The solution should be able to jump server RDP/SSH connections. The user should be able to proxy RDP/SSH connection using RDP/putty client without being logged into the main interface.		
A	Architecture		
18	The solution should have a Generic Target System Connectors to enable one to use this connector for non-standard devices etc.		
19	The solution should have Multi-tenant architecture compatible with service providers' environments, with a complete isolation of instances		
20	The solution should support DC & DR Concept.		
21	The solution must have inbuilt capability – HA, Disaster recovery, Backup and restore, Management API's		
22	The solution must have Easy and efficient deployment toward quickly attainable milestones resulting in better control over implementation and cost, while also optimizing the Total Cost of Ownership		
23	The PAM solution must be protected with OEM hardened and Security plugin included.		
24	The solution should be residing on hardened OS with OS being only Linux and Database should be inbuilt.		
25	The solution must be agentless for session and password management.		
26	The solution must support live session sharing for RDP protocol.		
27	The proposed solution must provide All-in-One Solution where the database and application levels are together.		

28	The solution should be available as On Premise or On Demand		
29	The solution must be Available as a hardware appliance for virtual machine, or as a software		
30	The solution should have only proxy-based architecture for connections to RDP, SSH		
31	The solution should also work without a browser using native applications (mstsc/ssh/putty).		
32	The solution must provide REST-API without any licensing cost.		
33	The solution Should support full customization of logo, fonts, text, disclaimer on login page, Background Images, Names etc.		
34	The solution only uses RDS/Terminal server to host web applications & thick clients.		
35	Solution should not install any ActiveX, Java, Plugins in the browser \ end user machine		
36	The Solution must support Active-Active Configuration.		
37	The solution vendor must provide OS & Database updates & Patches for solution in future.		
38	The solution should provide the flexibility to push all the logs to an external storage automatically without any human intervention		
39	The solution should have all the configuration options only from the front end of the application.		
40	The solution should log all activities, issues, errors in the front end in the form of syslog's		
B	Session Management		
41	The solution should record all videos on the PAM server		
42	The solution should gather metadata to supply dashboards with detailed and context-relevant information		
43	The solution should have feature to OCR through sessions to read the meta data of a privileged session		
44	The solution must have Complete audit logs and advanced searches to isolate incidents		
45	Video recorded & metadata, system logs, audit logs should be downloadable.		
46	The solution should allow auditors to monitor privileged users on demand real-time		
47	The solution audit logs should clearly show who accessed which target device with duration (start time & end time)		
48	The solution should automatically connect disconnected sessions		
49	The solution should also have flexibility to maintain session		



50	The solution should allow flexibility for users to automatically login to target devices with primary accounts		
51	The solution should provide high quality resolution video logs with the flexibility of increasing & decreasing resolution		
52	The solution should have exception policy to enable or disable video log for critical and non-critical devices.		
53	The Solution should restrict hop on feature – block mstsc at port level		
C	Access Management		
54	The solution must have Automatic session termination based on actions interception: blacklist, widget event, reports, process sequences, keyboard traffic		
55	The solution should be able to log commands for all commands fired over SSH Session and for database access through ssh		
56	The solution must have option to enable and disable of warning to user on blacklisted commands before terminate the ssh based session.		
57	The solution should support workflows designed with context relevant access configurations		
58	The solution must identify accounts at risk and map your privileged accounts using the Discovery.		
59	The solution must enforce regulatory requirements through traceable audit trails and separation of operational tasks from administrative Perimeter		
60	The solution should support checkout \ Check-in of passwords		
61	The solution should support quota on approvers for instance if 2 out of 3 approvers approve, request for access is approved		
62	The solution must support auto approvals within specified time approvals		
63	The workflow server access request should have flexibility to increase \ decrease time for requested session		
64	The workflow request for users should have free text field to write reason for access \ justification		
65	The workflow feature should have the flexibility of extend or reduce the time of an existing approved request and also deleting the approval request.		
66	The solution should provide a web portal for users and administrators to track operations more efficiently and in real-time.		
67	The solution should have Global search feature.		





68	The solution should Protect assets and systems through set rules that can automatically authorize or revoke user access		
69	The solution should provide logs for approval history for privileged sessions		
70	The solution must provide authentication history for all users logged within a specified time		
D	Credentials Management		
71	The solution should be agentless in true sense in performing the following Session recording, Session recording, Command process restriction, Password management		
72	The solution should have dedicated plugin library for target password management		
73	The solution should support Enforce periodic change and rotation of passwords		
74	The solution should store all passwords in a secured vault with encryptions like AES 256 bit		
75	The solution should auto change the passwords if not checked in with in the specified time limit		
76	The solution should support Break the glass feature in case of emergency or outage of PAM servers.		
77	The solution must be capable of changing passwords for service account via API		
	Privileged Activity Monitoring		
78	The solution should have the ability to record privileged sessions on Windows, Virtual servers, Unix/Linux, Routers/switches, Database and applications.		
79	The solution must have a Dynamic Visualization that shows all sessions behavior on real-time which could be helpful for Security Operations Center (SOC).		
80	The solution should have a Threat Radar which should monitor all ongoing sessions and indicate any behavioral change graphically.		
	Additional Features		
81	The solution shall have option to secure and manage SSH keys and session of systems and applications effectively.		
82	Solution must have built-in functionality to integrate with Docker and Kubernetes containers.		
83	Solution must have task manager which will help to execute any privilege task; allowing a user to execute a specific task without the need of password granting or privileged session authorization.		

84	Solution shall have features around management, and protection of SSL digital certificates on PAM's infrastructure.		
E	Integration		
85	Solution must bulk onboarding feature for users, servers, domains, restrictions, groups etc.		
86	The solution should support access to Consoles, business web applications, and fat clients (e.g.: firewall management, Salesforce, or Sage)		
87	The solution must have Bi-directional SIEM integration for advanced reporting and real-time processing of malicious behavior detection		
88	The solution should have Open architecture to enable integration with third party vaults		
89	The solution should support Unix or Windows operating systems, network devices, databases, mainframes, virtual infrastructures, or SU/SUDO injection		
90	The solution must support following protocols for integration like HTTP/HTTPS, RDP/TSE, SSH, Internet, SFTP.		
91	The solution should support following authentication methods like Identifier, LDAP, Active Directory, Radius, TACAS+, Kerberos, X509, OTP, Web SSO		
92	The solution must have capability to integrate SNMP & e-mail monitoring tools, ticketing tools and workflows for administrator notifications.		
93	The solution should support Easy provisioning and synchronization with central Identity Access Management solutions within the REST API.		
94	The solution should support Delegation to third-party systems for user authentication and identification (SAML 2.0)		
95	The solution should have capability to create connectors on the fly to meet needs to technology products at the client end		
96	The solutions support Direct access to resources using native clients (PuTTY, WinSCP, MSTC, OpenSSH, etc.) with connection rules embedded directly into the PAM.		
97	The solution should support remote app management		
98	The Solution should not use any vendor provided thick client/agent application; it should work seamless with all major browser & Native applications		
F	Security		
99	The solution must have certifications. Please mention certification of the offered product.		
101	The Solution should only have custom Linux OS,		



	And the PAM Server must be hardened with Memory Corruption Defenses, Filesystem Hardening, Miscellaneous Protections, Role Based Access Control (RBAC).		
102	The solution database must be encrypted with custom encryption key to protect the solution.		
103	The solution must support backup of PAM configuration with encryption key. Where every configuration backup may have unique encryption key. And the restoration process should be security with the encryption and cannot be done without multilevel passphrase.		
104	The solution should store Password and SSH keys safekeeping in the certified vault (minimum AES 256-bit encryption)		
105	The solution should only support authentication for target devices on the Privileged Access management server and not on the user's machine		
106	The solution should have high encryptions standards like AES 256bit encryption		
107	Hardening of PAM server will be done by the vendors with DDOS protection		
108	Solution should use State of the art cryptography protections are used to secure the PAM users & target devices for privileged access		
109	The solution must support transparent mode		
110	The solution should not provide direct access to PAM Database		
111	The Solution should be capable to install TLS Certification of the devices on the PAM server for security		
112	The solution must have multiple levels of authentication to reach to the PAM database logs		
113	The solution should have video logs which cannot be tampered along with the flexibility to delete additional logs by only means of a custom command.		
114	The solution should only be connected using a custom port. The default ports like 22 & 3389 should not be used to connect to PAM servers		
G	Reporting		
115	The solution should have reporting feature for meaningful use		
116	<p>The solution should have reports like</p> <ul style="list-style-type: none"> • PCI • Traceability (access groups, password policy, password strength etc.) • Access to the system (logged Users, Access History, source access) • Events (Password Operation, Password view, backup performed, audit tracking) 		

	<ul style="list-style-type: none"> • Credentials (password use, users by group, policy definition, managed credentials) • Access Control (Access Control logs, Access Groups changes) • Permissions (user role, user profiles, role permissions, profile permissions) 		
117	Reports should be downloadable in csv format		
H	Hardware & Operating System		
118	Hardware as per solution requirement with high availability and backup to DR.		
119	OEM/Vendor should propose & supply the Operating System specification/solution as per product requirements.		
120	OEM/Vendor should propose & supply the Hardware specification/solution as per product requirements.		
I	Training		
121	Local Bidder/supplier must arrange three-days Training (Online/On-site) of the solution and related knowledge transfer for at least ten (10) personnel of the offered solution.		

General Terms and Conditions

1. The bidder should have experience in business of Supplying, installing, commissioning, Operating of similar solution/ service in Bangladesh for the last Two years in Financial Organization.
2. The bidder should have the Valid Partnership with OEM.
3. The offer/ bid must be made in an organized, structured and neat manner. Brochures/leaflets etc. should not be submitted in loose form.
4. Photocopy of all the relevant documents should be submitted with the offer including:
 - Copy of Trade License.
 - Copy of TIN certificate.
 - Copy of VAT registration certificate
5. The Bank reserves the right to flexible, change or drops any of the terms and conditions of the schedule without any further notice.
6. All quoted prices should include delivery, installation, configuration, testing and AIT, VAT, Tax and other Duties if applicable as per Govt. rules. All VAT, Tax, Govt. duties etc. will be deducted from the bill as per rule prior payment of the same.
7. The Bank reserves the right to verify/evaluate the claims made by the vendor independently. Any decision of the Bank in this regard shall be final & conclusive.
8. Proper documents, brochure, data sheet, technical spec papers of mentioned Products have to be provided by the bidder in the Technical Proposal.
9. Bidding prices must be quoted in BDT. All payment will also be made in BDT.



10. Payment will be made after successful delivery of the solution/activation of the License.
11. Any decision as to compliance of the terms and conditions of the tender and on rejection of any Tender or any part thereof shall be at the sole discretion of the Bank and shall be final, conclusive and binding on the bidder.
12. The Bank reserves the right to re-issue the Tender and or any part thereof without assigning any reason whatsoever, at the sole discretion of the Bank. Any decision in this regard shall be final, conclusive and binding on the bidder.
13. The Bank reserves the right to accept or reject in part or full any or all the offers without assigning any reasons thereof. Any decision of the Bank in this regard shall be final, and binding on the bidders.
14. **Validity of Offered Price:** Offered Price should be valid for three (4) months.
15. **Supply & Installation:** Successful bidder should supply the solution/activate the License within 21 (twenty-one) working days' time after receiving of confirm work-order from First Security Islami Bank Limited, ICT Division, Head Office, Dhaka.
16. **Mode of Payment:** Payment will be made by First Security Islami Bank Limited after successful delivery of the solution/activation of the License.
17. **Submission of Tender:** Sealed tender must be dropped in the tender box kept in ICT Division on 06th October 2021. Bidder shall submit Price of Operating System & Hardware solution in separate envelope. No late tender shall be received by the Bank.
18. The bid will be automatically cancelled if the requisite terms & conditions are not fulfilled and The Bank shall not accept the quotation if not supplied as per specification.

Note: If bidder failed to comply any general terms and condition, First Security Islami Bank hold the rights to disqualify the bidder.

