Trust Bank

Trust Bank Limited
Corporate Head Office
Shadhinata Tower
Bir Srestha Shaheed Jahangir Gate
Dhaka Cantonment, Dhaka-1206
Bangladesh

ANNEXURE- A

REQUEST FOR PROPOSAL

FOR

"SELECTION OF VENDOR FOR SUPPLY, IMPLEMENTATION and SUPPORT for Privileged Access Management (PAM) Solution"

for

Trust Bank Limited

Trust Bank Ltd. ★ Purchase & Procurement Division ★

Technical specifications of Privileged Access Management (PAM) Solution

SL	Required Technical Specification	Bidders Response	
		Complaint (Y/N)	Response /Remarks
1	**Solution Overview**		
1.1	**Brand:** To be mentioned by the bidder		
1.2	**Model:** To be mentioned by the bidder		
1.3	**Country of origin:** U.S or EU		
1.4	**Manufacturing Country:** U.S or EU		
1.5	**Quantity:** 03 (Three) Units		
2	**Market Recognition**		
2.1	The proposed solution must be recognized as Leader or Challenger in the Gartner Magic Quadrant and Forrester Wave		
3	**Solution Architecture**		
3.1	The bidder must submit proposed Architecture for the offered solution considering DC and DR. The solution should have HA (Active-Active) in DC and a single instance in DR.		
3.2	The solution should have load balancing provision and fully automatic failover to another active instance with a fully replicated repository.		
3.3	The solution should be designed to have own clustering capability/ technology for application. In case of non-capability of own clustering, the solution provider/bidder will arrange such with hardware or some other means including licensing if required.		
3.4	The solution must be delivered as virtual appliance. In case of requirement of separate database, the vendor shall provide all required DB license for clustering purpose. The bank shall not provide any license for database.		
3.5	The password storage repository must be secured, hardened, encrypted and controlled remote access, etc. where the super administrator user should not be accessible via web interface/remote client.		
3.6	The password storage should have strong encryption standards (mention in detail)		
3.7	The solution should be capable to encrypt database for embedded solution. If the solution is offering non-embedded database, then it should have encryption mechanism in application level and later it should be encrypted in database level with database software's own mechanism.		
3.8	Restoration of the backup data to the solution shall be protected with strong authentication.		

3.9	Solution shall have features around management and protection of SSL digital certificates on infrastructure.		
3.10	The communication between all system components in the PAM server should be encrypted.		
3.11	The solution must have the capability for session isolation.		
3.12	The solution should support multiple session launching and capability to switch between sessions (mention session handling capability)		
3.13	The solution shall support concurrent sessions recording (mention concurrent session recording capability).		
4	**Sign-on Provisions**		
4.1	The solution should also have single sign-on feature for the applications accessed through browser i.e. automatically inject credentials into sessions.		
4.2	The solution shall get preference for supporting both client-based (in the case where browser is not available) and browser-based administration i.e. web-based and agentless login interface for single or concurrent access to servers		
4.3	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.		
4.4	The solution should be able to create seamless single sign-on for following devices: **Operating System:** Mac OS, Solaris, Windows Server 2012, 2016, 2019,2022, Linux, Unix **Data Base Servers:** MongoDB, MySQL, Oracle and MS SQL **Directories**: Active Directory, LDAP **Network/Active Devices:** Router (Cisco, Microtik, Fortinet), Switch (Cisco & others), & NGFW (Palo Alto, Checkpoint & Fortinet), Blue Coat, f5, Radware, Sophos, SafeNet, Thales-HSM, MFA-RSA, VACO, Fortinet etc. **Hardware/Server:** IBM Pureflex Server, DELL Server, IBM External Storage System, SAN Switch, EMC Storage, SUN SPARC Server, etc. **Software/Application:** Major Foreign and Local CBS **Virtualization:** VMWare, Citrix, Azzure, AWS **Microsoft:** Microsoft Exchange, Active Directory, SCCM etc. **Remote Application**: VNC, radmin etc. This is an indicative list and the product should be capable of integrating with other systems/OS/devices too, which may be		

Trust Bank Ltd.

	deployed by the Bank at a later date.		
5	**Integration Capabiiities**		
5.1	The proposed solution shall have the feature to automatically discover privileged accounts in a Windows Active Directory environment using a simple and intuitive web-based wizard, and following a review of the results, to allow automatic provisioning of these accounts for password management.		
5.2	The solution should have ability to provision users via AD/LDAP service including on-going, transparent and automatic provisioning of accounts to reflect changes in the directory. The proposed solution should also support local administrator accounts.		
5.3	The solution shall support open API / provide API's to add "connectors" to manage devices that are not currently supported 'out-of-the-box'. It should also be capable of connecting to legacy applications.		
5.4	The solution should have integration capability for REST/SOAP API for the various programming languages (net framework, php, Java, asp.net, python, C#, PowerShell, Ruby and Unix Shell Script etc.)		
5.5	The solution should be capable to integrate with Log Management System (LMS) and renowned SIEM.		
5.6	The solution alert or notification system should have integration capability with email solution/SMS engine of the bank.		
5.7	The solution should have capability to integrate with renowned multifactor authentication (MFA) solution.		
5.8	The solution should be capable to integrate with customized software/applications (CBS, SWIFT, internet banking etc.)		
5.9	Integration capability with SOAR will be added advantage.		
6	**Role Base Controls**		
6.1	The solution shall support requester, approver and reviewer roles for segregation of duties.		
6.2	The solution can restrict end-user entitlements to target accounts by days and times of day.		
6.3	The solution can restrict end-user entitlements to target from a specified PC or range or class of PCs.		
6.4	The system should allow to use CTRL + C and CTRL + V between the remote session and the host machine.		
6.5	The solution enables an administrator to restrict a group of		

	commands using a library and define custom commands for any combination of target account, group or target system and end user.		
6.6	The solution should get preference for dual control/maker-checker concept for administrative functions (e.g. asset adding, changing asset role, requesting for temporary access, modification of system configuration, etc.)		
6.7	The solution should get preference to have in-built workflow to manage various functions which are customizable. The features may have: a. User requesting the use of a target account for a future date/time for on demand access. b. Workflow approval process that requires approvers to be in sequence before final approval is granted. c. Workflow approval process that is flexible to assign multiple level of approvers based on product or model (i.e. require 2 or more approvals before access is allowed). d. Step timeout to escalate the process to the next step when request is not approved based on a given time.		
7	**General Specifications**		
7.1	The solution should support multiple browsers like Chrome, Firefox, Opera, Internet Explorer, safari, edge etc.		
7.2	The solution shall not allow to require any browsers plugins like Flash, Java, etc. for any function of accessing, initiating, reviewing, administration, or management		
7.3	The solution shall have option to secure and manage SSH keys and session of systems and applications effectively.		
7.4	The solution should have capability to blacklist/ whitelist specific commands.		
7.5	The solution should be able to store log commands fired over console-based session.		
7.6	The solution shall get preference for having the capability to limit the number of sessions a user can open for certain set of privileged accounts at one time.		
8	**System Administration**		
8.1	The product should support central administration within a unified suite (single user interface, central repository).		
8.2	The solution must restrict the solution administrators from accessing or viewing passwords or approving password requests.		

Trust Bank Ltd. ★ Purchase & Procurement Division ★

8.3	The solution should be able to restrict access to different reports by Administrator, group or role or rule based permission.		
8.4	The solution should be able to configure password age and reuse. The solution may be capable to sync with AD's password policy also.		
8.5	The solution should be capable to create open templates of password change. The system administrator should be able to create a new template using the system main interface.		
8.6	The solution shall enable an administrator to change the password by a unique random value based on a manual trigger or automatic schedule and the system should maintain history of such rotation.		
8.7	The session timeout duration should be configurable as per different Device/User Groups and accounts. There should have the option to exclude selected systems from session timeout/lock option.		
8.8	The proposed solution should allow system administrators to continue utilizing familiar access tools, such as SSH and RDP clients for the administration ease of use.		
8.9	The solution shall be capable of handling segregation of duties i.e. the Administrator user cannot view the data (passwords) that are controlled by other teams/working groups		
8.10	The solution should be able to handle lock out of Super Admin/Master Admin.		
8.11	The solution should be able to manage adverse situation for connecting/login into systems with if PAM solution is unavailable. The Super/Master admin should have a glass break method for accessing the systems with the passwords as stored in password repository.		
9	**Session Recording**		
9.1	The solution should have the ability to record privileged sessions on Windows, Virtual servers, Unix/Linux, Routers/switches, Database and applications on Low Cost Storage as well as SAN/NAS		
9.2	The session recording should be temper proof and should save the video file in its own format other than convention format so that it cannot be played with regular video players		
9.3	The solution shall have ability for session recording on multiple platforms simultaneously for multiple users.		
9.4	The solution should have the provision to save session instance file into local drive for security & flexibility.		

★ Trust Bank Ltd. ★ Purchase & Procurement Division

9.5	The solution should not expose password while initiating any session through the solution.		
9.6	System should have provision or separate group/role who can visit/analyze the recorded session		
9.7	The system should have provision to archive the recording based on the Bank's Archival Policy (Configurable)		
9.8	The system should have provision to put Legal Hold of any recorded session.		
9.9	The solution should be having feature for live session monitoring with option to terminate a session.		
9.10	The system should allow content search on recorded sessions with keystrokes and through PowerShell.		
9.11	The solution should provide separate logs for commands and session recordings.		
9.12	The solution shall not require any agent to be deployed on target systems to allow for recording search capability across all platforms.		
9.13	The solution may have recording log compression mechanism.		
9.14	The solution may get preference if it have option to automatically terminate a requested session if it exceeds its approved time frame.		
10	**Activity Monitoring**		
10.1	Dashboard Capabilities may include real-time view of activities performed by the administrators, heartbeat/live status of assets and current sessions summary.		
10.2	Advanced alert generation should also be performed for sudden increase in privileged account access by certain users or systems, typical access of the most privileged accounts or secrets, high number of privileged accounts accessed at once and accounts accessed at unusual times of day.		
10.3	The solution shall have the capability to search across both text and windows-based recording by keywords, time, users and target address.		
10.4	The solution should get preference if it is capable of alerting and send notification on actions like execute critical listed commands and attempts of access violations (running elevated/ higher privilege commands, modifying password/ user files, adding users to privileged groups etc.)		
10.5	The solution may get preference for having the capability to send email notification to designated personnel upon discovering new		

Trust Bank Ltd. ★ Purchase & Procurement Division ★

	target systems or found systems are no longer reachable.		
10.6	The solution should be able to provide intelligence-driven visual analytics to identify suspicious and malicious privileged user behavior. Dynamic Visualization that shows monitor all ongoing sessions, sessions behavior on real-time and indicate any behavioral change graphically which can be used for SOC should also be included.		
11	**Alerts & Reporting**		
11.1	All session related information should be logged & report the activities.		
11.2	Audit Trails for user activity tracking should be available		
11.3	The solution should require to generate reports in HTML,CSV, XML, PDF etc.		
11.4	The solution should have ability to report on all system administrative changes performed by PAM Administrators with relevant auditable records.		
11.5	The system should have all regular preconfigured report templates like entitlements reports, user activities, privileged accounts inventory, applications inventory, compliance reports, etc.		
11.6	The solution should be able to provide option to generate customized reports on given scenarios		
11.7	The solution should be able to distribute reports to intended users through e-mail, the ability to run all reports by frequency, on-demand and schedule them.		
11.8	The solution should be able to ensure out-of-the box security and compliance reporting templates for PCI DSS, ISO 27001 and other international standards.		
11.9	The solution may get preference if it can run analysis and provide reports for target systems, denied access attempts, time and length of session, attempt to execute blocked commands, execution of monitored commands.		
11.10	The solution may get preference if it can assess privileged account security risks and provide reports accordingly.		
11.11	The solution should log all administrator and end-user activity, including successful and failed access attempts and associated session data (date, time, Hostname, IP address, mac address). The tool should be able to generate on-demand or according to an administrator-defined schedule reports showing user activity filtered by an administrator, end user or user group.		

Trust Bank Ltd. ★ Purchase & Procurement Division ★

12	**Bidder's Minimum Requirement**		
12.1	Local bidder must be operating in IT industry in Bangladesh for at least last five (05) years		
12.2	Manufacturer Authorization must be submitted to be issued by OEM only for the qualified bidder who meets the bid submission criteria.		
12.3	Local bidder must be a direct partner of the offered OEM solution vendor for at least last three (03) years in Bangladesh. Manufacturer (OEM) letter needs to be provided to support it. No 3rd party letter would be accepted.		
12.4	Local Bidder/supplier must have two (02) in-house certified (of the offered PAM solution) engineers to carry out necessary installation, commissioning for operational acceptance.		
12.5	The local bidder must be able to supply the solution directly from OEM; not through any 3rd party distributor.		
13	**Bidder's Responsibility on implementation**		
13.1	The bidder must provide a complete Project Plan from starting to end. The plan should cover detailed of the project activities, modifications, design, implementations & integration activities. The bidder must take full responsibility related to successful project implementation till its live operation. OEM will engage with bidder during implementation.		
13.2	The bidder should be involved in installation & configuration of the Equipment's i.e. Software (SW) and Licenses as well as provide relevant services and features. Must enable the respective configuration which is recommended as best practices.		
13.3	The bidder should provide solution architecture, design and commissioning of SW, upgrade or migration in accordance with the scope and prerequisites		
13.4	The bidder should provide solution specific design related to HLD, LLD and operational documentation of the solution before UAT.		
13.5	After deployment and Integration of the solution with MBL infrastructure the technical expert should ensure on site presence till solution stability for 07 working days.		
13.6	If MBL discovers any error, shortcoming, malfunction or any other defect in the system MBL shall as soon as practicable notify the same to the bidder's Project Manager.		
13.7	Vendor must ensure the platform dependency (like hardware or		

Trust Bank Ltd. ★ Purchase & Procurement Division

	virtualization environment) during implementation		
13.8	The bidder should develop any script which is required for compatibility with latest patches of applications or hardware OS.		
14	**Support & Maintenance**		
14.1	The bidder should provide access to support portal for unresolved issues where support ticket can be submitted with unlimited ticketing capability.		
14.2	During the warranty period the bidder shall ensure support and maintenance support which includes but not limited to Onsite Support, Remote Support (i.e. on call, telephone, email, remote desktop), Case Logging, Monitoring, Root Cause Analysis Report, Periodic Heath Check and Preventive Maintenance Support, Routine Maintenance (quarterly), Bug Fixing & Patching, service upgrade and migration, Corrective Maintenance as per SLA, Error Verification Procedure etc.		
14.3	Supplier must assist to integrate devices i.e. servers, network devices, DB etc. with the PAM solution		
15.	**Training**		
15.1	The bidder must provide foreign instructor-led OEM onsite training to 10 officials. The trainer should be certified/implementation experience for the quoted product		
15.2	The training should cover product installation, configuration, administration and customization. It should also cover day to day operation of the product. Detailed documentation and manuals should be provided as part of training.		
16.	**Licensing and Service Model**		
16.1	License to be provided for **unlimited target devices and 25 Admin Users for 05 years license.**		
16.2	The license requires to be activate after successful UAT. During implementation, the bidder should provide interim license.		
16.3	SLA and NDA requires to be signed for the license period		
17.	**Hardware Requirements**		
Brand	Please specify.		
Model	Please specify.		
Memory	Please specify.		
Storage	Please specify.		

Trust Bank Ltd. ★ Purchase & Procurement

Network Interface	Please specify.		
Dimension	Please specify.		
Power	At least dual redundancy power supply		
Processor	Please specify.		
18.	**Additional Software Requirements**		
Software Name e.g. DB/OS/VM etc.			
Version	Please specify.		

Terms and Conditions.

a. The vendor must have prior experience of implementing the offered product in Financial Sector (Min 1 Work Order). **Inexperienced vendors will be disqualified during evaluation.**
b. The vendor must provide the original equipment and mention the country of origin. Product must be delivered from authorized channel.
c. The vendor must provide original Manufacturer Authorization Certificate with the bid.
d. The vendor must have OEM partnership and OEM warranty should be provided.
e. The product must be implemented by a certified engineer and QA must be done by the OEM.

Scope of the Project

Supply, install, configure, testing, live run and maintain the product at TBL's DC and NDC, that will meet the functional and technical requirements as specified in this tender document.

Evaluation Criteria (Total 100, Technical Mark - 70 and Company Profile Mark – 30)

Sl no.	Specification	Allotted Marks
1	Year of establishment (Min 5 Years gets 5 Marks, every subsequent years carries 1 Marks each)	10
2	Total No. of Work Order in related product (Min 2 W/O gets 3 Marks, every additional W/O carries 1 Marks each)	5
3	No. of Engineer in related product (Min 2 Engineer gets 5 Marks, every additional engineer carries 1 Marks each)	10
4	Total No. of Work Order in other products	5

Trust Bank Ltd.
Purch-
Division