

29 September 2026

CLARIFICATION NO 1

APPOINTMENT OF A SERVICE PROVIDER TO IMPLEMENT A CLOUD-BASED PRIVILEGE ACCESS MANAGEMENT (PAM) SOLUTION FOR A PERIOD THREE (3) YEARS; RFB 041/2026/EWSS/CLOUD-BASE/RFB

Herewith please find clarification No 1 which forms an integral part of the above-mentioned RFQ.

PLEASE ACKNOWLEDGE RECEIPT OF THIS CLARIFICATION AS FOLLOWS:

1. Complete the section below and **without delay** email a copy of this page to TCTA, email address tenders09@tcta.co.za; for the attention of The Receiving Officer to confirm that you have received this clarification.

Regards

Signed by:TINA YVONNE MKHULISE MKHULI
Signed at:2026-09-29 09:35:04 +02:00
Reason:Witnessing TINA YVONNE MKHULISE



Tina Mkhulise

MANAGER: SUPPLY CHAIN MANAGEMENT

I/We herewith acknowledge receipt of CLARIFICATION NO 1 for
RFB NO: 041/2026/EWSS/CLOUD-BASE/RFB

SIGNATURE: DATE:

ON BEHALF OF:

QUESTION 1

How are the 100 PAM licenses measured: named users, concurrent users, administrators, or privileged accounts?

RESPONSE:

The 100 PAM licenses are measured per user. Bidders must explain how their proposed licensing model accommodates the users and the full scope of privileged access specified in the RFB.

QUESTION 2

Approximately how many IP addresses, servers, network devices, databases, applications, cloud accounts and privileged accounts must be managed?

RESPONSE:

Item	Approximate quantity
Servers, including both Windows and Linux operating systems, in production and non-production	44
Network devices to be included in the PAM scope	7
Database applications	3
Cloud accounts (Microsoft Azure, Google Cloud & AWS)	7
Privileged accounts (Domain Admin)	14
Service accounts	10

QUESTION 3

Is a vendor-hosted SaaS platform acceptable, and must the platform and its data be hosted within South Africa?

RESPONSE

Yes, a vendor-hosted SaaS platform is acceptable. Hosting of the platform and its data is not limited to South Africa. Bidders must disclose the proposed hosting location and describe the security and data-protection controls applicable to TCTA's information.

QUESTION 4

Please confirm the existing products that the PAM solution must integrate with, including directory services, MFA, SSO, SIEM, ticketing and cloud platforms

RESPONSE:

The solution must support integration with TCTA's directory and identity services, including Active Directory and Microsoft Entra ID (Azure AD); multi-factor authentication, Conditional Access and single sign-on; and SIEM solutions through an appropriate integration method. It must support privileged access across on-premises systems, Microsoft 365 and cloud platforms, including Azure, AWS and Google Cloud. Bidders must identify any connectors or configuration required for these integrations.

QUESTION 5

Are all capabilities listed in section 4.1 mandatory, or may bidders identify exceptions or capabilities that require additional integration or development?

RESPONSE:

Yes. All capabilities listed in section 4.1 are mandatory. Bidders must state for each capability whether it is available out of the box, requires configuration, or requires integration or development.

QUESTION 6

What implementation timeframe, support hours, system availability, and incident-response SLAs are required?

RESPONSE

The successful bidder's project manager will develop and present the detailed implementation schedule. Given the relatively small size of TCTA's environment, TCTA anticipates that implementation may take approximately **three to four weeks**, subject to the agreed project plan, dependencies, and testing.

As specified in section 4.1.1.11 of the RFB, the contract includes **three years of post-implementation support and maintenance**, commencing after successful implementation,

with **300 support hours in total, allocated as 100 hours per year**. The bidder must specify the hourly rate and annual cost in the pricing schedule.

The solution will be used in production. TCTA requires **100% system availability and does not anticipate downtime** apart from system maintenance, which will follow Change control. Bidders must set out how they will meet this requirement, including continuity arrangements and their proposed availability SLA. Incident response and resolution must be covered within the specified support and maintenance hours, with response and resolution times defined in the SLA.

QUESTION 7

Can you advise if TCTA is using Unix Linux or just Linux?

RESPONSE:

TCTA uses Linux servers. No separate Unix operating system is included in the current PAM scope.

QUESTION 8

Could you kindly confirm whether the requirements are specifically for Administrators? If so, please provide the required number of Administrators.

RESPONSE:

The PAM requirements cover TCTA administrators and external service providers who require privileged access. The current scope includes approximately 14 Domain Admin accounts, 10 service accounts, 44 Windows and Linux servers, 7 network devices, 3 database applications, and 7 Microsoft Azure, Google, and AWS cloud accounts.

QUESTION 9

Please assist us the below enquiries to be able to scope and price the solution required by TCTA:

Question	Response
○ Scope & Scale Summary ○ Total target / privileged systems in scope: ○ Total end users who will use the PAM solution: ○ Total PAM administrators (to manage the solution): ○ Peak concurrent privileged sessions expected: ○ Remote and third-party / vendor privileged users: ○ Approximate number of secrets / credentials to manage:	○ The PAM scope includes 44 servers, 7 network devices, 3 database applications, 7 cloud (AWS, Azure & Google) accounts, 14 Domain Admin accounts, and 10 service accounts. There will be 5 PAM users, who are the same 5 PAM administrators, and 3 third-party vendors identified so far.
○ Data Centre & Infrastructure Landscape ○ List your sites and their role (e.g. HQ, DR, secondary) and location: ○ Hypervisor/virtualisation per site (VMware, Hyper-V, Nutanix, other): ○ Public-cloud platforms in use (Azure, AWS, GCP, OCI) and workloads hosted: ○ How many data centres / environments are in scope for PAM?	○ TCTA has 2 sites and 2 data centers in scope. We use VMware for virtualization and have workloads across Microsoft Azure, Google Cloud Platform, and Amazon Web Services (AWS).
○ Deployment Model & Architecture ○ Preferred deployment model: ○ SaaS / cloud-hosted (vendor-managed) ○ On-premises virtual appliance	○ TCTA's preferred deployment model is a SaaS/cloud-hosted PAM solution in the service provider's environment. The service provider will be responsible for hosting, maintaining, securing and

Question	Response
○ Hybrid ○ Is a SaaS / cloud-hosted PAM solution acceptable? (Yes/No) ○ Data-residency requirements (POPIA / where data must reside):	updating the platform, including its availability, backups and disaster recovery arrangements. Data residency is not limited to South Africa; bidders may propose hosting in another jurisdiction, provided they explain where TCTA data and backups will be stored, how access will be controlled, and how the arrangement will comply with POPIA and other applicable requirements. The solution must securely integrate with TCTA's on-premises environment and its Azure, Google Cloud and AWS platforms.
○ Availability & Resilience ○ Is High Availability (HA) required? (Yes/No) ○ Is a Disaster Recovery (DR) site required as part of the solution? (Yes/No) ○ Recovery objectives - RTO and RPO for the PAM service: Required uptime / availability SLA:	○ Yes, the proposed SaaS PAM solution requires high availability and disaster recovery. The service provider must provide geographically separate recovery capability, resilient backups and a tested failover process so that privileged access can be restored during an outage. Bidders must state their proposed recovery time objective (RTO) and recovery point objective (RPO), explain how each will be achieved and tested, and identify any dependencies on TCTA. The solution must meet the 100% production availability requirement stated in the RFB, with outages, escalation, and service restoration addressed in the support and maintenance arrangements.

Question	Response
- Privileged Password & Credential Management - Is credential vaulting and rotation required? If so, how many systems are in scope? - Account types to be managed: - Shared admin/root, Local administrator, Domain / AD admin, Service / non-human accounts, Application & database accounts, Network-device accounts, Cloud console/root accounts - Password rotation policy required (frequency, and rotate on check-in?): - Check-out / approval workflow required? (single, dual or multi-level approval; reason codes; ticket link): - Break-glass / emergency access process required: (Yes/No) - Personal password vault for business (non-privileged) accounts of interest? (Yes/No) - Secret vaults to integrate / synchronise with (AWS, Azure, HashiCorp, Jenkins, Kubernetes, other):	Credential vaulting is a critical requirement for all privileged systems and account types listed, including shared, local, domain, service, application, database, network and cloud accounts. Password rotation must be configurable and flexible so TCTA can set or change schedules in response to operational needs, audits or incidents, including rotation after use where required. The solution must support single-level and multi-level approval workflows and a controlled, auditable break-glass process. A personal password vault for non-privileged business accounts is not required. Integration with cloud secret vaults may be required; bidders should state their supported integrations.
- Privileged Session Management & Recording - How many systems require privileged session recording? - Expected peak number of concurrent privileged sessions: - Protocols in scope:	Session recording is required for 44 systems, covering Windows servers, Linux servers and database systems. The solution must support SSH, RDP, HTTPS, VNC and Telnet sessions. It must provide searchable session recordings and audit metadata, real-time monitoring and alerting, and the

Question	Response
○ SSH, RDP, HTTP(S) / web, Telnet, VNC, ICA / Citrix, Database protocols, Other ○ Recording depth required (keystroke, full video, metadata, OCR full-text search): ○ Real-time monitoring, alerting and session blocking required? (Yes/No) ○ Four-eyes / session approval / live shadowing required? (Yes/No) ○ Credential injection / session isolation (admins never see the password) required? (Yes/No)	ability to terminate a session when necessary. Four-eyes approval and live session oversight are required. Credential injection and session isolation are also required so users can access approved systems without seeing or handling privileged passwords.
○ Authentication, Authorisation & Policy ○ Primary identity source: ○ Active Directory ○ Microsoft Entra ID ○ LDAP ○ Other ○ MFA / 2FA required? Method and number of users: ○ RADIUS-based ○ SAML SSO ○ TOTP authenticator ○ Push / mobile ○ Smartcard / PKI ○ SSO / federation requirements: ○ Role-Based Access Control (RBAC) model - are roles already defined? ○ Segregation of Duties (SoD) policies required for privileged access? (Yes/No)	○ Integration with Active Directory, Microsoft Entra ID and LDAP, together with MFA, SAML single sign-on and federation, is required as specified in the RFB. The solution must support role-based access control (RBAC), segregation of duties, just-in-time access and least privilege. TCTA's detailed roles and policies will be configured during implementation. These capabilities are essential requirements and must be available out of the box. Integration with a ticketing system for access requests is outside the scope of this RFB.

Question	Response
○ Just-in-Time (JIT) access / least privilege / zero standing privilege required? (Yes/No) ○ Ticketing integration for access requests (ServiceNow, Remedy, Jira, other):	
○ Remote & Third-Party Vendor Access ○ Number of remote privileged users requiring access: ○ Is VPN-less remote privileged access required (browser-based, no client)? (Yes/No) ○ Third-party / vendor privileged access to be controlled? How many vendors? ○ Current remote-access method (VPN, jump host, ZTNA, bastion):	○ Five privileged users currently require remote access; these are the same five PAM users and administrators identified above. Privileged access for three third-party vendors must also be controlled. TCTA currently uses VPN and jump hosts for remote access and is gradually moving towards Zero Trust Network Access (ZTNA). The PAM solution should support secure, auditable remote access and accommodate that transition, including VPN-less, browser-based access where available.
○ Unix / Linux, SUDO & AD-Bridge ○ Centralised SUDO / NIX policy management required? How many endpoints? ○ AD bridging (Unix / Linux / Mac authenticate to Active Directory) required? How many hosts? ○ Delegation of root / Active Directory administrator privileges required?	○ Linux systems and their privileged accounts are included in the PAM scope. The solution must support controlled, auditable access to root and Active Directory administrator privileges. Centralized SUDO policy management and AD bridging have not been specified as separate mandatory requirements in the RFB. Bidders may describe these capabilities if available but should base their pricing on the published scope. The number of applicable Linux hosts is 9.

Question	Response
- Operating System & Platform Coverage - Windows servers - approximate count: - Linux / Unix hosts - count and distributions (RHEL, Ubuntu, AIX, Solaris, etc.): - Mainframe / IBM i (iSeries) / z-Series - in scope? - Network devices (firewalls, routers, switches) - count and vendors: - Databases - count and types (Oracle, SQL Server, PostgreSQL, MySQL, etc.): - Cloud consoles / platforms (Azure, AWS, GCP) - in scope? - End-user endpoints - in scope for privilege management? (Yes/No)	The PAM scope covers approximately 35 Windows servers and 9 Ubuntu Linux hosts, making 44 servers in total across production and non-production environments. Mainframe, IBM i and z-Series systems are not applicable. Seven network devices and three database applications are in scope, with vendors and 3 databases. Privileged access to Azure, AWS and Google Cloud must be supported, with 7 cloud accounts currently identified. End-user endpoints are not in scope for privilege management; the solution is intended to manage privileged accounts, administrators, and their access to the systems identified above.
- Governance, Compliance & Audit - Compliance standards in scope: - POPIA, PCI-DSS, ISO 27001, SOX, GDPR, King IV, Other - How often do you certify / attest privileged access today, and how long does it take? - Is privileged access already part of your certification / attestation processes? (Yes/No) - Audit & reporting requirements (who accessed what, when and why): - Interest in Privileged Access Governance - linking PAM to identity governance (IGA) for attestation and SoD across all identities? (Yes/No)	- The solution must support TCTA's audit and compliance obligations, including POPIA and the governance and security requirements stated in the RFB. Bidders should describe how their reports can support relevant frameworks such as ISO 27001 and King IV; the listed standards should not be treated as separate mandatory certifications unless the RFB expressly requires them. - TCTA currently reviews privileged access. As required by the RFB, the solution must provide searchable, exportable records showing who accessed which account or system,

Question	Response
	when, for what approved purpose, and what activity occurred, including approvals and session recordings. Integration with a future identity governance (IGA) capability is desirable; bidders should describe their support for attestation and segregation of duties without treating a current IGA integration as mandatory.
○ Integrations ○ SIEM platform (which), and events / logs to forward: ○ ITSM / ticketing platform (which): ○ Identity Governance (IGA) / Identity Manager in place or planned: ○ Directory / IdP (AD, Entra ID, Okta, etc.): ○ Notification, monitoring and other tooling to integrate: ○ DevOps / CI-CD and application secrets to manage:	○ TCTA uses Splunk, IBM QRadar and Microsoft Sentinel. The PAM solution must be able to forward privileged-access events and audit logs to these platforms through standard, configurable integration methods, so TCTA can also connect a different SIEM if it transitions in future. Active Directory and Microsoft Entra ID are the applicable directory and identity platforms. Identity governance (IGA) is planned for the near future, so bidders should describe available IGA integration capabilities. ITSM/ticketing integration, additional notification or monitoring tool integrations, and DevOps/CI/CD application-secret integrations are not in scope.
○ Users, Administrators & Training ○ Number of PAM end users (people who will request / use privileged access): ○ Number of PAM administrators (who manage the platform): ○ Training seats required, and audience (admins / operators / auditors):	○ TCTA anticipates five PAM users. These are the same five administrators who will manage the platform, so they should not be counted as two separate groups. The RFB requires training for 10 administrators and end users,

Question	Response
	covering platform administration and day-to-day use.
○ Support & Managed Service ○ Preferred support model: ○ OEM / vendor support only, Local support points (remote), Fully managed service ○ If managed service - required duration and support hours (business hours / 24x7):	○ The preferred support arrangement is vendor or OEM-backed support with an accessible local or remote service contact, in accordance with the RFB. A fully managed service is not specified as a requirement. Bidders must provide support for the three-year contract period and price the support hours and service levels stated in the RFB.