



PO Box 10335, Centurion, 0046
TCTA, Byls Bridge Office Park, Building 9,
Corner of Olievenhoutbosch & Jean Ave, Doringkloof, Centurion
Tel: +27 12 683 1200 | Fax: +27 12 683 1361
Email: info@tcta.co.za | Website: www.tcta.co.za

13 April 2026

CLARIFICATION NO 4

APPOINTMENT OF A SERVICE PROVIDER TO IMPLEMENT A CLOUD-BASED PRIVILEGED ACCESS MANAGEMENT (PAM) SOLUTION; RFB NO: RFB No:105/2025/EWSS/CLOUDBASE/RFB

Herewith please find clarification No 4 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

Tina Mkhulise

SCM ACQUISITION MANAGER: CORPORATE

I/We herewith acknowledge receipt of CLARIFICATION NO 4 for RFQ NO. RFB NO: 105/2025/EWSS/CLOUDBASE/RFB

SIGNATURE: DATE:

ON BEHALF OF:

QUESTION 1

We would like to submit the following clarification questions regarding the Cloud-based PAM RFP:

1. Section 4.1 – Scope Alignment (IGA vs PASM)

Section 4.1 appears to include several Identity Governance and Administration (IGA) related processes rather than being strictly PASM-focused:

- 4.1. 2 Enforcement of SoD, access reviews, and certification workflows – typically associated with IGA processes
- 4.1.3 Multi-level approval mechanisms and policy-based access governance – please clarify the expected depth of workflow capabilities, as PASM solutions generally provide limited approval functionality rather than full workflow orchestration
- Just-in-Time (JIT) and Just-Enough-Access (JEA) provisioning – while partially supported within privileged access solutions, please confirm whether advanced provisioning workflows are required, as these may require additional modules

RESPONSE

- TCTA confirms that while the primary focus of this RFB is on Privileged Access Management (PAM), the solution is expected to support integrated IAM capabilities where applicable. This includes alignment with governance controls such as Segregation of Duties (SoD), access reviews, and approval workflows, particularly where they relate to privileged accounts.
- The expectation is not for a full standalone IGA solution, but rather PAM-aligned governance capabilities that enable controlled privileged access, including approval workflows and policy enforcement.
- JIT (Just-in-Time) and JEA (Just-Enough Access) are **mandatory capabilities**.

QUESTION 2

2. Password and Credential Management Scope

- Management of SSH keys, API keys, and service account credentials – SSH keys

and API keys typically fall under a secrets management component. Please confirm whether this is within scope and should be included in the proposed solution

- Just-in-Time (JIT) and Just-Enough-Access (JEA) provisioning – while partially supported within privileged access solutions, please confirm whether advanced provisioning workflows are required, as these may require additional modules

RESPONSE

- TCTA confirms that the scope includes comprehensive credential management, including privileged passwords, service accounts, and secrets such as SSH keys and API keys, as these are critical to securing modern environments.
- JIT and JEA provisioning are required as part of enforcing least privilege access. Where advanced capabilities require additional modules, bidders should clearly indicate this in their proposals.

QUESTION 3

3. Reporting and Analytics

- Risk-based analytics and anomaly detection for privileged activities – please confirm whether this is expected as a native PASM capability, or if additional licensed modules would be acceptable to support this use case
- Where applicable, please also advise on the number of users within the Identity Provider (IdP), as this may influence licensing requirements for analytics components
- Just-in-Time (JIT) and Just-Enough-Access (JEA) provisioning – while partially supported within privileged access solutions, please confirm whether advanced provisioning workflows are required, as these may require additional modules

RESPONSE

TCTA expects that risk-based analytics and anomaly detection for privileged activities form part of the core Privileged Access Management (PAM) capability. This includes the ability to monitor, analyse, and detect anomalous behaviour associated with privileged accounts, sessions, and access patterns.

With respect to licensing considerations, the current requirement is based on **100**

privileged user accounts for the PAM solution. The number of users within the Identity Provider (IdP) environment may be approximately 70 users at the moment.

QUESTION 4

4. Customer References

- Kindly confirm whether references must be provided on official client letterhead, as this may not always be feasible
- Additionally, please clarify whether all requested reference details (client name, contact person, designation, contact details, scope of work, technologies, and engagement period) are mandatory, considering potential PII restrictions

RESPONSE

- TCTA requires that reference letters be **verifiable and credible**, preferably on official client letterheads.
- If it is not possible for the bidder to provide reference letters, the bidder can fully complete annexure A
- All key reference information (client name, contact details, scope, duration, technologies) is required for evaluation purposes.

QUESTION 5

5. Licensing Model Clarification

- The RFP references a scope of 100 licenses across the ICT environment. We also have the option to propose an asset-based licensing model (e.g., per device, OS, database), which can often provide a more cost-effective and scalable approach compared to named user licensing
- To ensure we provide the most appropriate and cost-efficient proposal, could you please share an estimate or breakdown of the total number of assets (devices, operating systems, databases, etc.) that need to be managed
- Just-in-Time (JIT) and Just-Enough-Access (JEA) provisioning – while partially

supported within privileged access solutions, please confirm whether advanced provisioning workflows are required, as these may require additional modules

RESPONSE

- TCTA's current requirement, as stated in the RFP, is based on a **minimum of 100 privileged user licenses**. This approach was selected to ensure alignment with identity-centric security controls, governance, and auditability of privileged access.
- However, TCTA acknowledges that alternative licensing models, such as asset-based licensing (e.g., per device, operating system, database, or managed account), may offer cost efficiencies and scalability depending on the solution architecture. Bidders are therefore encouraged to include, in addition to the base requirement, an alternative proposal based on an asset-based licensing model, clearly outlining:
 - The licensing metric used (e.g., per server, endpoint, database, or account),
 - Cost implications compared to the user-based model, and
 - Any impact on functionality, scalability, or integration.
- For purposes of proposal alignment and estimation, the current environment is as follows:
 - **Total Servers: 52**
 - 35 Windows Servers
 - 12 Linux Servers (including database servers)
 - **Privileged Users: 15** (including internal administrators and service providers)
 - **Service Accounts: 25**
- All licensing assumptions and dependencies must be clearly stated to ensure transparency in total cost of ownership and alignment with TCTA's governance and budgeting requirements.

QUESTION 6

6. Elevated Access / Least Privilege

- The RFP refers to elevated access; however, this is typically aligned to Least Privilege principles, which are separate from credential vaulting and session management capabilities
- Kindly provide more detail on the expected scope and requirements for Least

Privilege, specifically in relation to elevated access activities, so that we can align the proposed solution accordingly

- Just-in-Time (JIT) and Just-Enough-Access (JEA) provisioning – while partially supported within privileged access solutions, please confirm whether advanced provisioning workflows are required, as these may require additional modules

RESPONSE

- TCTA confirms that Least Privilege principles are a core requirement of the PAM solution. The solution must support:
 - Controlled elevation of privileges
 - JIT/JEA access provisioning
 - Session monitoring and control
 - Policy-based enforcement of privileged access
- The expectation is that PAM capabilities will enforce least privilege access dynamically, reducing standing privileges and minimizing risk exposure.

QUESTION 7

7. Hosting / Data Residency Requirements

- Kindly confirm whether there are any specific hosting or data residency requirements (e.g., preferred cloud provider, on-premises deployment, or specific geographic region such as in-country hosting) that we should adhere to

RESPONSE

- The solution must support a cloud-first deployment model, preferably hosted in secure and compliant environments aligned with data protection regulations (e.g., POPIA).

Preference will be given to solutions that:

- Support in-country compliant data hosting
- Provide flexibility for hybrid integration (cloud and on-premises systems)
- Ensure strong security, availability, and compliance controls
- Bidders must clearly indicate their hosting model, data residency approach, and compliance with relevant standards.