Description of Request	Provision of an Artificial Intelligence (AI)-powered Unified IdentityProtection Platform Managed Services for Subscription Licenses,Maintenance and Support for a period of five years.

1. High level background

The AI-powered Unified Identity Protection Platform will provide Automated Identity Intelligence, Authentication, Access, Protection, Governance and Life Cycle capabilities for the corporate network (on-premises, hybrid, and multi- cloud) as well as the Operational Technology (OT) environments within Eskom.

The AI-powered Unified Identity Platform combines automated identity intelligence, authentication, access, governance, and lifecycle into one cohesive solution, to protect the gaps and blind spots that result from combining multiple point solutions.

1) Automated identity intelligence provides AI-powered adaptive authentication policies, mobile threat detection, dashboards, reports and insights.
2) Authentication provides passwordless, mobile security, risk-based authentication, advanced multifactor authentication (MFA), supports for software and hardware authenticators and phishing-resistant hardware tokens.
3) Access provides Single Sign-On (SSO), unified directory, federated directories, and integrations.
4) Governance and lifecycle provide end-to-end visibility, audit and compliance readiness and visualizations into entitlements.

Eskom requires an AI-powered Unified Identity Protection Platform to ensure that only authorised end users, devices, and applications have access to the correct network resources to reduce risk of human error in managing privileges, improve operational efficiencies for credential management, and lower costs with automation.

2. Scope of work/Business requirements

2.1. Product/service requested:

Eskom requires an AI-powered Unified Identity Protection Platform managed services for a period of five (5) years. The managed services must cater for the Eskom hybrid (on-premises, hybrid, and multiple cloud) environments including the OT environments and must include software licenses, subscriptions, hardware, professional services, maintenance, and support on a 24x7x365 basis for the duration of the contract:

The AI-powered Unified Identity Protection Platform must have the following capabilities but not limited to:

2.2. Automated Identity Intelligence

a) AI-powered adaptive authentication policies: The platform must support AI-powered adaptive authentication policies.
b) Mobile threat detection: The platform must provide threat detection mechanism for mobile devices.
c) Dashboards, reports and insights: The platform must provide dashboards, reports and risk insights.

2.3. Authentication

a) Passwordless: The platform must support passwordless technologies such as FIDO security key, biometric, push to approve, smart cards but not limited to these technologies.
b) Mobile security: The platform must establish trust in managed and unmanaged devices by scanning for critical security threats when users try to authenticate to enable and support the Eskom bring your own device (BYOD) policy.
c) Software and hardware authentication: The platform must support for software and hardware authenticators and phishing-resistant hardware tokens.
d) Zero Trust: The platform must align with NIST Zero Trust Architecture (ZTA) and provide risk-based analytics, role- and attribute-based access, dynamic decision-making, capabilities to establish trust and be able to integrate with identity systems.

2.4. Access

a) Single Sign-On (SSO): The platform must provide SSO.
b) Unified Directory: The platform must provide unified directory.
c) Federated Directories: The platform must support federated identities such as SAML, Oauth and OpenID.

2.5. Governance and Lifecycle

a) Security: Ensures that only authorized users have access to sensitive information and resources, reducing the risk of data breaches and insider threats. Ability to discover, manage, and secure ALL user access including employee, non-employee, and machine identities.

b) End-to-end visibility, Audit and Compliance: The platform must provide end-to-end visibility, audit and compliance readiness and visualizations into entitlements.

c) Auto Discovery: Automated AI-based discovery of all accounts including discovering accounts that are being shared by both human users and services.

d) Automation: ability to automate access to reduce over-provisioning or back door access by former workers and third-party non-employees.

e) Central Management: Capability to centrally manage and enforce access policies for all users and service accounts across your entire network and all on-prem and cloud resources.

f) Risk Management: Identify and mitigate risks associated with access management, such as orphaned accounts and excessive access privileges.

g) Access Certification: Regularly review and certify user access rights and service accounts to ensure compliance with policies and regulations. Verify that users have appropriate access and revoke access when no longer needed. Ability to automate Data Subject Access Request to meet data privacy requirements.

h) Automated Access Reviews: Automatically review user access rights on a regular basis to ensure that users have the appropriate level of access to reduce the risk of unauthorized access.

i) Risk-Based Access Control: Dynamically adjust access controls based on risk factors such as user behavior, location, and device to prevent unauthorized access based on unusual activity.

j) Integration with IAM, SIEM Systems and Other Monitoring Systems: Integrate with existing Identity and Access Management (IAM) systems for user authentication and authorization. Also, integrate with Security Information and Event Management (SIEM) systems and other real-time monitoring and reporting systems.

k) Scalability and Flexibility: Scalability to accommodate growing user bases and organizational needs by proving flexibility in deployment options and customization capabilities.

l) Reporting and Analytics: Provide dashboards and reports to monitor access patterns, identify risks, and track compliance with access policies.

m) Strong Identity Analytics: Provide robust identity analytics capabilities, leveraging machine learning algorithms to detect and mitigate potential risk issues and anomalous activities within the system to enables Eskom to monitor and respond to access-related risks effectively.

n) Audit Trail: Maintain a detailed audit trail of all access-related activities for compliance and forensic analysis. Tracking the usage patterns, access requests, and behaviour of each service account, including high-level permissions, broad use, and repetitive behaviour.

o) Compliance Management: Ensure compliance with regulatory requirements and internal policies related to access management.

p) Policy-based Access Management: The solution must support defining and enforcing access policies based on contextual for all users, including administrators and service accounts across the entire network and all on-prem and cloud resources. and reporting for administrators

q) Identification: Identify and remediate overexposed permissions to reduce risk and satisfy strict compliance requirements. Also govern access to sensitive and regulated unstructured data across applications, files and storage devices — whether on-premises or in the cloud.

r) Segregation of Duties (SoD) Enforcement: Identify and prevent conflicts of interest by enforcing rules that prohibit users from having conflicting roles or permissions that could lead to fraudulent activities or data breaches.

s) Detection of toxic access: Detect and prevent toxic access combinations that could lead to fraud or data theft. Expose access rights to unstructured, regulated, and sensitive data.

t) Behavior Analytics: Analyze user behavior to detect anomalies and potential security threats to identify and respond to security incidents in real-time on both user and service accounts.

u) Alert: Anomaly detection alerts of any deviation from the account’s standard behaviors, including service accounts.

v) Service Account Monitoring: Monitoring service account activity continuously in real time.

w) Cloud Identity Management: Extend identity governance capabilities to cloud-based services and applications to ensure a consistent approach to identity management across on-premises and multiple cloud environments.

x) Integration with identity providers to deliver secure authentication across every resource on- prem and in the cloud.

y) Consistent Sign-in Process: Consistent sign-in process to resources including all legacy and cloud resources.
z) Fully automated visibility, risk analysis and adaptive Zero Trust policies.
aa) Continuity: Make provision for technology changes during contract termination.

2.6. Advanced Multifactor Authentication

a) Multi-Factor Authentication Factors: Support for a variety of authentication factors, including but not limited to biometrics, FIDO2, smart cards, SMS, hardware tokens, smartphone app, emergency password, and contextual factors ensuring flexibility to adapt to different user roles and security needs.
b) Compatibility with Legacy Systems: The MFA solution must seamlessly integrate with existing legacy OT and IT systems, ensuring compatibility with diverse communication protocols and technologies commonly found in utility organizations. Thick Client and web-based applications that uses a mixture of NTLM, Kerberos, LDAP and local application accounts.
c) Support for Operational Technology (OT) Environments: The MFA solution should be tailored to the specific requirements of OT environments, accommodating the unique challenges and communication protocols associated with control systems, industrial equipment, and other critical OT components.
d) Adaptive Authentication Mechanisms: The MFA solution should employ adaptive authentication, considering contextual factors such as user behaviour, location, and risk assessments to dynamically adjust authentication requirements, providing a balance between security and user experience.
e) Intelligent Risk Scoring and Threat Analytics: Implementation of risk scoring mechanisms and advanced threat analytics to detect and respond to anomalies, providing real-time insights into potential security threats or suspicious activities across both OT and IT environments.
f) Secure Integration with Critical Infrastructure: Ensure secure integration with critical infrastructure components, such as SCADA systems and industrial control systems (ICS), without compromising the integrity and availability of these systems.
g) Device and Location Awareness (Geo-Fencing): The MFA solution should exhibit awareness of user devices and geographical locations, allowing for context-aware authentication policies to be enforced based on user and device attributes.

h) Usability for Diverse User Roles: User-friendly interfaces that cater to the diverse skill sets and roles within the organization, including both technical staff managing OT systems and administrative personnel overseeing IT operations.

i) Centralized Management and Reporting: The solution must enable centralized management, enforce access policies and reporting for all users, including administrators and service accounts across the entire network and all on-prem and cloud resources.

j) Scalability and Performance: The MFA solution must scale to accommodate the size and growth of the organization's user base and infrastructure, while maintaining optimal performance, particularly during peak operational periods. The solution must make provision for true up (increase) and true down (reduction) on volumes.

k) Redundancy and Failover: Built-in redundancy features and failover mechanisms to ensure continuous availability of MFA services, minimizing downtime and disruptions to critical operations.

l) Vendor Support and Roadmap: The solution must provide support services and the roadmap for future developments that align with Eskom's requirements.

m) Compliance with Regulatory Standards: Compliance with industry-specific regulatory standards and frameworks, such as NERC CIP, IEC 62443, or other relevant regulations governing the utility sector.

n) Integration with Identity and Access Management (IAM) Systems: Seamless integration with existing IAM, web, agents, and RADIUS. solutions to streamline user provisioning, de-provisioning, and identity lifecycle management, ensuring consistent and secure user access across both OT and IT systems.

o) Continuity: Make provision for technology changes during contract termination.

p) Support all Directory Services: Support all directory services. Eskom employee has multiple user accounts linked to a single Identity. The single identity facilitates the synchronization of user attributes between the two accounts, including passwords.

q) Interoperability with Security Frameworks: The solution must integrate with independent SASE and/or SSE solution.

r) Support Hybrid Environment: The solution must support a Hybrid (On premise, hybrid and Multi Cloud) environment. Cloud service must cater for multiple cloud service providers e.g., Azure, AWS, GCP etc.

s) Agentless: Agentless, Seamless, Risk-based authentication to all applications and resources across on-prem, hybrid and multi cloud environments, including third parties.

t) Advanced Workflow: The platform must provide advanced and automated workflow.

u) Integrate with Helpdesk Services: Provide helpdesk functions that can assist users when there are issues with the MFA tokens and can assist users to register their authentication methods.

2.7. Maintenance and Support

a) Maintenance and Support for subscription service
b) Subscription Licences for all components
c) Telephonic/Remote Support.
d) 24x7x365 expert level support with OEM.
e) Full-service functionality, no limitations

2.8. Professional Support Services

a) Professional consulting services (Telephonic/Remote and On-Site Support when needed) to address business requirements.
b) This includes the products specialists that will assist Eskom with Project management, implementation, and enhancements to interfaces to Eskom applications.

2.9. Training/Transfer of skills

a) Provide web-based training for end-users and system support staff.
b) Mentor Eskom resources through the installation, configuration and deployment stages using a defined skills transfer program.
c) Expert level training with relevant certification for five resources.

2.10. Landscape

a) A minimum of 40 000 Users
b) A minimum of 35 000 Laptops and desktops.
c) A minimum of 5000 servers
d) A minimum of 60 critical Applications.
e) Unspecified number of mobile devices

3. Service Level Agreement requirements

The Service Provider must provide **24x7x365** monitoring of the environment as well as support with severity categories, and lead times indicated on the table below.

Service Level	Description	Escalation to SP	Escalation to OEM
Critical	Business has stopped	Response within 30 minutes – Level 1 Response within 1 hour – Level 2	Response within 2 (two) hours
Major	Business severely impacted	Response within 1 (one) hour – Level 1 Response within 2 (two) hours – Level 2	Response within 4 (two) hours
Normal	Minor business impact / product failure	Response within 1 (one) business day – Level 1 Response within 2 (two) business days – Level 2	Response within 1 (one) business day
Low	No business impact but requires one or more updates	Response within 2 (two) business days – Level 1 Response within 2 (two) business days – Level 2	Response within 2 (two) business days
Informational	Request for information	Response within 3 (three) business days – Level 1 Response within 3 (three) business days – Level 2	Response within 3 (three) business days

4. Approvals:

End User / Requestor:	**Name:**	Ronald Netshishivhe
	Designation:	Chief Advisor: IT Security Services
	Date:	27/02/2024
	Signature:	
Middle Manager	**Name:**	Skhumbuzo Gama
	Designation:	Middle Manager: Cyber Security
	Date:	28/02/2024
	Signature:	
Senior Manager:	**Name:**	Sithembile Songo
	Designation:	Senior Manager: IT Security Services
	Date:	28-02-2024
	Signature:	