Description of Request	Zero Trust Network Access Services

1. High level background

Zero trust network access (ZTNA) is a security strategy that operates under the presumption that no user or device can ever be completely trusted. This indicates that only after the user or device has been approved and authenticated is access to apps and data provided. ZTNA is made to defend businesses from a variety of cyberattacks, such as phishing scams, ransomware assaults, and data breaches.

ZTNA aims to enhance the security posture of static DMZ network configuration by only allowing the specific communication that is required for the applications to work and implement ever evolving controls. Micro-segmentation will require communication between devices to be limited with just enough access to complete the intended task of communication between servers, devices, and applications. Communication will be controlled not only at the network level between hosts, but also from process to process and in the application stack through API Micro-segmentation. Additional Authentication and Authorization will be part of each step of the process towards the data layer.

A system may be completely patched, but a single change to another part of the system may cause that system to become more susceptible to compromise. ZTNA aims to change this by giving a unified centralized evaluation of systems and a coordinated response to not only system status but event analysis and action over the environment and on individual devices.

The ZTNA enforces authentication and authorization of entity requests and makes decisions to grant or deny access based on the requesting entity's identity, need-to-know, and device posture. They hide the network and resource details to mitigate the most common network-based attacks. It also looks to add confidence scoring not only to users but also devices. ZTNA security model shifts to a more focused use of multi-attribute-based confidence levels to enable authentication and authorization policies based on the concept of least privileged access.

Adopting a zero-trust remote access strategy that reduces complexity, enables security and keeps users productive on any device and from any location whenever they access corporate resources. The conventional use of persona-based identities, credentials, and attributes are not dynamic or context aware. Current methods tie to a user's physical location. After authentication, every person entity and non-person entity is treated the same. Two factor authentications, authentication tokens, and username and password login have not kept pace with the industry's multi-factor authentication advances. Conventional authentication methods do not address non-persona entities such as bots, hardware devices, or software applications.

ZTNA draws on technologies such as multifactor authentication (MFA), enterprise identity service, and user/entity behaviour analysis (UEBA) to enable continuous and dynamic authentication. These tools evaluate the identity of the user or NPE (non-person entity) in

real time as access to applications and data are requested. User and entity transactions are continuously monitored for anomalous behaviour, which is then flagged, and the user/entity is then restricted access. Use of a single unified platform with integrated identity and access management to provide MFA is ideal to avoid any gaps in security or any hurdles to implementing ZTNA, enabling thorough and continuous monitoring.

ZTNA augments traditional VPN technologies for application access, and removes the excessive trust once required to allow employees and partners to connect and collaborate.

2. Business motivation & benefits

a. Business motivation:

- Improved security: It helps to improve organisation security posture by reducing the risk of data breaches and other cyberattacks.
- Increased agility: ZTNA can help organizations to increase their agility by making it easier to onboard new users and devices.
- Reduced costs: ZTNA can help organizations to reduce their costs by eliminating the need for expensive and complex perimeter security solutions.
- Improved compliance: ZTNA can help organizations to improve their compliance with industry regulations, such as the PoPIA.
- Reduce attack surface: Agentless services.

b. Benefits to Eskom

The ZTNA services will bring forth the following benefits for Eskom:

- Reduced risk of data breaches: ZTNA can help to reduce the risk of data breaches by preventing unauthorized users from accessing sensitive data.
- Improved user experience: ZTNA can improve the user experience by providing a seamless and secure access to applications and data, regardless of the user's location or device.
- Increased visibility and control: ZTNA can provide organizations with increased visibility and control over user access to applications and data. This can help organizations to identify and respond to security threats more quickly.

c. Zero Trust Network Access versus Traditional VPN Services

ZTNA, a more recent security method, operates under the premise that no user or device can ever be completely trusted. This indicates that only after the user or device has been approved and authenticated is access to apps and data provided. ZTNA is made to defend businesses from a variety of cyberattacks, such as phishing scams, ransomware assaults, and data breaches.

A ZTNA environment dispenses with the distinction between "internal" and "external" users. An internal user should have no implicit trust associated with it than an external user. All users are untrusted. One outcome that can follow is the removal of VPN. In a ZTNA environment, all users are effectively "external" or untrusted and therefore must undergo the same rigorous authentication and authorization processes.

In the conventional approach, off-site users connect to the internal network via a VPN, which effectively places them on the "internal" network with on-site users. If the external user accesses external or Internet resources, traffic first passes through the enterprise perimeter before heading back out. This increased traffic flow requires continuous bandwidth and can create significant latency issues. Additionally, VPNs pose a threat to enterprise security. They create a path in the network perimeter and provide access to network resources after authentication. The conventional approach cannot provide a method to intelligently confirm the identities of users and entities attempting to access the network or provide adaptive policy enforcement based on authentication.

In ZTNA, all users and Non-Person Entities (NPE) pass through the same Policy Enforcement Point and gateways before they can access resources with Comply-to-Connect, many of which will reside in data centre resources and cloud services accessible via the Internet. All requests for access will be highly scrutinized using continuous multi-factor authentication and the concept of least-privilege. In this model, formerly external users do not incur additional latency by hair-pinning through a VPN.

Zero trust network access (ZTNA) as products and services that create an identity- and context-based, logical-access boundary that encompass an enterprise user and an internally hosted application or set of applications. The applications are hidden from discovery, and access is restricted via a trust broker to a collection of named entities. The broker verifies the identity, context and policy adherence of the specified participants before allowing access and minimizes lateral movement elsewhere in the network. ZTNA removes excessive implicit trust that often accompanies other forms of application access, such as legacy VPN.

Zero trust network access (ZTNA) offers significant advantages for distributed organizations with remote workforces accessing on-premises resources. ZTNA gives secure access to specific on-premises resources, applying zero trust security principles to minimize impact of breaches.

A ZTNA model:

a. Authenticates every device and user, no matter where they are located.
b. Limits access on an application-by-application basis.
c. Applies granular in-app controls and authorization.
d. Hides unauthorized applications from the user and internet to minimize lateral movement.
e. Continuously monitors user activity and enforces policy in real time.
f. Agentless

3. Scope of work/Business requirements

The scope of the project includes an enterprise wide ZTNA solution. The solution should be scalable to meet the enterprise business requirements meaning it must be able to allow for increase and decrease as in when required.

All the requirements detailed below will need to be demonstrated by the tool chosen:

1. Cybersecurity policies dynamically determines access to PAAS, driven by robust real-time analytics.
2. NPE (i.e., devices/ platforms/ AI apps) continuous compliance vetting and diagnosis.
3. Continuous and adaptive authentication and authorisation.
4. User and device identity based on Enterprise Federated Identity Service.
5. Fully implementation of just-in-time and just-enough access policy.
6. Ability to integrate with existing or new Data Prevention services and access rights management.
7. Advanced analytics enabling automation and orchestration of threat detection.

All the principles detailed below will need to be demonstrated by the tool chosen:

1. Assume no implicit or explicit trusted zone in network.
2. Identity-based authentication and authorization are strictly enforced for all connections and access to infrastructure, data, and services.
3. Risk profiles, generated in near-real-time from monitoring and assessment of both user and devices behaviours, are used in authorizing users and devices to resources.
4. All user sessions are encrypted by default.
5. All access sessions are continuously monitored, collected, stored, and analysed to assessed against security policies.
6. Policy management and distribution is centralized.

3.1. ZTNA Service Capability and Functionality

Below listed ZTNA features will need to be demonstrated by the Service chosen:

3.1.1. User Access Service Integration
   a. Access Management
   b. Third Party Security Access Management
   c. Authentication
   d. User and Event Behaviour Analytics
   e. Identity Management
   f. Conditional Access
   g. Dynamic Risk Scoring

3.1.2. Device Service Security Governance/ Integration
   a. Vulnerability Management
   b. Device Security
   c. Device Identity
   d. Device Compliance
   e. Device Authentication
   f. Device Management
   g. Device Inventory

3.1.3. Network Security

a. Zero Trust Security Architecture
b. Network Services Access Control
c. Transport Encryption
d. Session Protection

3.1.4. Application Security
a. API Security
b. Container Security
c. Secure Access Cloud
d. Isolation (Sandboxing)
e. Any Device Access

3.1.5. Visibility and Analytics
3.1.6. Orchestration and Access Control Automation
3.1.7. DevSecOps Interoperable
3.1.8. Machine Learning
3.1.9. SASE Capable
3.1.10. SSE Capable
3.1.11. Artificial Intelligence

3.2. Maintenance and Support

a. The supplier will be required to conduct an initial assessment to ascertain the ecosystem requirements.
b. Provide 1st and 2nd Line support and maintenance on a per request basis over the period of the contract.
c. Telephonic and on-site (when needed) on software and hardware.
d. Align advisory services with Eskom governance practices.
e. Change management.
f. Develop a change management programme to prepare users and administrators to adopt the new processes introduced by the solution.

3.3. OEM Premium Support

a. Telephonic/Remote Support.
b. 24 x 7 x 365 expert level support with OEM.
c. Access to support base and OEM support portal.
d. Full suite software licensing - All components.
e. Full ZTNA service functionality, no limitations.

3.4. 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 hardware.

f. Unspecified number of smart meters

3.5. Professional Services

Professional consulting services post project execution during the four years of the system operations and support. This includes products specialists that will assist Eskom with the following:

a. Project management for major products upgrades and enhancements,
b. Solution design,
c. Development, testing, configuration, documentation, and implementation of enhancements of products that are currently deployed including associated interfaces to Eskom applications.

3.6. Training/Transfer of skills:

a. Provide onsite, classroom-based, and web-based training for end-users and system support staff on a pre-booked basis. The recommended method of training delivery would be required on implementation and, as per request in future.
b. Mentor Eskom resources through the installation, configuration and deployment stages using a defined skills transfer program.
c. The service provider will be required to train Eskom IT staff to provide first line support. This will be determined as part of the contract terms.
d. Expert level training with relevant certification 10 resources.

4. Service Level Agreement requirements

The Service Provider must provide **24/7/365** second- and third-line support with OEM.

Service Level	Description	Escalation to SP	Escalation to OEM
Critical	Business has stopped	Response within 1 (one) hour – Level 1 Response within 3 (three) hours – Level 2	Response within 4 (four) hours
Major	Business severely impacted	Response within 1 (one) hour – Level 1 Response within 3 (three) hours – Level 2	Response within 4 (four) 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

5. Definitions

NPE - An entity with a digital identity that acts in cyberspace but is not a human actor. This can include an autonomous service or application, hardware devices (e.g. IOTs), proxies, and software applications (e.g. Bots).

6. Approvals:

End user / requestor:	**Name:**	Charles Sello Kungwane
	Designation:	Middle Manager Information Security
	Date:	29 August 2023
	Signature:	
Senior Manager:	**Name:**	Sithembile Songo
	Designation:	Senior Manager Information Security
	Date:	29 August 2023
	Signature: