REQUEST FOR INFORMATION (RFI)

Lanka Government Network 3 (LGN 3) -Secure Access Fabric Aligned with the Sovereign Government Cloud

1. Introduction

The Government of Sri Lanka (GoSL) is advancing its national digital transformation agenda through the establishment of a unified, secure, and legally recognised digital communication framework across the public sector. A key enabler of this vision is the Lanka Government Network 3 (LGN 3) initiative representing a strategic transformation of the existing LGN platform toward a cloud-first, secure access fabric aligned with the Sovereign Government Cloud (SGC) model.

LGN 3 is not a conventional WAN upgrade or routine network refresh. Instead, it seeks to evolve LGN into a policy-driven, identity-centric access platform that enables secure connectivity to government workloads hosted across multiple sovereign cloud regions and approved Cloud Service Provider (CSP) environments, while maintaining centralised identity, policy enforcement, and compliance controls.

This RFI is issued to gather comprehensive market information on modern WAN, SD-WAN, SASE, Zero Trust, identity-based access, and multi-cloud connectivity solutions, and to assess the feasibility of different underlay connectivity models, including:

i) Commodity Internet + SD-WAN/SASE overlay, and
ii) Provider-operated Private Networks with integrated security.

Special consideration is required for remote service points for field level officers of the Government such as Grama Niladhari (GN), Agriculture Instructor, Samurdhi Managers, Midwife etc., where connectivity is constrained or intermittent. Solutions must therefore support a broad spectrum of last-mile conditions.

Responses to this RFI will guide the Government in defining architectural standards, connectivity strategy, solution design, and implementation pathways for LGN 3, the future secure digital backbone for government agencies, officers, and services nationwide.

2. Disclaimer

This RFI is issued solely for market research and strategic planning. It does not guarantee commitment to procure goods or services. The Government of Sri Lanka is under no obligation to proceed with procurement based on responses received. All costs associated with preparing and submitting responses shall be borne exclusively by respondents. A response to this RFI does not have any impact on future or ongoing engagements with the ICTA or the MODE (Ministry of Digital Economy).

3. Terms of Reference (ToR)

3.1. Project Background

The Government of Sri Lanka aims to provide a secure, high-speed, and resilient digital communication infrastructure to support efficient inter-agency communication, data exchange, and digital service delivery. The LGN 3 initiative forms a central element of this strategy by providing seamless access to applications hosted in the Sovereign Government Cloud, which contains critical government systems and sensitive data maintained within nationally controlled environments.

LGN 3 aligns with the Universal Broadband Vision of ensuring affordable, high-quality connectivity across urban, rural, estate, coastal, and underserved regions. As part of this model, government entities will leverage available ISP broadband infrastructure while maintaining secure connectivity through standardized security, identity, and access control mechanisms.

Importantly, LGN 3 must extend beyond ministries and district offices to reach local authorities, divisional secretariats, Grama Niladhari (GN) divisions, other micro-sites, and field officers operating with limited or intermittent connectivity. Solutions must therefore support scenarios ranging from well-connected urban buildings to single-officer GN offices and remote community service points.

Secure communication to the Sovereign Government Cloud will be established using SD-WAN/SASE overlays, private network, or equivalent mechanisms ensuring encryption, segmentation, and resilience.

3.2. Objectives of this RFI

This RFI aims to:

i) Understand available WAN, SD-WAN, SASE, NGFW, ZTNA, and identity-based access solutions
ii) Assess vendor experience with large-scale or nation-scale government network deployments
iii) Evaluate underlay connectivity options including:
   a) Fibre / DIA / business broadband
   b) Mobile broadband coverage (4G/5G)
   c) Fixed wireless / microwave
   d) MPLS / private WAN fabrics
   e) Identify connectivity approaches for covering islandwide government officers, field level officers and offshore officers
iv) Obtain indicative CapEx + OpEx models, licensing models, for both 5-year and 10-year TCO projections
v) Understand risk factors and best practices for nationwide implementation
vi) Support the Government in shaping the architectural, operational and commercial strategy for LGN 3

3.3. Participation Eligibility and Partnerships

i) Participation in this RFI is open to all technology vendors, regardless of whether they directly provide connectivity or telecommunications services.

ii) Vendors who do not operate as a network service providers are still strongly encouraged to respond. Such vendors may:

   a) Submit proposals covering security, SD-WAN, SASE, ZTNA, identity, orchestration, analytics, cloud on-ramp, monitoring, or other LGN 3 components

   b) Respond independently with non-connectivity components

   c) Form partnerships, consortia, or collaborations with licensed telecommunications and connectivity providers in Sri Lanka

   d) Provide modular, interoperable components intended to integrate with connectivity underlays supplied by others

The intention of this RFI is to encourage inclusive, broad-based market participation and allow for multi-vendor, interoperable, and partnership-driven architectures that avoid lock-in and support the long-term sovereignty requirements of the Government of Sri Lanka.

4. Scope of Requirements

4.1. Core Network Capabilities

i) Centralised SD-WAN management and orchestration

ii) Dynamic path selection and intelligent traffic steering

iii) Application-aware routing and optimisation

iv) Multi-region routing and cloud on-ramp capabilities

v) Coexistence with current LGN/MPLS during migration

4.2. Security Requirements

To ensure secure, policy-driven access to Sovereign Government Cloud services across ministries, provincial/district offices, field officers, and remote GN-level sites, solutions must align with a Zero Trust architecture and incorporate strong network, identity, and endpoint-level controls. Respondents are required to demonstrate how their solution provides comprehensive protection across the entire access path from user to device to application while supporting diverse connectivity conditions, including low-bandwidth and mobile-only environments.

Solutions must support the following capabilities:

i) Zero Trust Network Access (ZTNA) with granular, application-level access control

ii) Next-Generation Firewall (NGFW) with IPS/IDS capabilities

iii) End-to-end encrypted tunnels for traffic protection

iv) Device trust and endpoint posture validation, including real-time compliance checks

v) Identity-based policies with MFA, leveraging government identity systems

vi) Behavioral analytics and anomaly detection for proactive threat defense

vii) Compliance with the Sri Lanka Data Protection Act and Electronic Transactions Act

viii) Security for end-user devices across all locations, covering both government-owned and BYOD
ix) Support for secure browser-based access, including browser isolation or secure enterprise browsers
x) Ability to operate in constrained or mobile-only environments, especially at GN-level sites
xi) Endpoint-level Zero Trust enforcement, combining identity, posture, and contextual risk signals
xii) Clear licensing models, including device-based, user-based, and government-wide options

4.3. Connectivity & Integration Requirements

Solutions must operate effectively across a wide range of connectivity conditions, including:

i) Fixed Connectivity: Fibre / FTTx, Business broadband / DIA, MPLS / L2/L3 VPN / private WAN
ii) Wireless & Last-Mile Connectivity
  a) 4G / 5G mobile broadband (primary or backup)
  b) Fixed wireless LTE CPE
  c) Microwave or satellite links (where necessary)
iii) Remote & Micro-Site Scenarios (GN-Level) , Solutions must support:
  a) Remote GN offices with only mobile broadband
  b) Low-bandwidth or intermittent connectivity

Single-officer locations using:

iv) Small form-factor SD-WAN/SASE devices with zero touch provisioning
  a) Dual-SIM routers
  b) ZTNA-only client access
v) Integration Requirements
  a) API-based integration with LGN orchestrator and Sovereign Cloud
  b) Traffic anchoring within Sri Lanka
  c) Identity and application-aware routing
  d) Real-time link monitoring and automated failover

Respondents must specify minimum connectivity baselines for:

vi) Large ministries/departments/central offices
vii) Provincial/district/divisional offices
viii) Local authorities
ix) GN-level or similar micro-sites
x) Remote Fields

4.4. Secure Isolation Model

i) Support for logical segregation per government entity / clusters
ii) Secure tunnel establishment for mobile and fixed users
iii) Traffic isolation and segmentation mechanisms

4.5. Identity & Access Management

i) Integration with Government Officer Digital ID and SLUDI systems
ii) Centralized SSO capability

iii) Identity-based access policies
iv) Context-based access policies
v) Device identity and posture checks
vi) MFA and passwordless authentication

4.6. Monitoring, Analytics & SOC Integration

i) Centralised network and security visibility
ii) Integration with Government SOC
iii) AI-driven threat detection and anomaly analysis
iv) Reporting on policy violations and abnormal behavior

4.7. Scalability & Reliability

i) Scalability from pilot deployment to nationwide over 1 million user base
ii) Horizontal scalability across geographic regions
iii) Guaranteed SLA of minimum 99.9% uptime
iv) Multi-region failover and active-active capability

4.8. Cost Model, TCO & Decision Framework Requirements

To support a transparent and objective evaluation of the future LGN 3 architecture, respondents are required to provide a comparative Total Cost of Ownership (TCO) and Operating Model analysis across the following deployment models:

Model 1 – SD-WAN Over Commodity Internet
(leveraging fiber, broadband, DIA, 4G/5G)

Model 2 – ZTNA-Only Access Over Commodity Internet
(agent-based access without branch CPE)

Model 3 – Service-Provider Private Network with Integrated Security
(MPLS, L2/L3 VPN, provider-managed SD-WAN/security stack)

Model 4 – Any combination of above

4.8.1. TCO Requirements

Vendors must submit:

i) 5-year and 10-year TCO projections
ii) CapEx vs OpEx analysis
iii) SASE vs SDWAN vs Service Provider Network cost models
iv) Per-user and per-site cost scalability
v) License renewal and upgrade costs
vi) Operational cost optimizations

4.8.2. Decision Framework: SASE vs Branch-Level Connectivity

Vendors must provide a clear framework indicating:

i) When SASE should be used
ii) When SD-WAN branch devices are required
iii) When Service provider operated managed service required
iv) When hybrid models are optimal

Scenarios must include:

i) High-density urban offices
ii) Remote rural offices
iii) Mobile workforce
iv) Agencies with local servers
v) Disaster recovery scenarios

4.8.3. Licensing Models

Respondents must outline:

i) Subscription models
ii) Perpetual models
iii) Hybrid licensing
iv) Usage-based pricing
v) License portability
vi) Exit strategy
vii) Government-wide volume licensing

5. Information Requested from Respondents

Part A – Company Profile

a) Overview of organization and presence in Sri Lanka
b) Experience in large-scale government WAN implementations

Part B – Solution Overview

a) Description of proposed solution and product stack
b) Architecture diagram and deployment model
c) Data sovereignty compliance

Part C – Technical Compliance Matrix

a) Detailed response mapping against each requirement in Section 4

Part D – Implementation & Support

a) Recommended pilot implementation plan
b) Change management and training strategy
c) Support model and SLAs

Part E – Pricing & Licensing

a) Pricing model and indicative government-wide pricing
b) Additional implementation and support costs

Part F – Case Studies

a) Past government implementations
b) Lessons learned and outcomes

6. Migration Strategy Requirements

Respondents must provide a phased migration strategy from the current LGN MPLS-based model to the proposed LGN 3 architecture, including coexistence model, risk mitigation strategies, rollback mechanisms, and change management frameworks.

7. Key Areas of Considerations

The following areas will guide the evaluation of responses:

i) Alignment with LGN 3 strategic vision
ii) Scalability and resilience capability
iii) Security maturity - Integration flexibility
iv) Migration feasibility
v) Cost model transparency
vi) Vendor credibility and experience
vii) Redundancy for the Branch level Connectivity

8. Post-RFI Engagement Process

Following evaluation, the GoSL may invite selected respondents for technical workshops, solution demonstrations, and architecture validation discussions with subject matter experts.

9. Instructions for Respondents

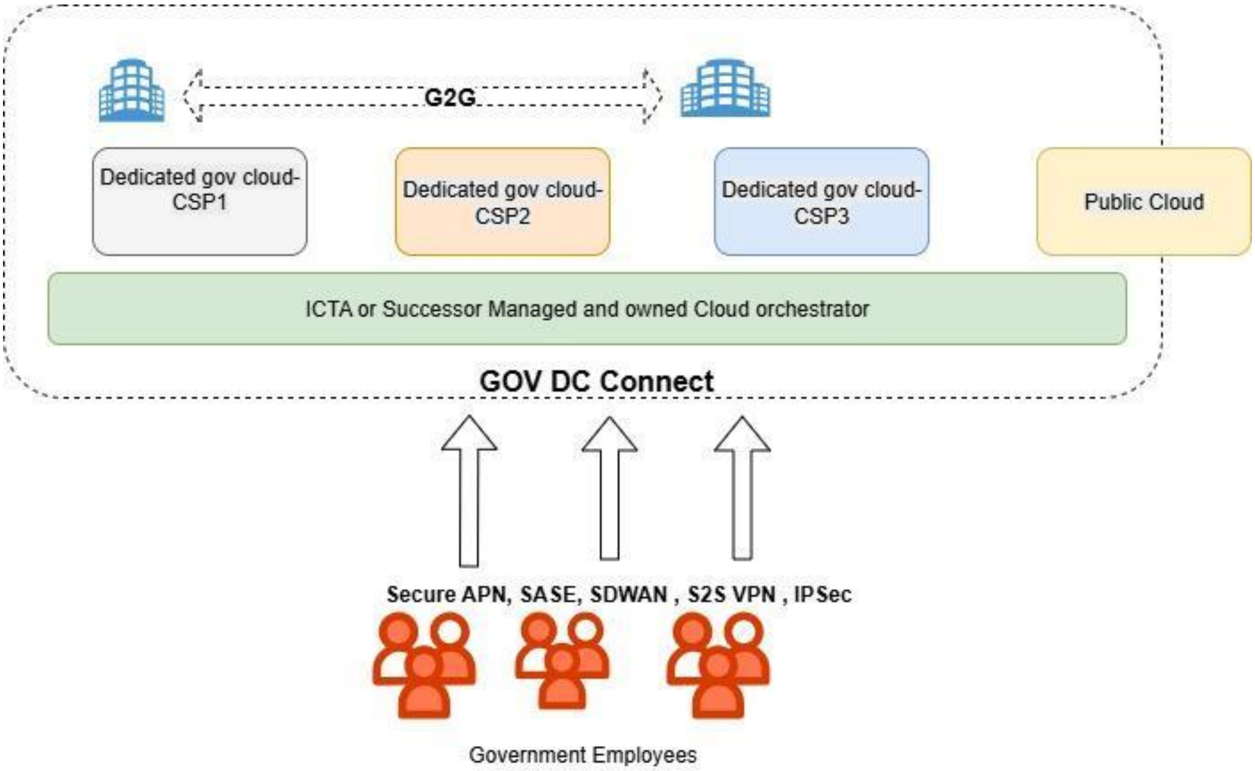
Responses must be submitted electronically in PDF format to procurement@mode.gov.lk

Email Subject: “Response to RFI: LGN 3 Secure Access Fabric”

Responses must follow the structure outlined in this document and be submitted in English.

Closing Date: 17.02.2026 at 17:00 (SLST)

Annexure 1: High-Level Design Diagram of Envisioned LGN 3


G2G
Dedicated gov cloud-CSP1
Dedicated gov cloud-CSP2
Dedicated gov cloud-CSP3
Public Cloud
ICTA or Successor Managed and owned Cloud orchestrator
GOV DC Connect
Secure APN, SASE, SDWAN , S2S VPN , IPSec
Government Employees