# Secured Edge Node Technical Compliance Register: Nokia Altiplano Access Controller Open API

## SECURITY POSITIONING

The Nokia Altiplano Access Controller represents a paradigm shift in fixed access network security, functioning not as a traditional hardware perimeter device but as a cloud-native, software-defined domain controller that enforces security through open, programmable interfaces. In the context of an increasingly distributed and multi-vendor access environment, the Access Controller serves as the centralized policy and authentication authority, brokering secure interactions between operations support systems (OSS/BSS), orchestration layers, and the underlying physical and virtual network functions. Its security posture is fundamentally rooted in the rigorous application of open API standards, enabling granular access control, encrypted telemetry, and tamper-evident audit trails across the entire access domain. The platform is designed to meet the stringent compliance requirements of carrier-grade deployments, providing a hardened software foundation that abstracts the complexity of multi-technology, multi-vendor network management while maintaining strict isolation between tenants, services, and management planes .



LINE-RATE ENCRYPTION AND API SECURITY CAPABILITIES

The security architecture of the Altiplano Access Controller is delivered through a comprehensive suite of open API mechanisms and encrypted transport protocols. All northbound and southbound communication channels are secured via TLS 1.2 or higher, ensuring confidentiality and integrity for data in transit. The Northbound Interface (NBI) exposes RESTCONF and REST APIs that are protected by OAuth 2.0 and OpenID Connect, leveraging Keycloak for identity and access management. This enables fine-grained Role-Based Access Control (RBAC), allowing operators to define precise permissions for distinct user groups, such as network administrators, field technicians, and wholesale tenants . For high-volume telemetry and event streaming, the platform utilizes Kafka with SSL/TLS encryption, providing a secure, scalable message bus for alarm and performance data. Additionally, the API framework supports

intent-based networking (IBN) abstractions, which decouple business intent from device-specific configuration. This not only reduces operational errors but also enforces policy consistency, preventing unauthorized configuration drift. The Developer Portal and SDKs further extend security by enabling operators to build and onboard custom applications within a controlled, authenticated sandbox environment, ensuring that third-party extensions adhere to the same rigorous security standards as native microservices .

## PHYSICAL TAMPER-RESISTANCE AND PLATFORM HARDENING

While the Access Controller is primarily a software platform deployed on commercial off-the-shelf (COTS) or cloud infrastructure, its security hardening extends to the underlying host and orchestration layers. The platform is delivered as a set of Docker containerized microservices, providing process isolation and immutable infrastructure benefits. Security best practices are enforced through the deployment lifecycle, including the mandatory replacement of default credentials, the disabling of unnecessary physical interfaces (such as USB ports) on the host hardware, and the application of regular security patches to the operating system and container runtime . The system supports X.509 certificate-based authentication for all internal and external endpoints, with the capability to integrate with an operator ‘s Public Key Infrastructure (PKI) or utilize self-signed certificates managed by the

platform’ s internal Certificate Authority. For deployments requiring enhanced physical security, the Access Controller can be hosted in hardened, tamper-evident server chassis within controlled datacenter environments, adhering to the physical access controls mandated by standards such as ISO/IEC 27001. The platform ‘s cloud-native elasticity also allows for the rapid re-deployment of compromised instances, minimizing the blast radius of any potential security incident .

DETAILED PARAMETERS

The following table delineates the critical security and compliance parameters of the Nokia Altiplano Access Controller Open API framework.

| **Parameter** | **Specification** |
|---|---|
| Deployment Model | Cloud-native, containerized microservices (Docker/Kubernetes) |
| Northbound API Protocols | RESTCONF, REST (HTTPS), Kafka (SSL/TLS) |
| Southbound API Protocols | NETCONF/YANG (TLS), SNMPv3, SSH |
| Authentication Framework | OAuth 2.0, OpenID Connect, X.509 Certificates, Keycloak RBAC |
| Encryption Standards | TLS 1.2+, HTTPS, SSL for Kafka, |

| | |
|---|---|
| | WPA2-Enterprise (for managed CPE) |
| API Documentation | OpenAPI (Swagger) specification, Developer Portal with SDKs |
| Audit & Logging | Structured audit logs via Kafka, OpenSearch integration, syslog support |
| Identity Management | External LDAP/AD integration, Keycloak realms for multi-tenancy |
| Policy Engine | Integrated intent-based networking (IBN) with policy enforcement |
| Compliance Support | GDPR, NIS Directive, TIP/ONF interoperability, CJIS (configurable) |

## REGULATORY CERTIFICATIONS AND COMPLIANCE MATRIX

The Nokia Altiplano Access Controller is engineered to facilitate operator compliance with a broad spectrum of international and regional regulatory frameworks. Its API security mechanisms support the data protection and privacy requirements outlined in the General Data Protection Regulation (GDPR), ensuring that subscriber data is processed lawfully and access is strictly logged and auditable. The platform ' s role-based access controls and

encryption standards align with the security objectives of the Network and Information Security (NIS) Directive, aiding operators in securing critical network infrastructure. Furthermore, the use of standardized YANG models and NETCONF/RESTCONF interfaces promotes interoperability and vendor independence, a key tenet of the Telecom Infra Project (TIP) and Open Networking Foundation (ONF) initiatives. For deployments in the United States, the Access Controller's logging and audit capabilities can be configured to support Criminal Justice Information Services (CJIS) compliance, should the access network serve public safety entities. The platform's software integrity is maintained through signed container images and a verifiable software bill of materials (SBOM), facilitating supply chain security audits and adherence to emerging frameworks such as the Cybersecurity Maturity Model Certification (CMMC) for defense-related networks .

## PERIMETER DEPLOYMENT AND ZERO-TRUST ARCHITECTURE

In a modern fixed access network, the traditional network perimeter has dissolved. The Altiplano Access Controller is designed to operate within a Zero-Trust security architecture, where no entity—whether inside or outside the traditional network boundary—is implicitly trusted. Every API request must be authenticated, authorized, and encrypted. The Access Controller acts as a Policy Decision Point (PDP) and Policy Enforcement Point (PEP) for the access domain,

continuously validating the state of managed devices and the legitimacy of configuration intents. Deployment scenarios typically position the Access Controller within a secure management zone, with strict firewall policies governing ingress and egress traffic to the NBI and southbound interfaces. It integrates with Security Information and Event Management (SIEM) systems via its Kafka-based notification streams, forwarding detailed audit logs of all API interactions, configuration changes, and authentication events. This enables security operations centers (SOCs) to correlate access network events with broader IT security telemetry, providing a unified view of the threat landscape. By centralizing control through open, secure APIs, the Altiplano Access Controller transforms the fixed access network from a collection of isolated elements into a cohesive, defensible, and compliant digital asset .

