Non-3GPP interworking function (N3IWF)

Untrusted access security frameworks for 5G

NOKIA

Executive summary

N3IWF is the 5G evolution of ePDG, enabling secure Wi-Fi and other non-3GPP access to integrate natively with the 5G Core. It strengthens identity protection, supports NAS-native services, delivers granular QoS, and improves mobility by aligning non-3GPP access with 5G authentication, policy, and service control.

By extending 5G capabilities beyond the radio network, N3IWF helps operators improve security, simplify migration from ePDG, reduce signaling during inter-access mobility, and create new revenue opportunities such as secure public Wi-Fi, premium AI traffic handling, and mission-grade connectivity for government and defense.

Introduction

Non-3GPP access has become an essential part of mobile service delivery as users increasingly rely on Wi-Fi, enterprise networks, residential gateways, and public hotspots to reach operator services. While these access types extend coverage and improve user experience, they also introduce security, mobility, policy, and service-continuity challenges because the access network is not directly controlled by the mobile operator.

In 4G networks, ePDG addressed this need by providing secure access to EPC-based services, particularly voice and video over Wi-Fi. As operators evolve toward 5G Standalone, however, the same model is no longer sufficient for the full range of 5G services. Capabilities such as NAS-native signaling, per-flow QoS, identity protection, access traffic steering, network exposure, and consistent mobility handling require deeper integration with the 5G Core.

N3IWF provides this 5G-native interworking layer for untrusted non-3GPP access. It enables Wi-Fi and similar access networks to behave more like a 5G access domain from the perspective of authentication, policy, QoS, and service control. This makes N3IWF not only a technical successor to ePDG, but also a strategic foundation for secure service parity, smoother migration, and new monetization models across consumer, enterprise, and public sector use cases.

ePDG: legacy solution

The evolved Packet Data Gateway (ePDG) is the 4G/EPC gateway for untrusted non-3GPP access, terminating the SWu interface from the UE using IPsec with IKEv2 for control-plane signaling and ESP for user-plane encryption, and integrating with the EPC via PGW-C/PGW-U over GTPv2 for control traffic and GTPv1 for user traffic. Authentication is anchored in AAA/HSS using EAP-AKA, with the ePDG receiving UE identifiers such as IMSI/IMEI during initial attach, directly from the UE, and through Diameter exchanges with the AAA server. ePDG's operational value is demonstrated by mature deployments for IMS offload, including VoWiFi and ViWiFi, stable device interoperability, and proven continuity across Wi-Fi and LTE/EPC domains.

These strengths make ePDG effective for today's voice-over-Wi-Fi use cases. However, ePDG's architecture is tightly coupled to 4G/EPC control and does not carry NAS, which constrains delivery of 5G services over non-3GPP access. Its authentication approach differs from 3GPP radio access, resulting in mandatory reauthentication during inter-access handovers, such as Wi-Fi to LTE/5G and back, and its QoS tools are coarser than 5G's QFI-based enforcement, limiting per-flow differentiation and precise policy control.

While ePDG successfully extends 4G services over Wi-Fi, it was not designed to deliver the full range of 5G capabilities, including NAS-native services, seamless mobility, and granular QoS control.

N3IWF: forward looking solution

N3IWF is specified by 3GPP as an NG-RAN element for untrusted non-3GPP access in 5G, mirroring gNB behavior on the control and user planes while serving Wi-Fi and residential gateways. Its principal interfaces are N2 between N3IWF and AMF using NGAP over SCTP for control-plane signaling, and N3 between N3IWF and UPF using GTPv1 for user-plane traffic. It also supports the virtual N1 interface between UE and AMF, which traverses NWu, and the Y1 and Y2 reference points between UE and Wi-Fi access point, and Wi-Fi access point and N3IWF respectively. NWu is the main interface for untrusted access, carrying control and user traffic inside IPsec: IKEv2 for signaling and ESP for payload encryption. On the control plane before IPsec establishment, the UE's NAS messages, encrypted end-to-end between UE and AMF, are encapsulated into IKEv2 via the EAP-5G payload defined by 3GPP for N3IWF. After the signaling IPsec tunnel is established, NAS travels over TCP within the IKEv2 tunnel, simplifying subsequent control exchanges. For the user plane, PDU packets arriving from the UPF over N3 using GTPv1 are encapsulated in GRE and transported via ESP within the IPsec tunnel between the UE and N3IWF. Crucially, child Security Associations can be established per Quality Flow Identifier, enabling per-flow encryption contexts and policy enforcement coordinated by SMF/PCF instructions delivered through AMF, achieving gNB-like QoS granularity across non-3GPP access.

Summarizing, the N3IWF operates through three essential interfaces, each serving a distinct purpose in enabling seamless connectivity:

- **NWu Interface:** This interface acts as a secure bridge between user equipment (UE) and the 5G core network. Utilizing advanced IKEv2/ESP protocols, it establishes encrypted tunnels that protect both user data and control signals, ensuring integrity and security over untrusted networks. For user plane traffic, the Protocol Data Units (PDUs) are carried over GRE (Generic Routing Encapsulation) over IPsec.
- **N2 Interface:** Serving as the primary communication channel between the Access and Mobility Management Function (AMF) and N3IWF, the N2 interface manages critical network functions such as session control and mobility management. It uses the NGAP protocol, which is similar for both 3GPP and non-3GPP access, ensuring smooth data flow.
- **N3 Interface:** Responsible for user data transmission within the core network, the N3 interface uses the GTPv1 protocol to maintain precise mapping between secure tunnels and data sessions. This ensures efficient and secure data delivery to its destination.

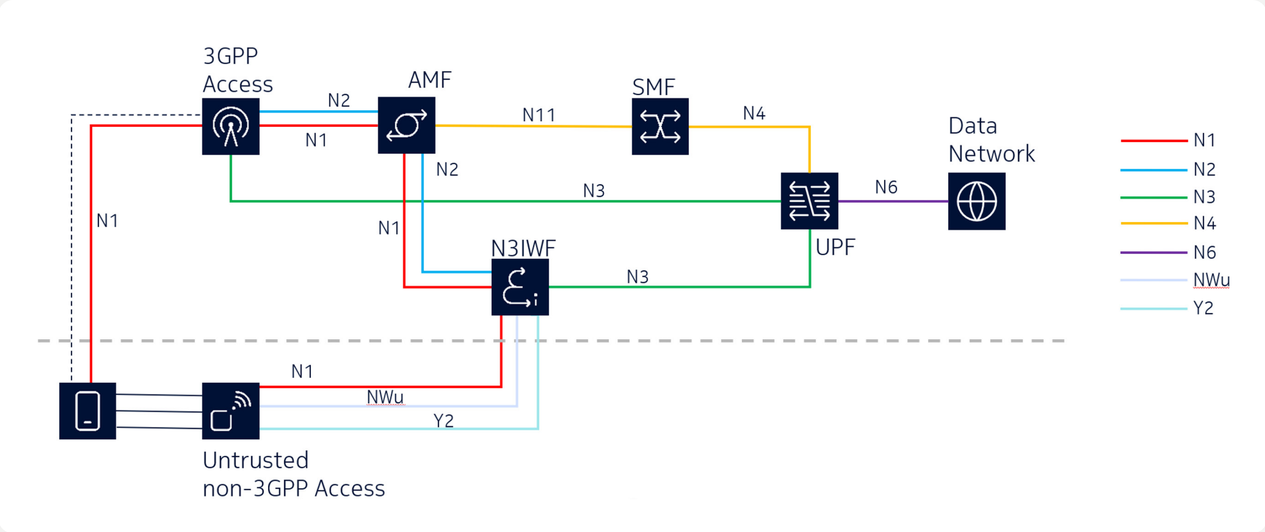
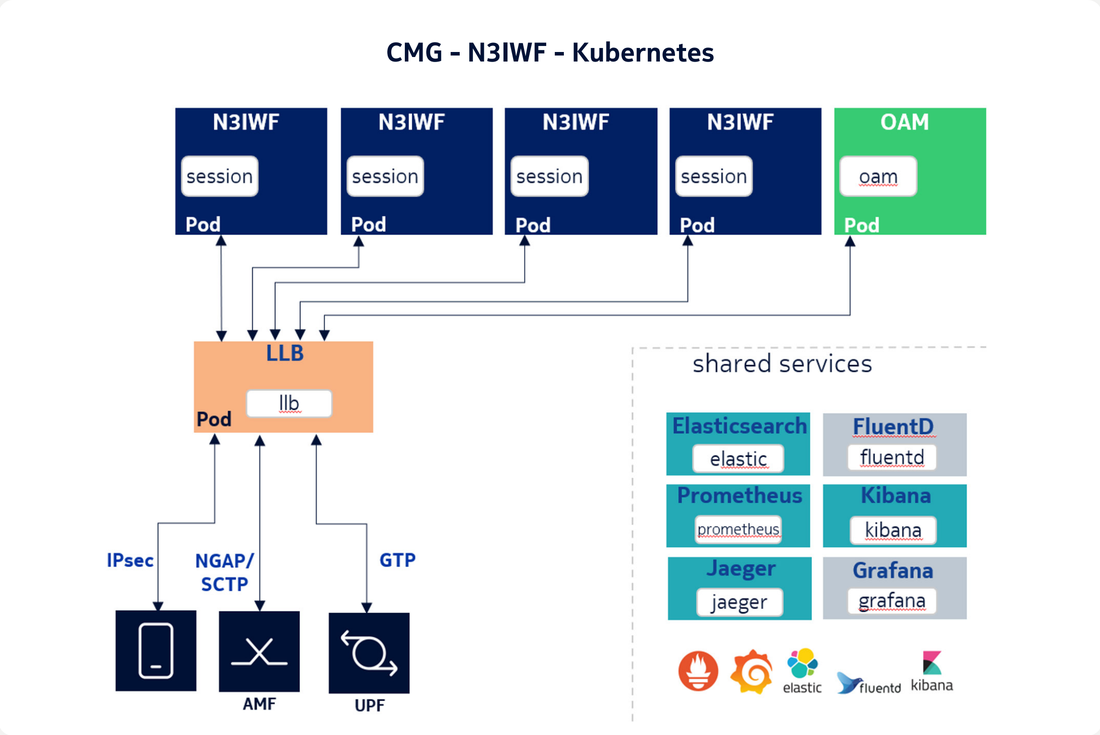
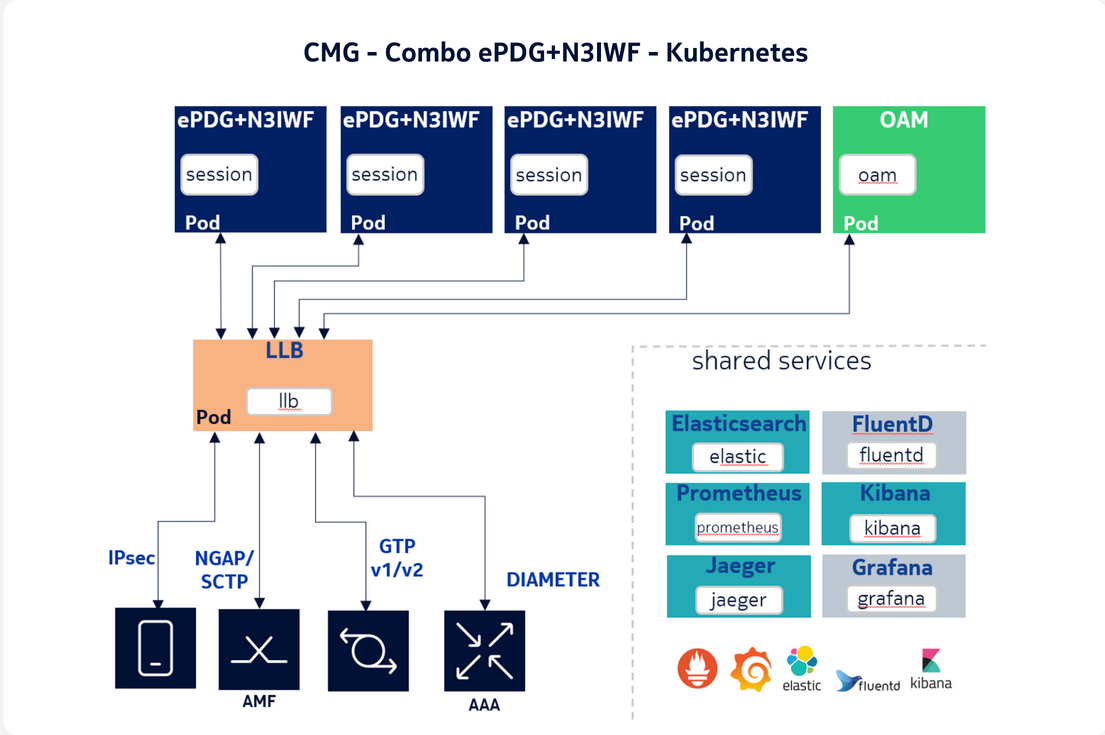


Figure 01: Non-3GPP current architecture

N3IWF's security and authentication model follows 5G principles by deferring authentication, authorization, and key handling to AMF/AUSF/UDM via NAS and EAP-AKA' (AKA Prime). This strengthens cryptographic protection compared with EAP-AKA through improved key derivation, stronger hashing, and better resistance to downgrade attacks. UE identities such as SUPI, SUCI, 5G-TMSI, and legacy IMSI are not exposed to N3IWF because NAS is encrypted end-to-end between UE and AMF and then encapsulated in the encrypted IKEv2 exchange, effectively applying layered encryption to identity-carrying messages. Service delivery is NAS-native, enabling **Network Slice Support**, Access Traffic Steering, Switching and Splitting (ATSSS), SMS over NAS, UE Route Selection Policy (URSP), XR Management (XRM), and Network Exposure Function (NEF) capabilities directly, as in 5G RAN access. Mobility is comprehensive: N3IWF supports inter-access handovers between N3IWF and gNB, N3IWF and EPC, and MOBIKE-based Wi-Fi access point transitions for IPsec mobility. Because authentication architecture is common across 3GPP and non-3GPP access, inter-access handovers generally avoid full reauthentication, reducing signaling by approximately 6–10 messages per handover per UE, which can aggregate to significant load reduction at scale.





Cloud deployment options include standalone N3IWF pods with OAM and a front-end load balancer (LLB) terminating IPsec toward UEs and distributing NGAP/SCTP, GTPv1, and management traffic internally.

A 3GPP accepted mechanism uses the IDi payload type in IKEv2 to differentiate the attach type (ePDG vs N3IWF) on a common termination, allowing seamless steering based on UE preference parameters and operator policy. In the device ecosystem, MediaTek chipsets have validated N3IWF via an IODT on Android devices, covering all UE call flows without issues.

A combo deployment option can co-locate ePDG and N3IWF functions on the same gateway pod, co-function at the same time, present a single IP address for both SWu and NWu toward UEs, and dynamically share CPU and memory resources between ePDG and N3IWF without manual partitioning. This combo pod supports IPsec for UE tunnels, NGAP/SCTP for AMF control, GTPv1 to UPF for N3IWF, GTPv2 C/U to PGW-C and GTPv1 to PGW-U for ePDG, and Diameter for AAA signaling.

Drivers for N3IWF

Architecturally, ePDG remains a 4G/EPC core element optimized for IMS voice and video over WiFi, whereas N3IWF is a 5G NGRAN element that presents gNodeB-equivalent control and user plane behavior for non-3GPP access.

- In security, ePDG relies on EAP-AKA with AAA, which is less aligned with modern 5G security requirements and exposes UE identifiers during attach and Diameter exchanges. N3IWF implements EAP-AKA' under a NAS-centric model where UE identities remain protected inside NAS and IKEv2 encryption, making N3IWF more privacy-preserving and more resistant to downgrade and interception risks.
- In mobility, ePDG's authentication architecture differs from 3GPP access and requires reauthentication during inter-access handovers, increasing signaling and latency. N3IWF's common authentication framework across access types avoids most reauthentication events, saving approximately 6–10 messages per inter-access handover per UE and improving session continuity.
- In services, ePDG does not carry NAS and therefore cannot deliver NAS-native 5G capabilities such as **Network Slice Support**, ATSSS, URSP, SMS over NAS, and XR Management. Its NEF exposure over Wi-Fi is more complex and device dependent, while N3IWF provides NAS-native services and NEF integration directly, ensuring parity with 5G RAN access.
- In QoS, ePDG's mechanisms are less granular than 5G's per-QFI enforcement, while N3IWF applies QoS at the QFI level as instructed by SMF/PCF via AMF and maps QFI to dedicated child Security Associations, enabling per-flow security and policy treatment for applications such as AI inference streams or XR traffic.
- In deployment, ePDG typically runs as a separate footprint, whereas a combo architecture runs ePDG and N3IWF on a single pod with a single UE facing IP, dynamic resource pooling, multiprotocol support (NGAP/SCTP, GTPv1U, GTPv2C, Diameter), and IKEv2/IDi attach differentiation, simplifying migration and maximizing hardware utilization.
- Finally, from a lifecycle perspective, ePDG is bounded to the EPC era, while N3IWF is designed for 5G, supporting a longer-term investment horizon with limited architectural rework, depending on deployment context.

N3IWF key drivers

The **primary driver** is elevated security aligned with 5G principles: identity confidentiality through NAS encryption, layered encryption and encapsulation via IKEv2, and stronger authentication with EAP-AKA'. This is particularly relevant for public Wi-Fi and enterprise scenarios where operators can offer encrypted, untrusted access for broadband data beyond IMS traffic.

A **second driver** is access-agnostic service parity: NAS-native capabilities ensure that the UE experiences consistent policy, exposure, and feature delivery across 3GPP and non-3GPP access, which simplifies service engineering and enhances user experience.

A **third driver** is precise QoS, **Network Slice Support** and monetization potential: per-QFI policy and per-QFI child Security Associations enable differentiated services with measurable SLAs, supporting latency-sensitive gaming, XR, and AI traffic flows that can be routed to specific or edge UPFs for performance guarantees. Coupled with dedicated network slice support (that allocates specific network resources for specific slices), over NAS (which is native in 5G for non-3GPP access), the delivered E2E QoE for the end user is superior and tailored to exact service requirements and use case requirements for any commercial or enterprise environment. Operationally, reduced inter-access signaling lowers control-plane load and latency and can reduce opex, while comprehensive tracing and KPI/KCI support improve assurance and troubleshooting across NWu, N2, and N3. Cloud simplicity and migration are also compelling, as the single-IP SWu/NWu terminator and dynamic multifunction pods reduce network design complexity and capacity partitioning, making it easier to use UE preference parameters to steer between ePDG and N3IWF.

N3IWF key advantages

1. **Enhanced Security Architecture**
   - N3IWF is directly integrated with the AMF, responsible for authentication procedures towards the AUSF and UDM systems. This integration enhances security by providing a unified authentication and encryption framework for both 5G 3GPP and non-3GPP access networks, ensuring consistent protection of user data across all access technologies.
   - The N3IWF operates solely with temporary identifiers, as it never has direct access to permanent subscriber identities (IMSI/SUPI/SUCI) of the User Equipment. These sensitive identifiers are transmitted exclusively within the NAS layer, which maintains end-to-end encryption between the UE and AMF. This encrypted NAS communication is further secured within the IKEv2 Security Association.
   - Since the N3IWF only processes temporary session identifiers and never stores permanent subscriber data, it enhances network security through compartmentalization. This design principle ensures that even if an N3IWF instance is compromised, no sensitive customer information can be exposed, thereby minimizing potential security risks to the network.
   - UE authentication to AUSF/UDM is based on EAP-AKA' (AKA Prime), strengthening authentication compared with EAP-AKA.
2. **Superior Service Delivery**
   - N3IWF allows end users to experience the same end-to-end services regardless of whether the UE is connected to 3GPP or non-3GPP access. This includes NAS-based signaling for services like **Network Slicing**, SMS, URSP, ATSSS, XRM, and any 5G or NAS-based service.
   - N3IWF offers the same Quality of Service (QoS) design as 5G 3GPP access. PDU sessions over the UPF and N3 interface are based on QFIs (QoS Flow Identifiers), mapped to one or more child Security Association tunnels to the UE. This architecture allows operators to control delivered QoS with fine granularity.
   - N3IWF can offer Network Exposure Functionality capabilities, exactly as in 5G 3GPP access, and allow the operator to offer unique differentiated end user experience based on different factors like Network slicing, QoS control, Policy Enforcement, Data Analytics and Monetization. This native NEF support can leverage highly popular commercial services like Low Latency Gaming, VR/AR, Streaming, Immersive Gaming Experience and more.
3. **Signaling optimization**
   - Reauthentication is generally not required during mobility between 3GPP and non-3GPP access, because security material can be derived from previous authentication. This saves signaling, energy, and time during mobility, especially for UEs that frequently move between access types, such as those in public areas or transport environments.

Revenue opportunities

As operators confront escalating security expectations, ubiquitous public Wi-Fi usage, and the rapid rise of AI-driven applications, N3IWF emerges as a pivotal platform to monetize connectivity while strengthening customer trust. By securely anchoring non-IMS traffic and enabling deterministic quality of experience, N3IWF allows carriers to offer differentiated services that address the most pressing concerns of consumers, enterprises, and public sector organizations. The result is a pragmatic, near-term path to revenue that leverages existing cloud and core assets, while laying the groundwork for advanced capabilities aligned with 5G evolution.

Secure Internet Traffic over Public Wi-Fi:

Public Wi-Fi is ubiquitous but often insecure, exposing users and carriers to elevated risk from hacking and data breaches. Operators can mitigate this by carrying data traffic over N3IWF, which provides stronger security than ePDG. By offering an “always-secure public Wi-Fi” add-on, operators can charge end users a small monthly fee to route internet traffic through encrypted tunnels whenever devices connect to public access points. North American operators have expressed interest, noting that existing cloud infrastructure can be repurposed for N3IWF—or a combined ePDG + N3IWF setup—allowing rapid introduction of this service with minimal incremental cost. The net result is a low-capex path to new revenue while enhancing customer trust and brand differentiation through better security.

Monetizing AI traffic with 5G slicing via N3IWF:

AI workloads are rapidly proliferating across consumer and enterprise devices. Operators can capitalize on this trend by establishing dedicated network slices or DNNs on the core and N3IWF for AI traffic originating from user equipment. Dedicated AI slices can reduce latency and enable advanced features by steering traffic to specific UPFs, including local or edge UPFs deployed on service provider premises, such as at major device or AI ecosystem partners. This creates multiple revenue streams: premium AI QoS offerings for end users, SLA-backed connectivity for device and AI vendors, and potential sales of edge UPF deployments to partners. In a market where device and AI vendors are competing to deliver the best user experiences, operators can position themselves as enablers of predictable performance and localized processing.

Military and Government Services with N3IWF:

Defense and government organizations have shown sustained interest in N3IWF since its introduction in 3GPP standards, driven by its security and architectural advantages over ePDG. With Nokia N3IWF available, engagement has increased across regions. Two early use cases are prominent. First, N3IWF-enabled Wi-Fi access points can terminate NWu tunnels directly to the N3IWF, providing secure internet and voice services without requiring immediate N3IWF support on end devices, accelerating adoption while maintaining strong end-to-end security. Second, agencies are encouraging vendors to deliver laptops, tablets, and handsets with native N3IWF support to enable secure mobility outside office environments. Together, these models support near-term deployment flexibility and longer-term device-level integration, positioning N3IWF as the preferred solution for 5G security, service delivery, and lifecycle longevity.

N3IWF enables operators to convert security and performance into tangible revenue: secure public Wi-Fi connectivity for consumers, premium AI traffic handling for both end users and ecosystem partners, and mission-grade services for defense and government. Its security posture, service agility, and 5G readiness make it a durable foundation for new monetization models.

Conclusion

N3IWF is the evolution of ePDG for 5G non-3GPP access. It provides RAN-grade security, supports NAS services natively, and delivers gNodeB-level QoS granularity over encrypted IPsec tunnels. The architecture preserves UE identity confidentiality, reduces inter-access signaling through common authentication, and supports comprehensive mobility, including MOBIKE, for Wi-Fi-based access.

N3IWF enables policy-based service control via standard 5G functions such as NEF, ATSSS, URSP, and XR features. These capabilities allow operators to implement secure Wi-Fi access, traffic steering across access types, and application-specific policies with consistent QoS and charging on non-3GPP connections.

Many market implementations support combined ePDG and N3IWF deployment to ease migration. Typical capabilities include a single IP address for SWu/NWu termination, dynamic resource sharing at node or pod level, full protocol interworking, including NGAP, GTPv1-U, GTPv2-C, and Diameter, and 3GPP-accepted IDi-based attach differentiation. This approach permits running legacy ePDG features alongside next-generation N3IWF services with limited network redesign, depending on deployment context.

As a result, N3IWF is suitable for Wi-Fi–based access services across 5G. Compared to ePDG, it offers critical improvements in security, mobility handling, and end-to-end service control, while combined deployments provide a practical path to adopt N3IWF with minimal disruption.

Nokia OYJ
Karakaari 7
02610 Espoo
Finland

Tel. +358 (0) 10 44 88 000

CID: 215501

nokia.com

About Nokia

Nokia is a global leader in connectivity for the AI era. With expertise across fixed, mobile, and transport networks, we're advancing connectivity to secure a brighter world.