The Nokia Cloud Mobile Gateway (CMG) is a multi-functional packet core mobile gateway that provides increased deployment flexibility, elastic scale, high reliability and the capacity to deliver a full range of mobile and IP services. Its cloud networking and state-efficient design meets the growing bandwidth and device connectivity demands for 4G, 5G and the Internet of Things (IoT). The CMG draws on the field-proven Nokia 7750 Service Router (SR) Mobile Gateway Operating System (MG-OS) software, which ensures service and operational consistency. The CMG operates in both virtualized and cloud network environments. It can be managed in either a cloud/IT life-cycle management or a traditional Telco network management operations model with a common packet core management system. The CMG gives communications service providers (CSPs) and enterprises a cloud-native architecture that supports the transition to cloud and software-defined networking (SDN) while providing both 5G non-stand-alone (NSA) and stand-alone (SA) core functions.
CMG features

Deployment flexibility
The CMG supports a wide range of mobile gateway functions in the mobile packet core, supporting 2G/3G/4G/5G cellular and Wi-Fi® access networks. Specifically, the CMG supports the following cloud network functions:

- Gateway GPRS Support Node (GGSN)
- Home Agent (HA) (3GPP2)
- Serving Gateway (SGW)
- Evolved Packet Data Gateway (ePDG)
- Trusted Wireless Access Gateway/Proxy (TWAG/TWAP)
- Subscriber Services Gateway (SSG)
- Session Management Function (SMF)
- User Plane Function (UPF)
- Network Repository Function (NRF)
- Network Slice Selection Function (NSSF)

These network functions can be deployed as separate virtual instances or in combination, providing maximum configuration flexibility.

Utilizing field-proven software from the Nokia 7750 Mobile Gateway and IP/MPLS service edge router, the CMG offers a comprehensive mobile core feature set that supports the following:

- Enhanced mobile broadband (eMBB) data services for 4G/5G consumers
- Mobile enterprise virtual private network (VPN) services with service assurance and charging
- Public safety, government and military applications for highly reliable/mobile broadband video and data services
- IoT and machine type communications (MTC)
- Enhanced mobile packet voice — voice over LTE (VoLTE) and voice over Wi-Fi (VoWi-Fi)
- Personalized, value-added data services with application and service assurance

CMG VNF architecture
A disaggregated, decentralized Virtual Network Function (VNF) tiered architecture is used in the CMG design (Figure 1):

- Operations, administration, and maintenance (OAM): Performs the control plane functions for the CMG, including management of the individual tiers and routing protocols
- Supported management interfaces: SNMP/Telnet/SSH/CLI and NETCONF/YANG
- Common data layer: Stores subscriber state and provides backup of session information
- Load balancer: Provides external network connectivity (input/output) to mobile gateway functions and load distribution across the CMG VNF. It supports the CMG micro-nets, response time monitoring, RTM, multiple VPRN/VRF, VPLS and contains the mobile gateway tunnel endpoint identifier (TEID) table. The load balancer forwards session and signaling traffic to the assigned control plane processing instance and optionally the user data traffic to the user plane forwarding instance. Optionally the load balancer can be removed from the CMG user plane VNF, providing increased throughput capacity for certain applications.
- Control plane processing: Performs the call/session processing functions as well as link termination interface (logical) and protocol termination (GTP-C, PMIP, Diameter, RADIUS, IPSec and HTTP/2), and the control plane for the Policy and Charging Enforcement Function (PCeF), as well as the control plane functions of multiple gateway types on a single virtual instance. With the evolution to 5G Core, it also supports the SMF, NRF and NSSF.
- User plane forwarding: Performs the packet processing, forwarding and policy enforcement of session data flows of the supported mobile gateway functions. User plane forwarding can be provided with and without the load balancing and either on server-based or physical hardware-based platforms delivering even greater capacity and performance.
Cloud-native design

The CMG application software has been built from the beginning on the principles and design requirements of cloud networking and web-scale while retaining the feature parity and field reliability of the existing physical Nokia Mobile Gateway. Its control plane is highly resilient, delivering the bearer and system level management with the reliability that is expected in the core network. Field-proven protocols that can handle failure scenarios or race conditions are the foundation of the CMG software.

The CMG cloud-native design supports the control and user plane separation (CUPS) delivering the independent scalability to meet the subscriber and IoT device capacities needed for today’s 4G and 5G services. This flexibility enables a distributed mobile gateway core architecture with either control or user plane resources deployed in either edge or centralized data centers. State-efficient processing intelligently moves session state information out of the CMG control plane cache into an external common data layer repository, which significantly improves scale and network resource utilization.

The CMG user plane forwarding uses a distributed processing architecture that supports dynamic scale and flexibility. The Nokia MG-OS is a compact software image that is optimized to operate on a very small memory footprint. This compact image is beneficial for server packet processing by minimizing CPU cache and delivering high packet processing throughput. The CMG implements a unique cloud forwarding data plane architecture, which is based on the in-house networking processor expertise and design concepts that minimize the packet handling, reduce the number of copies, limit header manipulations and optimize cache usage.

Service-based architecture

When the CMG is deployed in 5G SA networks, it supports a service-based architecture (SBA) where core functions use a services model in the control plane to communicate with RESTful APIs (OpenAPI 3.0) over TCP and HTTP2.0 protocols and JSON object serialization. In a SBA, 5G Core functions register with the NRF, providing a profile of its capabilities that can be discovered by other core network functions. In addition to the mobile gateway functions, the CMG supports the NRF in the 5G Core.

In addition to supporting various core network slicing methods (GWCN, eDECOR), the CMG supports 5G SBA network slicing where network resources are allocated to services and/or tenants. The CMG supports the NSSF either as a stand-alone entity or in combination with the NRF.

The CMG is designed to provide service performance comparable to that of dedicated physical hardware platforms. Its advanced software design and capabilities leverage technologies such as distributed symmetric multiprocessing (SMP) to maximize the use of multi-CPU architectures and a native 64-bit OS to maximize the access to multicore memory.

High performance

The CMG delivers excellent data plane performance and throughput on any server hardware platform. For bandwidth-intensive applications, the CMG can be optionally configured to remove load balancing from the user plane path to provide greater capacity and user plane processing throughput.

The CMG supports virtual input/output (VirtIO) drivers, and optionally, single root I/O virtualization (SR-IOV) together with the Intel® Data Plane
Development Kit (DPDK). For VMware environments, VMXNET3 virtual network device and drivers are supported, which provide improved throughput at higher speeds with no latency degradation.

With these design capabilities, the CMG delivers the software and hardware packet processing performance needed for high-speed mobile broadband services for 4G/LTE and 5G.

**Elastic scalability**

Utilizing the benefits of its cloud-native design, the CMG can flexibly adapt to support a changing mix of control plane and user plane resources. The CMG can also dynamically scale both in and out to meet instantaneous demand for services. The CMG distributed processing architecture enables it to horizontally scale beyond the physical limits of dedicated hardware platforms.

The control plane processing scales CPUs to support signaling and call processing while the CMG data plane can scale out by adding more mobile gateway data forwarding to support increasing user plane traffic. As subscriber growth patterns and traffic models change, the CMG can adjust control plane and data plane resources accordingly. The CMG has no dependencies on the protocol scaling limits in the network, allowing applications to dynamically scale and automatically adapt to loads without the need for CSP intervention.

**Resiliency and reliability**

The CMG is built on the Nokia SR OS, a real-time, modular and highly fault-tolerant OS design that meets carrier-grade network and reliability requirements. This robust software architecture delivers advanced resiliency capabilities, such as high availability and non-stop routing and services.

The CMG supports various intra-VNF redundancy protection schemes (1:1, 1:N, N+K). In addition, the CMG can be deployed in a 1:1 inter-VNF geo-redundant protection scheme. Intra- and inter-redundancy protection delivers reliability and availability levels not easily achieved in IT/cloud networking environments (greater than 99.999 percent).

**Deployment options**

The CMG offers deployment flexibility with multiple packaging options to address targeted service requirements and economic business models. In a fully virtualized network environment, the CMG software runs on an NFV/cloud infrastructure and is life-cycle managed using any MANO system to meet the most demanding scale, capacity and performance service requirements. It can also be deployed as a pre-integrated appliance with CMG software pre-loaded on Nokia AirFrame data center servers to meet the requirements of CSPs that want to continue to operate in their existing management environment. The CMG can also be deployed as a physical hardware-based platform to support existing packet core network expansions or to provide the user plane bandwidth capacity and packet processing that is needed for enhanced mobile broadband and multimedia services.

**CMG management**

For network management in a traditional telecom environment, the CMG is managed by the Nokia Network Services Platform (NSP) and together with Nokia NetAct they provide a single, consolidated view of the entire mobile network. The CMG supports both traditional telco TL1/SNMP and IT NETCONF/YANG management environments. The Nokia NSP is the same network management system (NMS) for the Nokia Cloud Packet Core and backhaul networks. The NSP provides the fault, configuration, accounting, performance, and security (FCAPS) management capabilities and analytics for the CMG and the Nokia mobile gateways. NetAct provides an end-to-end view of the entire mobile network (Radio Access Network [RAN] and mobile core). The NSP also provides an interface to NetAct for fault management and performance monitoring.

In an NFV operations environment, the CMG is orchestrated and managed with any NFV OpenStack-based platform. This gives CSPs and enterprises complete flexibility to select the vendor of their choice for an NFV cloud-networking environment. The NSP also adds a VNF supervision application module, which performs VNF monitoring and supervision providing health status and assisting in the life-cycle management of the CMG.
This module gives mobile CSPs the ability to manage both their physical and virtual packet core networks from the same user interface.

**Comprehensive NFV/SDN portfolio**

For CSPs that want a fully integrated cloud packet core solution, Nokia optionally offers an industry-leading, comprehensive NFV/SDN portfolio that combines the CloudBand™ software suite and Nuage Networks™ Virtualized Services Platform (VSP) along with a broad ecosystem of cloud partners. This complete solution provides smart multi-layer monitoring, alarming and the correlation of events enabling dynamic adjustment to changing demand. CloudBand also enables the automated management of a geo-distributed NFV infrastructure with coherent policies, giving CSPs the ability to quickly deploy the CMG while reducing the network integration support and interoperability risks in a multivendor environment.

**Network functions overview**

The CMG supports multiple network functions in the 3GPP mobile packet core (Figure 2), both individually as separate VNF instances or in combination as a single VNF instance.

*Figure 2. Cloud Mobile Gateway in 3GPP mobile packet core*

**SGW**

The CMG SGW forwards user data packets and acts as the local mobility anchor for the user plane during LTE RAN handovers, as well as handovers with other 3GPP technologies. The CMG supports both a stand-alone SGW instance or a combined SGW/PGW/GGSN single instance.

**PGW and GGSN**

As a stand-alone PGW, GGSN or combined PGW/GGSN, the CMG provides connectivity for user equipment (UE) to external packet data networks and is the mobile network IP anchor point. The CMG performs policy enforcement, packet filtering, charging support, lawful interception and packet inspection for each packet flow.
**ePDG and TWAG**

The CMG functions as either a stand-alone ePDG or TWAG function or as a combined Wi-Fi access gateway combining the functions into a single instance supporting both trusted and untrusted Wi-Fi access. As an ePDG in an untrusted non-3GPP access (public) network, it provides a secure entry point through an IPSec tunnel from the mobile device into the CSP packet core. Both open and closed SSID access devices are supported. The CMG ePDG capabilities support a variety of wholesale and retail deployment scenarios, enabling both wireline and wireless providers to leverage unlicensed Wi-Fi as an access technology. As an ePDG, it coordinates with the CSP’s back-end subscriber, policy and billing infrastructure for the authentication and parameters needed to create subscriber context. Consequently, CSPs have maximum network architecture flexibility and the number of network IP addresses required is reduced.

In a non-3GPP trusted access network, the CMG functions as a TWAG/TWAP by aggregating Wi-Fi traffic from multiple access points and is the proxy to the AAA server. It provides a secure entry point for mobile devices from the trusted Wi-Fi access points to efficiently aggregate subscriber traffic using secure tunneling protocols. This deployment option reduces the number of network IP addresses that are required.

**SMF**

The CMG SMF establishes, modifies and releases 5G sessions for all 5G access types to the 5G Core, provides UE IP address allocation and management, and selection and control of the UPF. It interfaces with the Policy Control Function (PCF), provides the control part of policy enforcement and QoS, as well as lawful intercept. The SMF can be provided as a stand-alone function or in combination with the UPF. PGW-c/SMF and PGW-U/UPF combos are also supported for seamless 4G/5G interworking.

**UPF**

As the anchor point for intra and inter-RAT mobility as well as the interconnect to the data network, the CMG performs the user plane forwarding and routing for the mobile network as well as packet inspection, policy enforcement and lawful intercept user plane collection. It also performs QoS, uplink/downlink rate enforcement and marking at the transport level as well as uplink classification. The CMG supports a stand-alone UPF on either virtualized or physical hardware and in combination with the SGW/PGW user plane functions.

**NRF**

As the NRF in the 5G Core, the CMG supports the discovery of services by receiving a discovery request from a Network Function (NF) instance, and providing details of the discovered NF instances to the NRF. It maintains the NF profile of the available NF instances in the network and their supported services.

**NSSF**

As the NSSF in the 5G Core, the CMG selects the appropriate set of network slices from the available set of instances serving the UE and determines the appropriate AMF(s) to serve the UE for that set of network slices. This can be pre-configured or presented as a list of candidate AMF(s) through NRF query.

**Mobile Application Assurance**

Nokia Mobile Application Assurance (AA) capabilities on the CMG deliver a range of high-touch packet processing functions. These may be deployed within the PGW/UPF as integrated Application Detection and Control (ADC), policy and charging enforcement, or in the SSG as a stand-alone 3GPP traffic detection function (TDF) along with other specialized SSG functions.

Nokia Mobile AA provides Layer 4 to Layer 7 packet inspection, classification, control and charging capabilities for advanced packet processing and service intelligence in addition to traffic optimization, dynamic congestion control, and Layer 7 stateful
firewall. AA provides classification of flows into applications and app-groups, in addition to using machine learning heuristics to classify flow attribute metadata for all flows, including encrypted traffic. When Mobile AA is integrated within the CMG PGW or UPF PCEF, both enforcement and AA capabilities are offered from a single subscriber policy charging and control (PCC) point. It provides seamless coupling and unification of PCC between both the bearer and application layers.

**SSG**

The CMG also supports an SSG function (Figure 3), which is located on the CSP SGi-LAN interface and provides service classification and enhanced traffic steering features that optimize the mobile end-user experience and generate new service revenue opportunities. In addition to TDF, it also supports Layer 7 charging, TCP-optimization, multi-path TCP hybrid-access gateway, RAN congestion detection and control, carrier-grade Network Address Translation, firewall- and policy-driven traffic steering and service chaining. The SSG enables CMG value-added use cases to be deployed as a stand-alone function for use in conjunction with existing SGW/PGW/UPF functions. This frees up the SGW/PGW/UPF processing resources for bearer management and packet forwarding.

In Nokia packet core networks, the CMG can support both SGW/PGW/UPF and SSG functions in the same instance.

Figure 3. Cloud Mobile Gateway as an SSG providing enhanced IP services on the SGi-LAN interface
Ordering information
The CMG is ordered through application subscriber licenses (ASLs) based on the required network functions and quantity of subscriber services per instance. For ordering questions, contact your Nokia sales representative.

Technical specifications

Standards and protocols
The CMG supports the mobile gateway function message types and procedures defined in the 3GPP Release 13 December 2016 versions of most specifications. It also supports the message types and procedures defined in 3GPP Release 15 March 2018 for the supported 5G Core network functions:

- TS 23.060,
- TS 23.203,
- TS 23.234,
- TS 23.401,
- TS 23.402,
- TS 23.501,
- TS 23.502,
- TS 23.503,
- TS 24.302,
- TS 29.060,
- TS 29.212,
- TS 29.244,
- TS 29.273,
- TS 29.274,
- TS 29.275,
- TS 29.281,
- TS 32.251,
- TS 32.295,
- TS 32.297,
- TS 32.298,
- TS 32.299,
- TS 32.102,
- TS 33.106,
- TS 33.107,
- TS 33.108,
- TS 33.402,
- TS 33.102,
- TS 33.402,
- TS 33.402,
- TS 33.402,
- TS 33.402,
- TS 33.402,

NFV infrastructure requirements
The CMG is verified and certified to operate on a diverse set of open NFVI operating environments and platforms that is continuously being expanded. Contact your Nokia Sales representative for more information.

Learn more