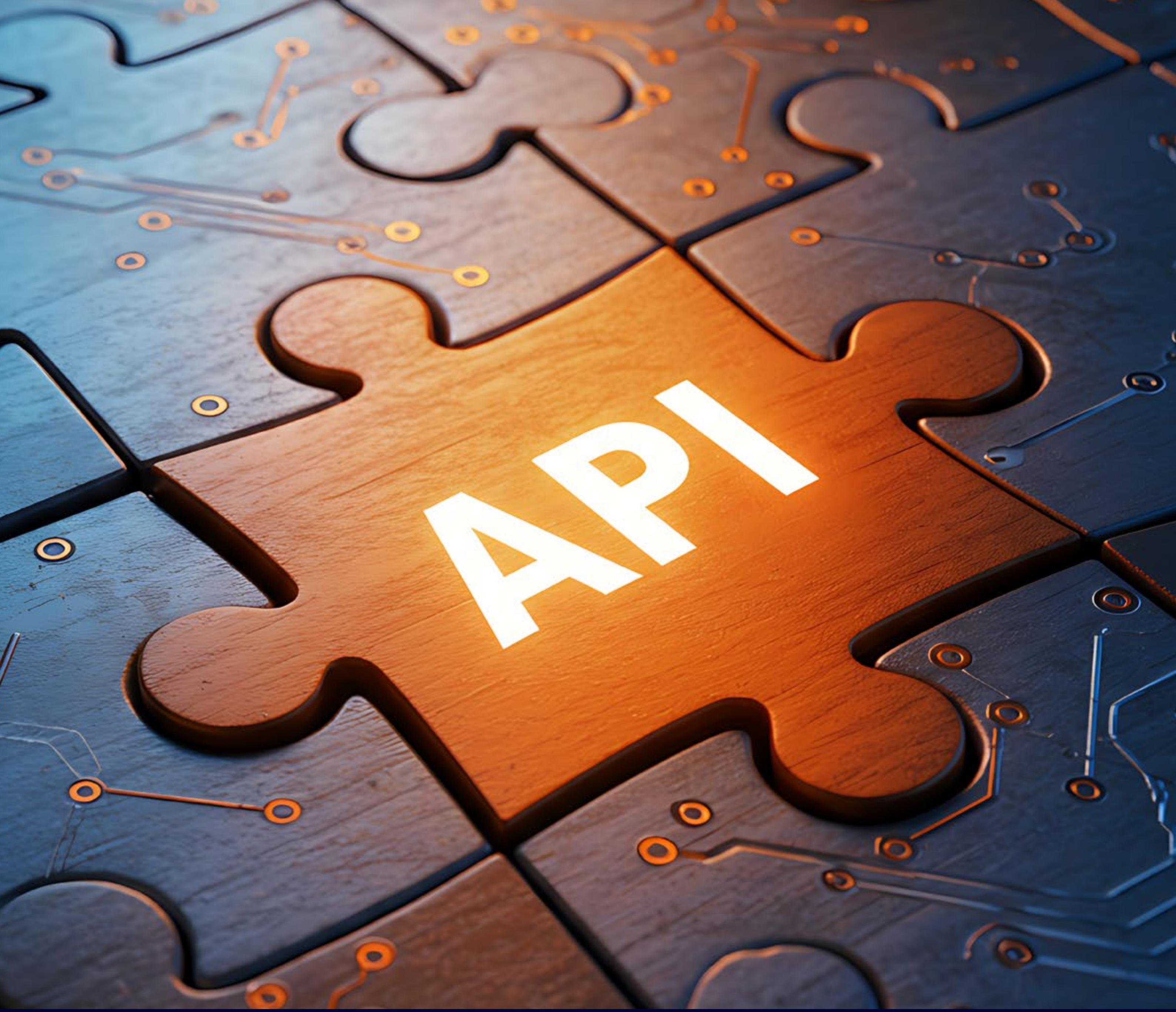


Why Open Gateway/CAMARA Isn't Plug-and-Play

WHITE PAPER

enea.com

Table of Contents

Navigation Instructions:

- ***Click on any chapter title*** *to jump directly to that section.*
- ***Click the Enea logo*** *in the bottom-left corner of any page to return to this overview.*
- **Click enea.com** *in the bottom-right corner to visit our website.*

01. Executive Summary 2

02. The API Exposure Business Opportunity 3

03. CAMARA API Integration Challenges 4

04. The Middleware Solution 9

05. Strategic Directions for Operators 12

06. Our Middleware: The Enea API Composition Engine 13

Appendix A

The Vision of Open Gateway and CAMARA 17

Appendix B

Questions You Should Ask Yourself and Your Team 19

CHAPTER 01

Executive Summary

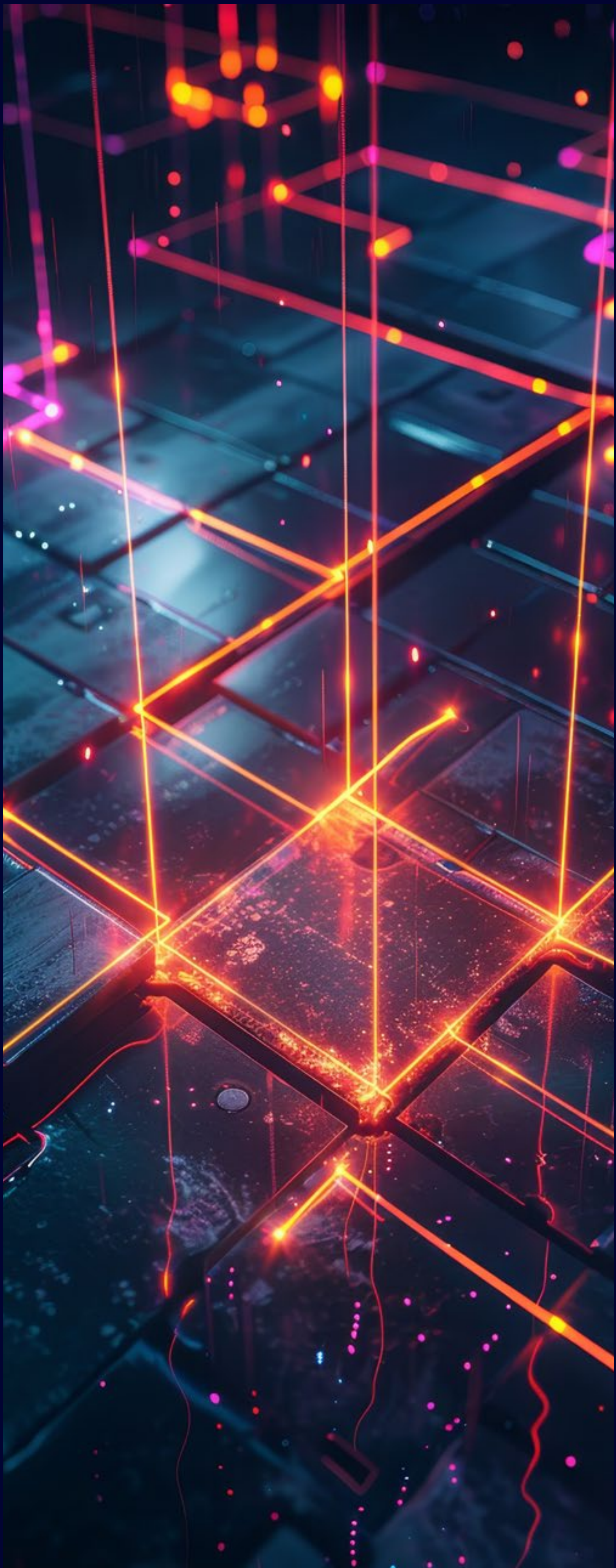
Despite global efforts to harmonize and standardize telecom APIs, CAMARA may not be as plug-and-play for mobile operators as they would like it to be.

The GSMA Open Gateway initiative and CAMARA APIs aim to simplify access to mobile network capabilities through standardized APIs, enabling enterprises and developers to build consistent, scalable services. While the initiative promotes a "plug-and-play" vision, the reality for mobile operators is far more complex.

This white paper explores why Open Gateway and CAMARA APIs are not plug-and-play from an operator's perspective. It highlights key challenges such as architectural diversity, fragmented backend systems, regulatory constraints, and inconsistent onboarding and commercial models. These factors lead to significant variation in API implementation, even when standards exist.

To bridge the gap between vision and execution, operators need robust middleware solutions. These platforms can harmonize data across silos, streamline integration with legacy and next-generation networks, and support critical features such as version control, high availability, authentication, and observability.

The paper outlines strategic options for operators—from building in-house platforms to utilizing middleware as a balanced path forward. Operators that embrace middleware can accelerate API exposure, reduce development overhead, and remain competitive in a rapidly evolving digital services landscape.



The API Exposure Business Opportunity

The global mobile operator market, once characterized by rapid growth, has now entered a saturation phase with single-digit growth rates.

A blog by Don Alusha from ABI Research, titled ***5G Innovation Maturity Strategies for CSPs: Seizing High-Risk, Long-Term Growth in the Telecom Industry,*** highlights these challenges:

- Consumer-centric business accounts for 75-80% of CSP revenues.
- Subscriber growth is slowing with price pressure, leading to stagnating revenues.
- 5G presents opportunities for new revenue streams, including data exposure, network slicing, private networks, and IoT.

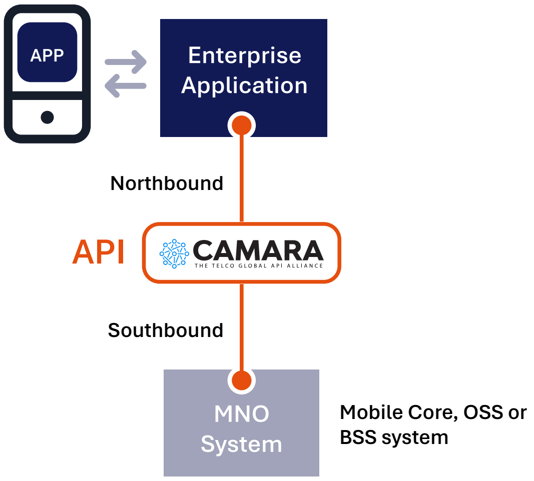
Read ABI Research's blog post

EXPLORE

Among these opportunities, data exposure stands out as a great opportunity for mobile operators. By leveraging their vast network assets and data—while maintaining strict privacy protections—operators can unlock new revenue streams and drive innovation.

The core objective of this evolving ecosystem is to empower enterprises to deliver greater value to their users through secure and seamless digital experiences. Mobile operators play a key role in this landscape, as they are widely regarded as trusted entities by end users.

The GSMA Open Gateway initiative and CAMARA APIs, introduced in February 2020, aim to standardize access to these capabilities. By providing interoperable APIs across operators, they enable both external developers, enterprises and operator in-house teams to build applications more efficiently.



About This White Paper

This white paper examines the practical realities of implementing Open Gateway and CAMARA from a mobile operator's perspective. While these APIs sometimes are considered to be a "plug-and-play" experience, the reality of southbound integration with core networks and OSS/BSS systems presents significant challenges. We highlight the need for middleware solutions to bridge this gap and enable more efficient adoption.

If you are not yet familiar with CAMARA, we recommend reading Appendix A: The Vision of Open Gateway and CAMARA at the end of this document before proceeding.

CHAPTER 03

CAMARA API Integration Challenges

For software developers and enterprises using CAMARA APIs on the northbound side, the experience often feels like plug-and-play.

This perception stems from the developer-focused design:

- **Standardized RESTful APIs:** Familiar and easy to implement for modern web developers.
- **Abstraction of Complexity:** Developers interact with clean interfaces without dealing with underlying network intricacies.
- **Cross-Operator Consistency:** A single integration works across multiple operators.
- **Open-Source Tools:** Collaborative resources make adoption more straightforward.
- **Aggregators:** Provide immediate operator access for enterprises and developers globally.

However, for mobile operators, southbound integration—connecting APIs to the core network, OSS, and BSS systems—is anything but simple.

The Southbound Integration Challenge

Southbound integration requires significant effort to align APIs with complex telecom infrastructures.

1: System Complexity

Telecom networks feature specialized architectures and diverse components (e.g., EPC, 5GC, OSS, BSS).

2: Siloed Data Sources

CAMARA APIs often require data from multiple systems, necessitating harmonization.

3: Customization Needs

To fulfill CAMARA API requests, operators may need to implement additional logic that performs lookups across multiple data sources.

4: Latency and Security

Ensuring compliance and maintaining performance SLAs add layers of complexity.

5: Legacy Systems

Many operators rely on outdated systems that require require specialized integration through legacy interfaces to avoid the complexity and cost of upgrading to support modern APIs.

6: Maintenance and Flexibility

Sustaining integrations over time demands robust, adaptable solutions.

Key Business and Operational Demands to Consider

From an outside-in perspective, enterprises require a secure, consistent API service that enables them to deliver a uniform experience to all consumers. This leads to several critical requirements.

Uniformity of APIs Across Operators

Enterprises need standardized APIs across different mobile operators to ensure seamless integration and avoid fragmentation in their services.

Consistent Customer Interaction Across Devices and Networks (4G & 5G)

- APIs must provide a seamless experience for consumers, whether they are on 4G or 5G networks.
- API responses should remain uniform regardless of the subscriber's network or device type.

Sustainable and Future-Proof API Services

- APIs must evolve rapidly to keep pace with changing user behavior and enterprise demands.
- New API versions should be introduced without disrupting existing integrations.
- Operators need mechanisms to track, manage, and maintain multiple API versions.

High Availability and Reliability

- APIs must meet stringent uptime requirements (e.g., 99.999% availability) to support critical services such as banking authentication (e.g., number verification for OTP-based logins).
- Frequent or prolonged outages could damage enterprise trust and negatively impact the customer experience.
- Operators must ensure reliability, redundancy, and rapid fault resolution.

Agility in Responding to Market Demands

- Enterprises operate on fast-paced development cycles, often launching new services within 6 to 12 months.
- They expect their operator partners to evolve just as quickly—or faster.
- Traditional operator turnaround times for launching market-facing initiatives are often too slow to meet these expectations.

Remember!
It's not the BIG that eats the SMALL.
It's the FAST that eats the SLOW!

Security and Trust

- Mobile operators are generally perceived as trusted service providers.
- APIs must inherently safeguard consumer privacy and prevent misuse.
- Any instance of data theft could seriously damage the operator's brand and must be proactively prevented.
- Enterprises need assurances that operator APIs are secure and not vulnerable to spoofing or unauthorized access.
- Operators must also protect their API infrastructure from DDoS attacks and other security threats to prevent service disruptions.

Critical Considerations for Reliable API Exposure Services

Currently, most operator-driven use cases focus on exposing core network data for services such as SIM swap detection, number verification, and quality-of-service on demand (as promoted by GSMA).

Even for these relatively straightforward services, the necessary data is often scattered across multiple systems and organizational units within a mobile operator.

As CAMARA API innovations grow in complexity, cross-silo integrations will become essential to ensure seamless data access and interoperability across different operator systems.

Challenges With Cross-Silo Integrations

Operator data assets are distributed across multiple operational silos, including:

- Core networks
- Business systems
- Customer care systems

Seamless integration across these silos is critical for delivering a cohesive, efficient, and reliable API service. Note that it is not always about technology, but also about organizational ownership.

Challenges in 4G and 5G Integration

Operators have leveraged off-the-shelf NEF (Network Exposure Function) solutions for 5G, but there is no equivalent standardized solution for exposing 4G core network data.

Key limitations and challenges include:

- The NEF solutions from core network vendors only expose predefined 3GPP-specified endpoints.
- Custom expansions to NEF often require alignment with vendor roadmaps, creating dependency risks.
- Since an NEF may be limited to HTTP/2 and REST interfaces, MNOs must develop their own exposure functions for pre-5G networks and legacy systems, supporting a variety of protocols such as Diameter, RADIUS, and SS7.
- Providing 4G and 5G data via a unified API remains a significant challenge, requiring integration across multiple silos.

Ensuring Sustainability and Reliability

Operators must commit to API-related SLAs to ensure consistent service delivery. Robust throttling and load control mechanisms—such as caching—are essential to manage API traffic effectively, preventing latency issues and avoiding overload of core network systems.

They also need reliable CDR and statistics capabilities to ensure accurate usage tracking and prevent revenue leakage.

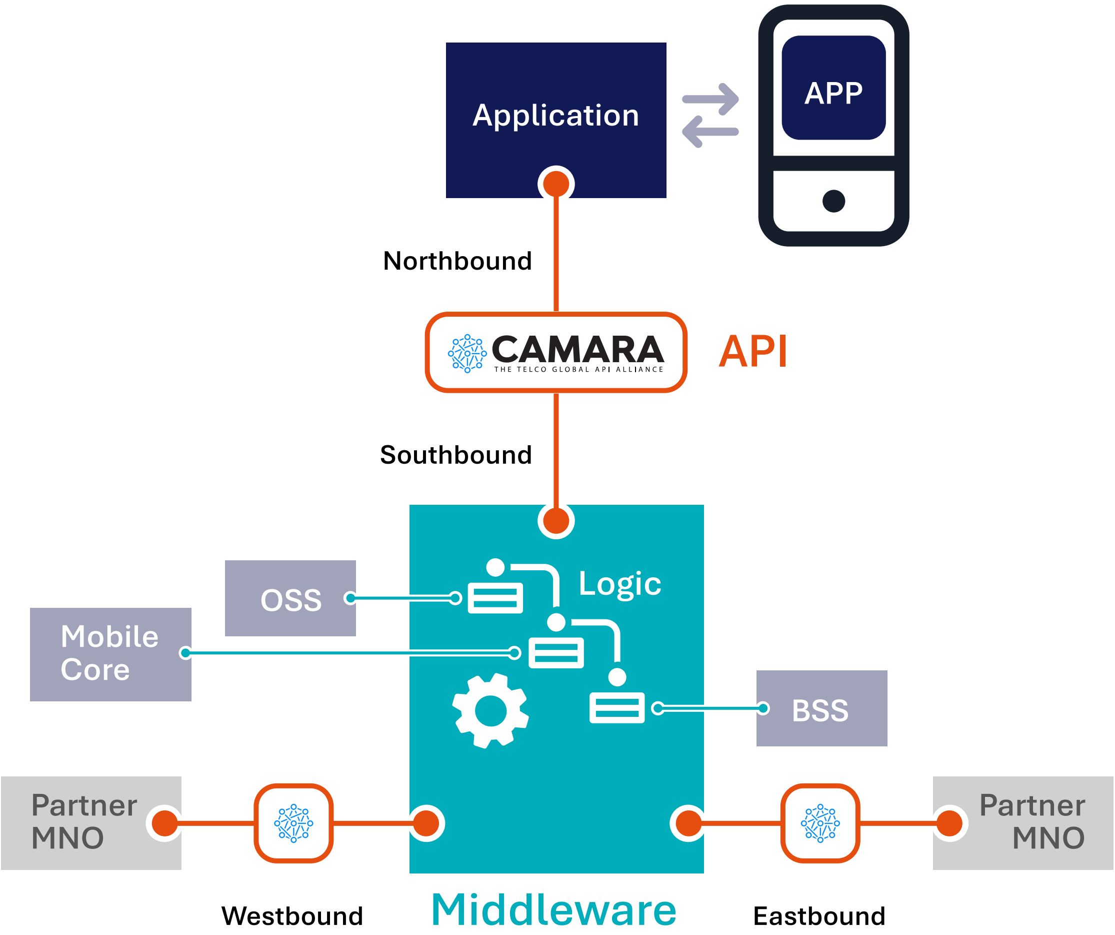
Security Considerations

Ensuring secure API access requires robust authentication mechanisms, such as API keys, to verify and control usage. Additionally, strong authentication and validation mechanisms help prevent unauthorized access, ensuring the integrity and confidentiality of exposed APIs.

CHAPTER 04

The Middleware Solution

A middleware solution—in the form of an abstraction layer, platform, or gateway—is essential for bridging these gaps.



A middleware solution provides standardized CAMARA API interfaces while managing the complexities of south-bound integration.

By harmonizing data across silos, it ensures seamless and secure access to operator assets. Additionally, it optimizes performance through caching, protocol conversion, and configurable logic while handling critical functions such as authentication, authorization, and CDR generation for billing.

To support operational and business needs, it includes audit capabilities, rate limiting for per-use business models, and robust Operations, Administration, and Maintenance (OAM) features. High availability is ensured through a robust design and geographical redundancy, while observability and troubleshooting tools enable proactive monitoring and issue resolution.

Bridging the Gap: Technical Aspects of a Middleware

Middleware solutions can bridge the gap effectively through features such as:

- **Complexity Abstraction:** Enables data retrieval from multiple underlying systems, with the flexibility to incorporate additional logic as required.
- **Protocol Flexibility:** Adapters that bridge standardized CAMARA APIs with legacy OSS/BSS interfaces. While APIs are exposed over HTTP/REST, backend integration can rely on legacy interfaces, with the flexibility to extend to gRPC as needed.
- **Data Normalization:** Converting formats, enriching data, and aligning models across systems.
- **Caching:** Distributed strategies to reduce latency and optimize performance.
- **Security Management:** OAuth 2.0, token-based security, and role-based access controls.
- **Scalability:** Load balancing and overload protection.
- **Billing & Usage Tracking:** Granular metering of API consumption to support accurate chargeback models, enforce usage quotas, and maintain cost transparency.
- **Audit Logging & Access Control:** Robust logging of API interactions, role-based access restrictions, and rate limiting to prevent misuse while ensuring fair and secure resource allocation.
- **Version handling:** Ensure a smooth roll-out of new API versions by implementing robust versioning strategies, backward compatibility, and seamless migration paths for enterprises relying on the APIs.
- **Error Handling:** Centralized logging, error codes, and troubleshooting tools.

Additionally, middleware can support east- and westbound integrations to facilitate collaboration among operators.

Bridging the MNO Organizational Divide

Technical Divide

Data assets such as subscriber profiles, device information, and session data are dispersed across organizational silos. Middleware addresses this by:

- **Seamless Access:** Harmonizing disparate data sources.
- **Efficient Responses:** Managing multi-system queries and caching data for faster processing.
- **Advanced Logic**:
  - Upload of Open API definitions.
  - Package advanced or commonly used logic into manageable plugins.
  - Using internal queries to pre-fetch and cache related data for subsequent requests.
  - Flexible addition of protocol adapters.

Operational Divide

Stakeholders in silos prioritize their systems' performance and security, often resisting external integrations. Middleware can:

- **Balance Stakeholder Concerns:** Ensure secure, SLA-compliant data handling.
- **Minimize Impact:** Reduce load on critical systems with intelligent query management.

CHAPTER 05

Open Gateway/CAMARA:Strategic Directions for Operators

Mobile operators engaging with Open Gateway / CAMARA must make critical strategic decisions regarding their approach to API exposure.

Don't miss Apendix B:

Questions You Should Ask Yourself and Your Team

GO THERE

There are two primary strategic options to select from:

1

In-House Bespoke Development

Building and maintaining an in-house platform provides full control but requires significant resources, expertise, and long-term investment. While it enables the development of unique offerings, responding to new customer requests may be slower compared to competitors leveraging middleware solutions. Middleware allows for faster development by streamlining integration and sharing part of the development effort with others, enabling quicker adaptation to market demands.

2

Middleware Solutions - A Balanced Approach

Middleware offers a scalable and flexible alternative, allowing operators to streamline API exposure without the heavy resource burden of fully bespoke development or the constraints of aggregator reliance. By leveraging middleware, operators can allocate their development resources more effectively, focusing on creating truly unique features that enhance competitiveness while maintaining efficiency and agility.

Our Middleware Solution: Enea API Composition Engine

The Enea API Composition Engine (ACE) is a powerful new solution built on Enea's highly scalable and reliable telecom framework, trusted by leading service providers worldwide.

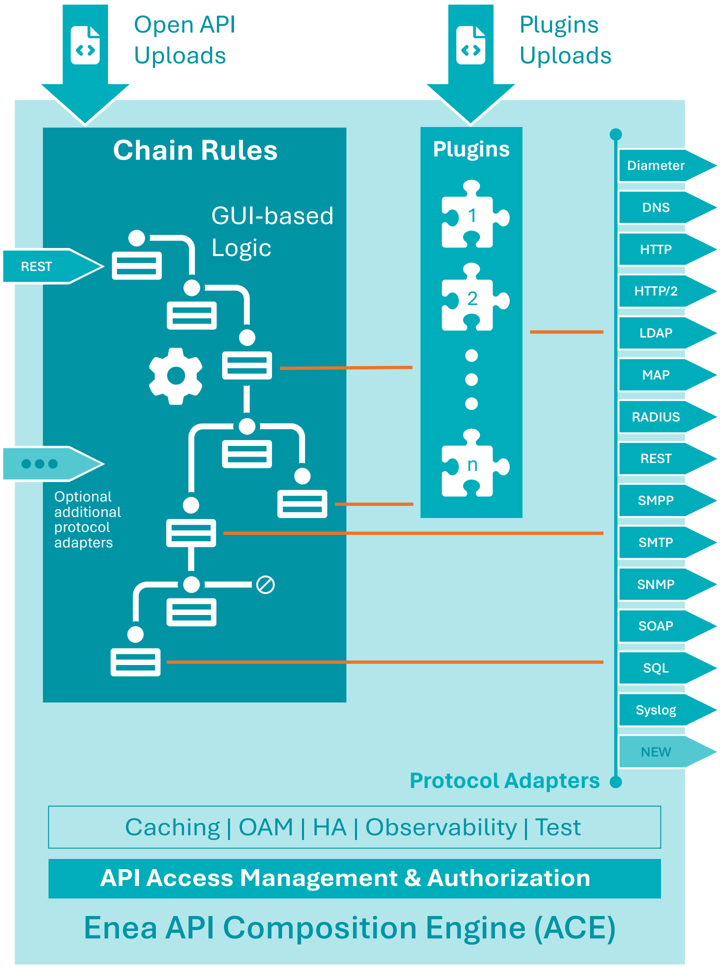
Built for Flexibility

Enea ACE enables operators to quickly adapt to evolving requirements without the need for extensive development skills. Its GUI-based configurable logic allows for intuitive use case implementation, where:

- New use cases can easily be added to a system by GUI configuration.
- A rule-set can be configured to fetch data from multiple sources and based on the result apply mobile operator-defined logic.
- Rule-sets can interact with other rule-sets (chained rules) and plugins.

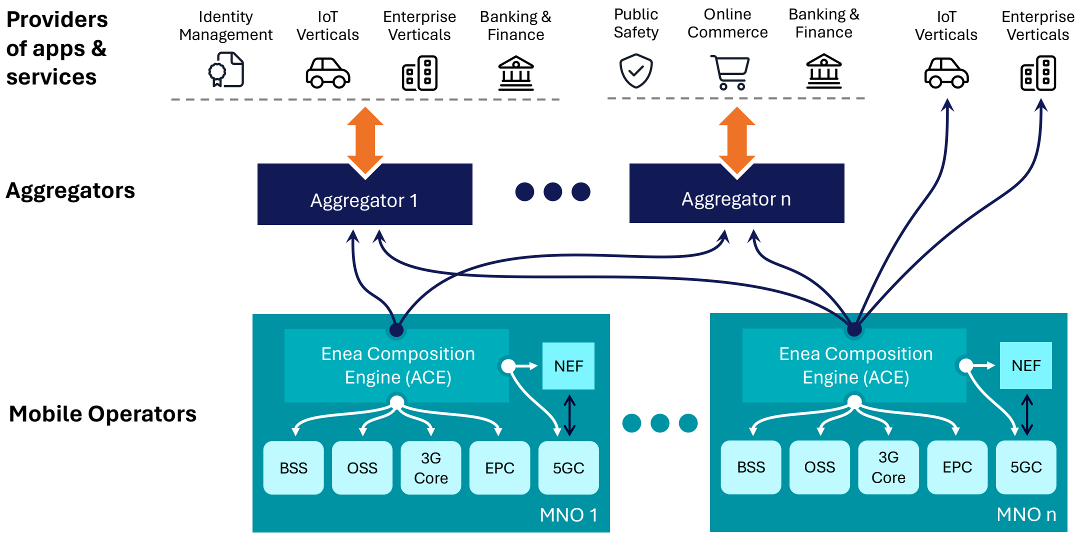
This modular approach, combined with a rich selection of protocol adapters, ensures seamless integration with existing systems. Operators can modify deployment logic through configuration rather than developing code, accelerating time to market.

Our flexible architecture also enables the development and integration of new protocol adapters as needed. Furthermore, service providers can upload Open API-based specifications—such as CAMARA APIs—directly into the rules engine, providing an ideal starting point for further logic development.



For advanced or common use cases, Enea's software engineers can extend functionality by developing software plugins, providing maximum adaptability in an ever-evolving telecom landscape.

Enea ACE in the API Ecosystem



“So, you’re an aggregator?”
That’s a question we’re often asked when people try to place Enea in the API exposure ecosystem. The answer is simple: **No, we’re not.**

Aggregators play a distinct role by acting as business and technology intermediaries. They manage commercial relationships between mobile operators and enterprises, route API requests, and often bundle additional services beyond pure API exposure—taking a share of the revenue in the process.

Enea API Composition Engine (ACE) plays a very different role. As a middleware solution, ACE is designed to simplify and streamline southbound integration—the complex task of connecting standardized APIs (like CAMARA) to diverse, siloed, and sometimes legacy backend systems. This need exists regardless of whether a mobile operator exposes APIs directly or relies entirely on aggregators.

Here’s a simplified view of the API exposure ecosystem:

- **Enterprises** – Providers of apps and digital services
  - Deliver services via APIs
  - Often need access to multiple MNOs across markets
- **Aggregators** – Business and integration facilitators
  - Manage contracts with MNOs and enterprises
  - Route requests to the appropriate operator
  - Add services such as security, billing, and analytics
  - Take a share of the API revenue
- **Mobile Operators** – Owners of network capabilities and data
  - Must abstract backend complexity from enterprises
  - May interconnect with partner MNOs
  - Need integration flexibility beyond CAMARA, especially to support 2G/3G/4G and legacy systems that NEF doesn't cover.

This is where Enea ACE excels. It equips mobile operators with the tools to efficiently expose APIs—across all generations of networks—through robust, flexible, and future-proof integration.

Enea ACE - Essential Supporting Capabilities

Beyond logic and flexibility, Enea ACE includes a suite of critical supporting functionalities, which can be extended over time based on customer needs:

- **API Management:** Authentication, CDR generation (billing), audit logging, and rate limiting.
- **API Discovery:** Empowers third-party developers to easily discover and use APIs.
- **Usage Monitoring:** Provides robust tracking to facilitate monetization strategies.
- **Cross-Integration:** Enables seamless integration with other cloud services to create business processes around APIs.
- **Deployment Flexibility:** The solution features a cloud-native architecture that leverages microservices, supporting deployment as VNF or CNF.
- **Caching:** Reduces load on backend systems by storing frequent requests.
- **Operations & Maintenance (OAM):** Robust tools for system administration including version handling of APIs.
- **High Availability (HA):** Geo-redundant architecture for maximum reliability.
- **Observability & Troubleshooting:** Advanced monitoring, testing, and diagnostics.

With its powerful combination of flexibility, scalability, and operational resilience, Enea ACEhelp operators streamline API exposure while ensuring high performance and reliability.

Conclusion

Middleware solutions are indispensable for realizing the potential of Open Gateway / CAMARA APIs. By addressing both technical and operational challenges, they enable mobile operators to unlock new revenue streams efficiently and sustainably.

With deep expertise in integration, AAA, and policy solutions, Enea is uniquely positioned to deliver carrier-grade middleware tailored for API use cases—including those based on CAMARA.

By partnering with Enea, operators can:

- Achieve faster time-to-market at reduced costs.
- Leverage proven integration expertise.
- Maintain control while benefiting from shared development resources.
- Ensure carrier-grade performance, scalability, and reliability.

Note: *Our solution works equally well for your internal APIs*

Contact us today to start your journey towards seamless and scalable API integration.

CONTACT US

About Enea

Enea is a global specialist in advanced telecom and cybersecurity software, with a vision to making the world's communications safer and more efficient. Dedicated to innovation and security, our solutions connect, optimize, and protect communications between people, companies, and connected devices worldwide. We serve 160+ communication service providers across more than 90 countries, supporting over 30% of the world's mobile subscriptions, with billions relying on our software every day.

Headquartered in Stockholm, Sweden, Enea is publicly listed on NASDAQ Stockholm.

To learn more, visit: www.enea.com.

Author

Iftikhar Waheed
Product Management Director, Enea

ENEA

APPENDIX A

The Vision of Open Gateway and CAMARA

The GSMA Open Gateway APIs, developed under the Linux Foundation's CAMARA project, aim to simplify developer access to telecom networks. These APIs provide:

- **Standardization:** Unified interfaces for global operator interoperability.
- **Enhanced Capabilities:** Access to features like quality on demand, location services, identity verification, and edge computing.
- **Open Source:** Collaborative development to foster innovation.
- **Operator Collaboration:** Alignment with real-world network capabilities and business needs.

These APIs transform telecom networks into service enablement platforms by exposing capabilities in an on-demand, secure, and controlled manner. CAMARA APIs' abstraction from network to service APIs ensures they are user-friendly, respect data privacy, and facilitate application-to-network integration. Additionally, their availability across telco networks and countries accelerates technology development and commercial adoption, reduces implementation efforts, and supports application portability.

As of January 2025, CAMARA APIs include features such as device status checks, SIM Swap, Know Your Customer (KYC) processes, location verification, and network quality management. While these northbound APIs are designed for simplicity and consistency, southbound integration poses significant challenges.

Below is an overview of the current (January 2025) CAMARA APIs:

API name	API product family	Description of use
Device Status device-reachability-status device-roaming-status	Subcriber Identity	Checks connectivity status for user equipment, including roaming status, country, and connection status. Can notify of status changes in subscription mode.
KYC Fill-in (Know Your Customer)	Subscriber Identity	Allows requesting and receiving verified user information from mobile operator KYC records. Useful for one-click checkout, form auto-fill, and verifying user details.
KYC Match (Know Your Customer)	Subscriber Identity	Validates user-provided information against verified mobile operator records to prevent fraud and ensure KYC compliance.
Number Verification[1]	Subscriber Identity	Verifies that the provided mobile number matches the one used in the device for authentication purposes.
One Time Password (SMS)[1]	Subscriber Identity	Delivers and validates a short-lived one-time password via SMS for proof of phone number possession and authentication.
SIM Swap[1]	Subscriber Identity	Checks when a SIM card associated with a mobile number was last changed, which is useful for fraud prevention.
Device Location Verification[1]	Location	Checks if a mobile device is near a given location within a specified accuracy range.
Device Geofencing Subscription	Location	Enables subscriptions to receive notifications when devices enter or exit specified areas.
Location Retrieval	Location	Retrieves a device's location based on current network conditions. For people-to-people payment, logistics etc.
Connectivity Insights	Network Quality / Optimisation	Allows an application developer to query the likelihood that networking requirements can be met for a given end-user session, which is useful for optimizing user experience.
Mobile Quality on Demand	Network Quality / Optimisation	Controls mobile connectivity service quality for applications like 5G online gaming. The app can request stable latency (reduced jitter) and minimum throughput.
Home Devices Quality On Demand (QoD)	Network Quality / Optimisation	Enables application developers to control the (Wi-Fi) network configuration of their End Users devices when they are connected through the Wi-Fi access point provided by a telco fixed line. Developers can request to change, on demand, the desired QoS behaviour.
Simple Edge Discovery[1]	MEC (Mobile Edge Cloud)	Allows applications to discover the nearest Edge-Cloud zone for connection.
Traffic Influence	MEC (Mobile Edge Cloud)	Provides intent-based interface to request optimal latency for edge-deployed services. (Optimal routing in terms of latency).
Carrier Billing	Payments & Charging	Allows an online merchant to enable the purchase of third-party digital goods and to request payment against the user's Mobile Operator billing system.

1) It should be noted that only Device location verification, Number verification, One-Time Password, Simple Edge Discovery, and SIM Swap are considered stable at this time (January 2025). For the latest information about the CAMARA APIs, please refer to the CAMARA project site at Github.

APPENDIX B

Questions You Should Ask Yourself and Your Team

These are some of the questions mobile operators should ask themselves when choosing their long-term strategy for Open Gateway / CAMARA (and other API initiatives).

1. Strategic Positioning & Control

- Do we want full control over our API exposure strategy, or are we willing to depend on third-party aggregators?
- What safeguards will prevent aggregators from commoditizing our network APIs?
- How will our choice impact our competitive differentiation in the market?
- What level of customization and flexibility do we require for our APIs?
- Will proprietary API extensions (beyond CAMARA standards) create competitive advantages or fragment the ecosystem?

2. Resource Investment & Operational Impact

- Do we have the internal expertise and resources to build and maintain an in-house API exposure platform?
- Can we justify the opportunity cost of dedicating engineering resources to bespoke API development vs. core network operations?
- What are the long-term costs and operational complexities of managing API infrastructure internally?
- How can we ensure smooth integration across our existing network, business, and customer care systems?
- How will we resolve conflicting priorities between network, IT, and business units regarding API ownership and revenue sharing?
- Do we have cross-functional teams capable of managing API lifecycle operations (development, marketing, support)?

3. Security and Compliance

- How do we manage security risks such as unauthorized API access, DDoS attacks, and data privacy concerns?
- How will we maintain API SLAs during network outages or cyberattacks?
- How will we audit third-party aggregators’ use of sensitive network data?
- What mechanisms ensure GDPR/CCPA compliance when exposing cross-silo data via APIs (e.g., device location sharing)?

- Are our API terms of service compatible with regional data sovereignty laws such as the EU's Data Act?
- How will we handle liability for API-driven fraud (e.g., SIM swap failures)?

4. Monetization & Revenue Sharing

- Should we adopt GSMA's proposed models (time-based, tiered access) or develop operator-specific monetization strategies?
- How will we avoid price wars with other operators offering identical CAMARA APIs?
- What monetization opportunities do we foresee with API exposure?
- Are we willing to share revenue with aggregators, or do we prefer to retain full ownership of API-related revenues?
- How do we balance cost efficiency with revenue potential in our API strategy?
- What contingency plans exist if a key aggregator changes pricing/terms?

5. Technical Challenges & Future-Proofing

- How do we ensure seamless API versioning and backward compatibility?
- Can we integrate both 4G and 5G core network data into a unified API offering?
- Can our OSS/BSS systems support real-time API orchestration across siloed data sources (core networks, CRM, billing)?
- How will we handle API version conflicts between CAMARA updates and legacy infrastructure?
- Can our architecture support AI-driven APIs requiring real-time data from 5G core, IoT platforms, and edge systems?

6. Agility & Market Responsiveness

- How quickly can we roll out new APIs and adapt to changing enterprise needs?
- What internal bottlenecks may slow down our ability to innovate with APIs?
- How do we benchmark our API exposure speed and agility against industry best practices?
- Do we have tools to simplify API testing/onboarding (e.g., sandbox environments, SDKs)?

7. Reliability & Service Quality

- What SLAs should we commit to for API uptime and performance?
- How do we handle API load balancing, throttling, and failover mechanisms?
- How can we prevent service disruptions that could damage enterprise trust in our APIs?