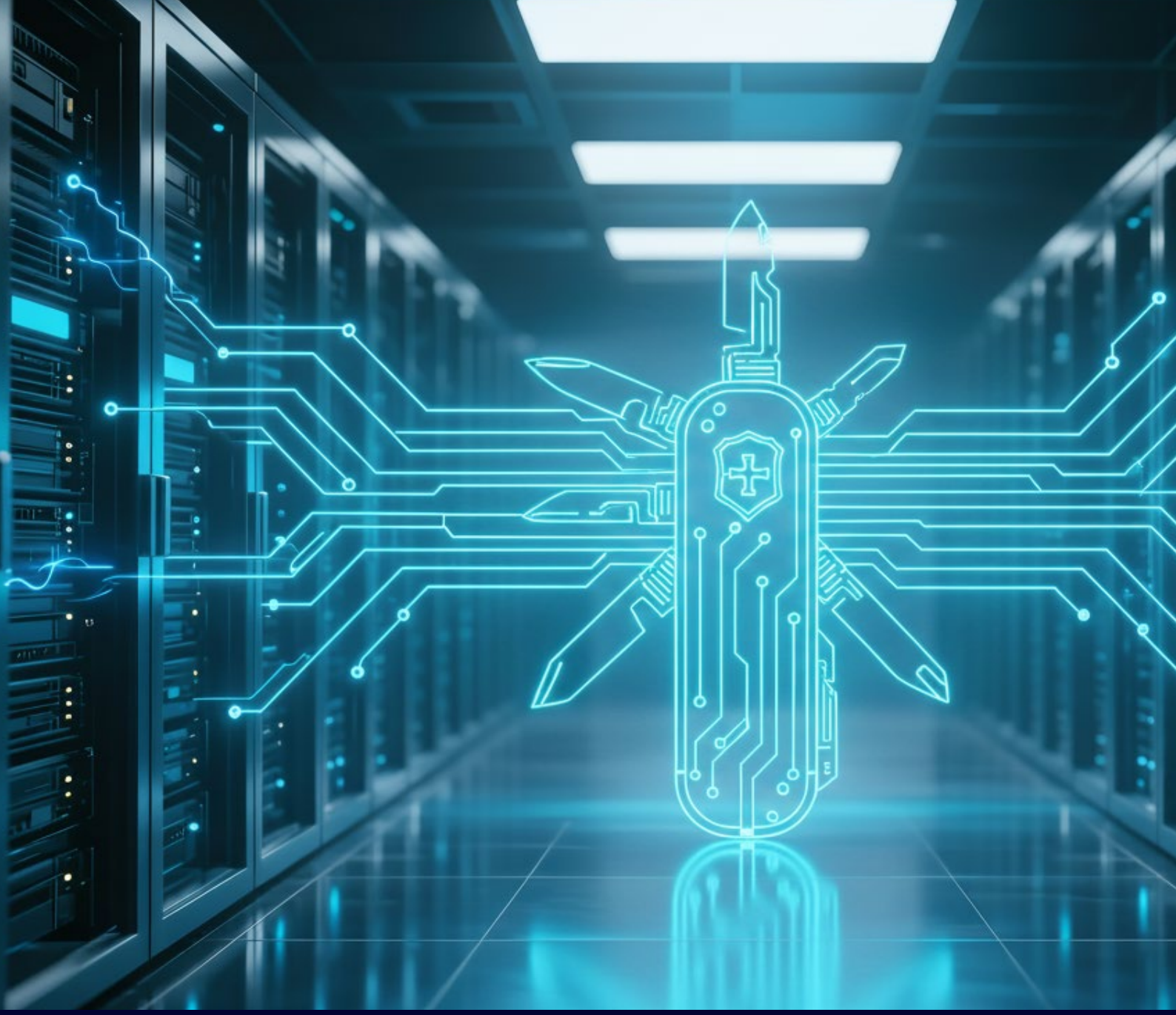


THE PROGRAMMABLE CORE

Why Intelligent AAA is the Swiss Army Knife of Telecom

Real-world CSP case studies demonstrating how the Enea AAA Server transforms operational complexity into scalable, automated, and revenue-generating services.

ENEA

Interactive Navigation

Click on the chapter of interest.

ENEA Click on the logo at the bottom of the pages to go back here.

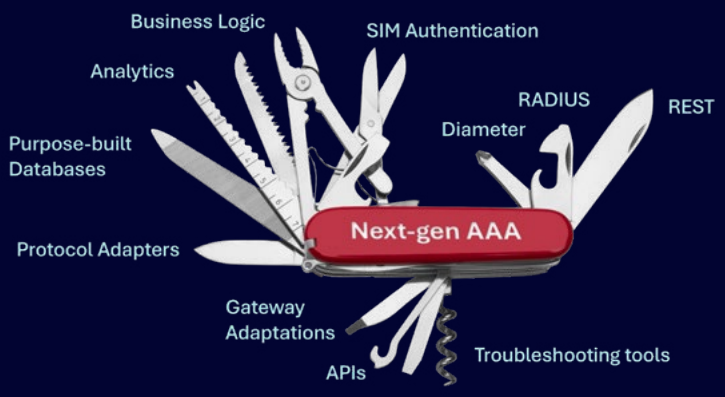
Contents

INTRO

About This White Paper

For decades, the AAA (Authentication, Authorization, and Accounting) server was viewed primarily as a static gatekeeper—a necessary but rigid component of the mobile core responsible for basic network access. However, as Tier 1 operators navigate the complexities of 5G Standalone (SA) transitions, massive IoT scaling, and specialized enterprise services, the role of the AAA has undergone a fundamental transformation.

Modern network architectures require more than just a "yes or no" to an access request. They require a Programmable Core—an intelligent mediation layer capable of executing sophisticated business logic at the signaling edge. This white paper explores why the Next-gen AAA Server has emerged as the "Swiss Army Knife" of telecommunications.



Beyond traditional AAA functions, this platform serves as a versatile multi-tool for the modern CSP, providing:

- **Intelligent Logic Mediation:** Decoupling complex business logic from rigid core elements to enable rapid service innovation.
- **Multi-generation Interworking:** Bridging the gap between legacy Diameter-based systems and next-generation 5G HTTP/2 service-based architectures.
- **Policy-Driven Orchestration:** Powering advanced use cases such as multi-tenant Private APNs, automated VPN provisioning, and high-precision IP Address Management (IPAM).

Through a series of anonymized **real-world case studies from Tier 1 operators** across North America, Europe, Asia and Latin America, we demonstrate how the Enea AAA Server solves the 'long tail' of connectivity challenges—transforming operational complexity into scalable, automated, and revenue-generating services.

While this document focuses on specialized, high-value use cases, operators beginning their modernization journey may also wish to consult our foundational guide, ***A Strategic Guide to AAA Replacement***. That paper provides a comprehensive framework for migrating away from legacy infrastructure, ensuring a risk-free transition to a cloud-native, future-proof AAA architecture.

CSP A – TIER 1 NORTH AMERICAN MOBILE OPERATOR

Intelligent AAA Proxy for Public and Private IoT

CSP A, a major North American Tier 1 mobile operator, maintains a robust IoT connectivity business serving both direct enterprise customers and IoT-focused Mobile Virtual Network Operators (MVNOs). To scale this business cost-effectively, CSP A required a flexible architecture to manage diverse authentication requirements across its Public and Private IoT ecosystems.

THE CHALLENGE

Overcoming Architectural Rigidity

CSP A's IoT operations are highly complex. While its core Public IoT services utilize the Cisco Jasper Connectivity Management Platform, the operator must also support multiple MVNO partners with varying technical capabilities. These range from MVNOs hosted on CSP A's Jasper AAA to those maintaining independent, third-party AAA servers.

Key challenges included:

- **Signaling Complexity:** Traffic must be routed using specific Access Point Names (APNs) , or a combination of RADIUS attributes, often with multiple APNs per MVNO.
- **Business Logic Requirements:** The operator needed to inject specific Attribute-Value Pairs (AVPs) from both Jasper and MVNO AAA systems into signaling toward the Packet Gateways (PGW/GGSN).
- **Integration Costs:** Adding unique business logic for every MVNO directly into the Jasper platform was deemed cost-prohibitive and technically inflexible.
- **Security:** CSP A sought to avoid exposing its internal Jasper platform directly to external third-party networks.

THE SOLUTION

Intelligent AAA Proxy

CSP A deployed the Enea AAA Server as a centralized, intelligent AAA proxy. Positioned between the Packet Gateways and the various AAA destinations, the Enea solution provides a powerful business logic engine that decouples the core IoT platform from external MVNO environments.

The system utilizes the Enea AAA Proxy Package, optimized for high-performance RADIUS proxying. It applies custom logic based on the "realm" of incoming messages, allowing administrators to define, modify, or delete flows by matching a combination of RADIUS Attribute-Value Pairs (AVPs).

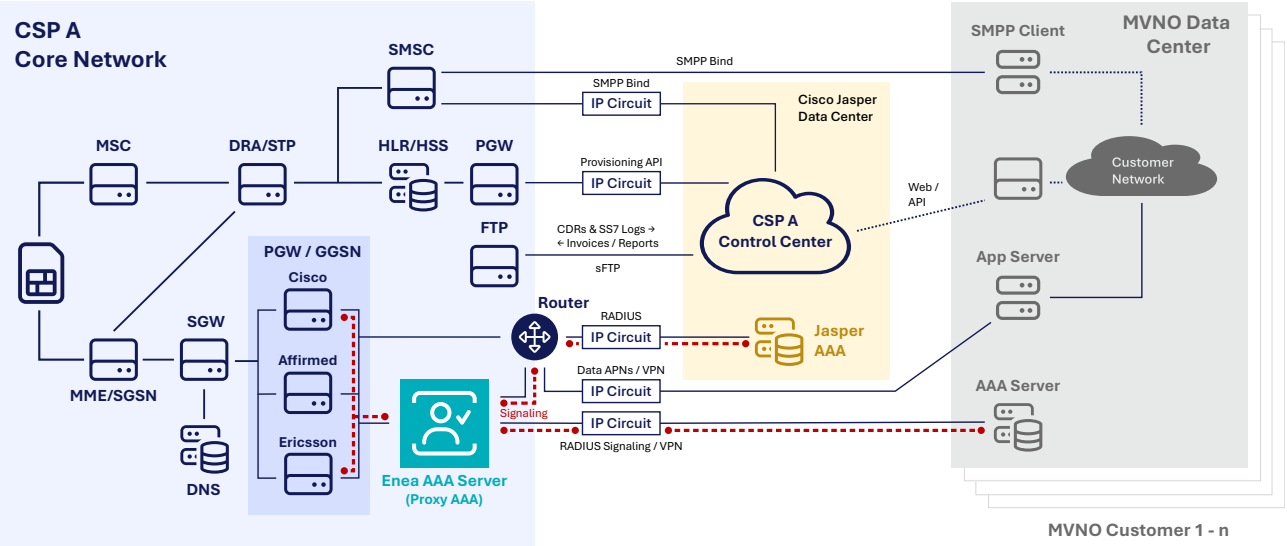
Proxy Package Key Capabilities

The deployment is optimized to reduce node requirements while maximizing throughput.

Core features include:

- **Flexible Mapping:** Advanced proxy-matching from Packet Gateways and to Home AAA servers. Support for proxy-matching that always accept and always reject.
- **Intelligent Load Balancing and Signaling Steering:** Since each Home AAA destination is configured as a Node Group, signaling can be distributed across one or more server nodes using Round-Robin, Failover, Sticky, or Hashed algorithms. The Hashed method steers signaling to a specific AAA node based on a configurable combination of parameters, such as User ID.
- **Server Health Monitoring:** Real-time monitoring of external nodes via Server-Status messages with configurable failover thresholds.
- **Advanced Signaling Support:** Includes Change of Authorization (CoA), Disconnect Messages (DM), and RadSec (RADIUS over TLS) for secure transport.
- **Observability:** RADIUS Copying for accounting audits and comprehensive SNMP counters for all nodes and policy matches.

Deployment Architecture: Public IoT



Enea AAA Server (Proxy AAA)

The IoT Proxy AAA system is deployed across three independent environments to ensure high availability and geo-redundancy:

- **Pre-production:** A two-node system for validation.
- **Production:** Dual-site deployment (Site 1 and Site 2), each featuring a two-node cluster.

CSP A Packet Gateways

The CSP A mobile core utilizes multiple Packet Gateways (PGW/GGSN) to initiate RADIUS requests to the Enea AAA. The Enea AAA then applies sophisticated business logic to determine the appropriate routing destination based on a unique combination of RADIUS attributes within the incoming packets.

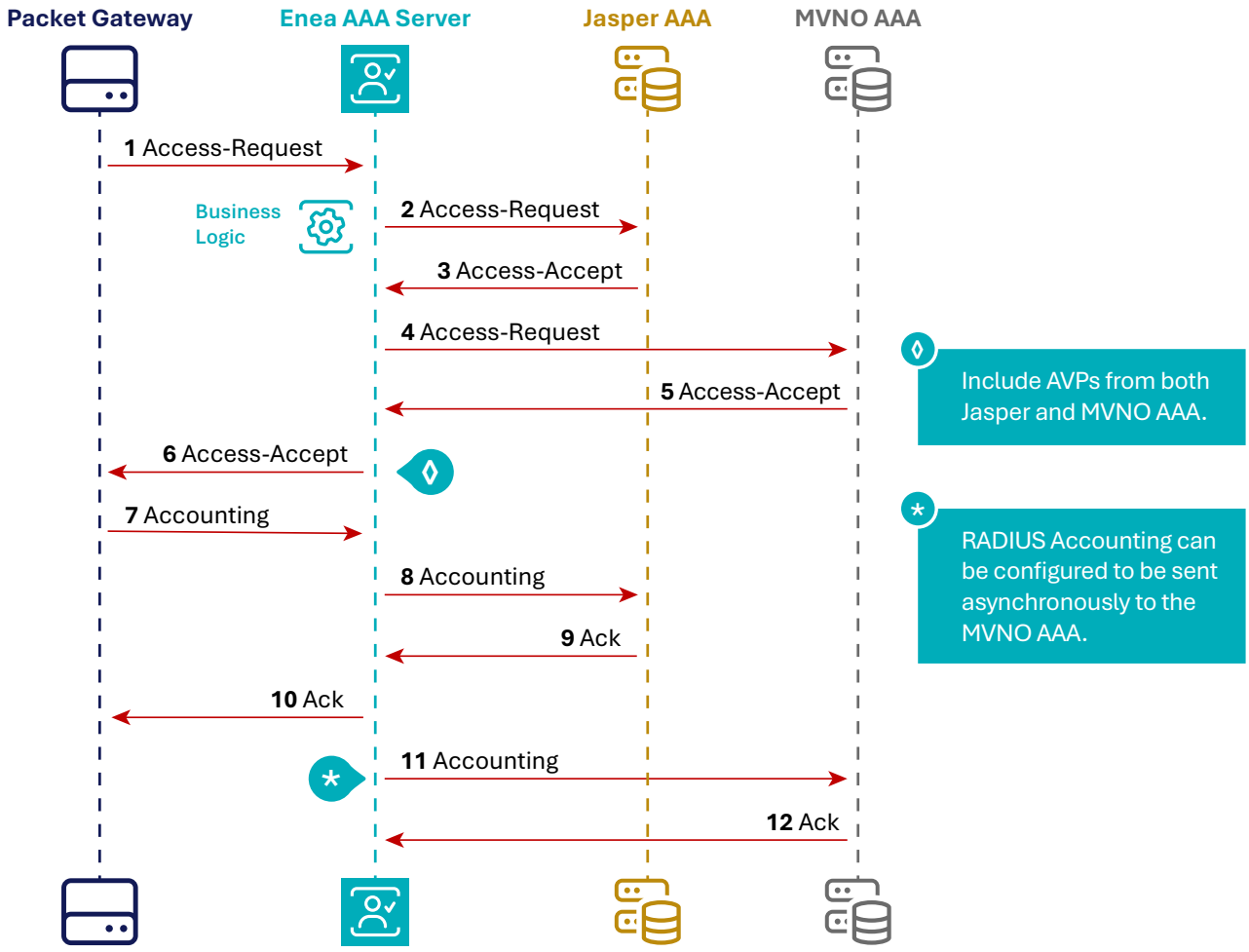
Jasper AAA System

The Jasper AAA system, hosted at the CSP A Control Center, receives RADIUS packets from the Enea AAA, executes internal policy rules, and proxies the requests back to the Enea AAA. Because the User-Name attribute remains identical for both the original Packet Gateway request and the returned Jasper request, the Enea AAA uses secondary unique attributes—such as the Source IP Address—to identify the flow. This allows the Enea AAA to apply the correct logic and successfully proxy the requests to the intended MVNO.

MVNO AAA Systems

In Public IoT scenarios, third-party AAA systems located at each MVNO's data center maintain the primary device account databases. These systems serve as the final authority for authentication and accounting. The Enea AAA acts as the intelligent bridge, proxying all relevant RADIUS signaling to these external systems to complete the session. In a few cases the MVNO has the primary device account database hosted with CSP A (Jasper AAA), and in this case only accounting will be exchanged with the MVNO AAA.

Call Flow for the Public IoT Use Case

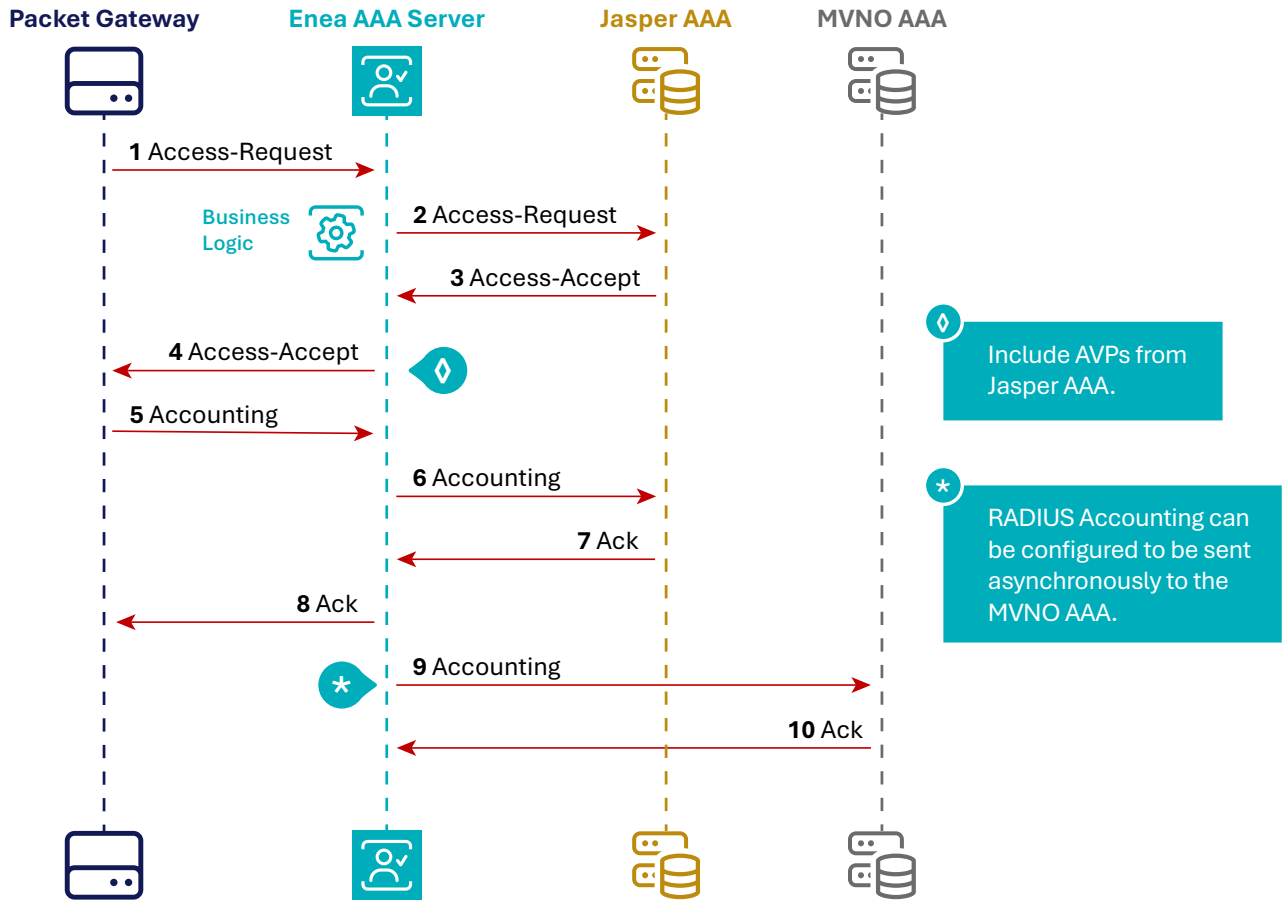


The Enea AAA facilitates a multi-step authentication process to ensure both CSP A and the MVNO approve the session:

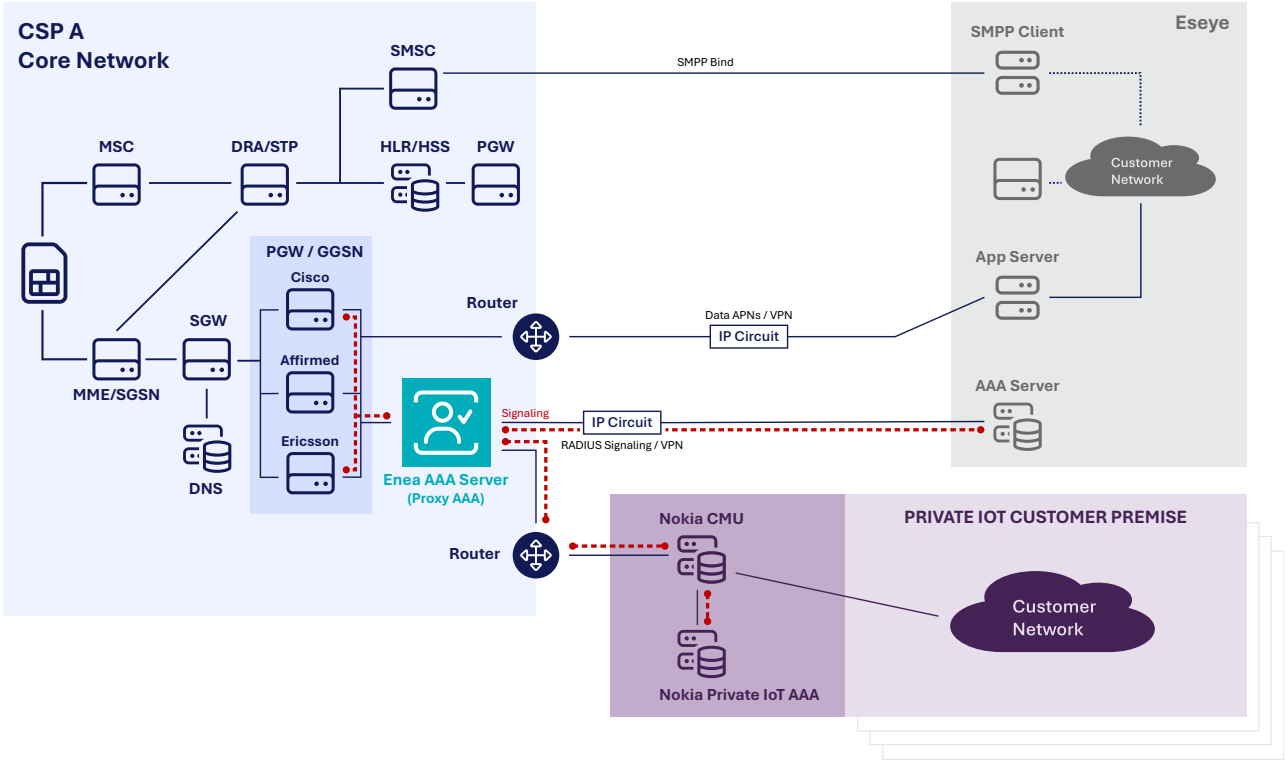
- **Initial Request:** The Packet Gateway sends a RADIUS Access-Request to the Enea AAA (1).
- **Tier 1 Validation:** Enea applies business logic and forwards the request to the Jasper AAA (2).
- **Secondary Proxying:** Upon Jasper's approval (3), the Enea AAA initiates a secondary Access-Request to the MVNO's AAA (4).
- **AVP Enrichment:** If the MVNO approves (5), Enea AAA aggregates the required AVPs from both Jasper AAA and the MVNO AAA, sending a final Access-Accept to the Packet Gateway (6).
- **Fail-Fast Logic:** If Jasper initially rejects the request (3), Enea immediately sends a rejection to the Packet Gateway, bypassing the MVNO and saving network resources.
- **Accounting Logic:** To optimize performance, Enea acknowledges Packet Gateway accounting messages once Jasper confirms receipt (7-10). It then asynchronously forwards accounting data to the MVNO AAA. Note: Since the username remains identical across these legs, Enea uses the Source IP Address as a unique discriminator to apply the correct routing rules for return traffic.

Public IoT Call Flow for MVNO With Accounts in Jasper

CSP A have MVNO partners that utilize the Jasper AAA for holding accounts rather than utilizing their own AAA. Here the call flow is very similar with the exception that RADIUS Access Request messages are not sent to the MVNO AAA.



CSP A – International and Private IoT



In this scenario, the Enea AAA Server leverages the core functionality of the AAA Proxy package to provide high-performance, transparent proxying without the need for additional business logic or AVP additions.

For international IoT connectivity, the Enea AAA manages RADIUS traffic exchange with the Eseye AAA server, while the Nokia Private IoT AAA serves as the destination for Private IoT sessions.

Change of Authorization / Disconnect Message

The Enea AAA supports Change of Authorization (CoA) and Disconnect Messages (DM) initiated by external AAAs. The system intelligently identifies the correct subscriber session by matching the User-Name AVP alongside the Acct-Session-Id, NAS-Identifier, or NAS-IP-Address, ensuring that session termination or profile updates are accurately routed to the originating Packet Gateway.

CSP B - TIER 1 NORTH AMERICAN MOBILE OPERATOR

Intelligent AAA Proxy for APN Selection

The primary objective of this solution, built for a major North American Tier 1 mobile operator, is to facilitate automated Access Point Name (APN) selection by assigning a predefined 4G/5G APN to an authenticating device. This selection is determined by evaluating the attributes within the incoming RADIUS Access-Request received from the Packet Gateway (PGW).

Once the APN Selection process is complete, the Enea AAA Server performs one of two actions based on the subscriber profile:

- **Proxy Authentication:** Forwards the request to an external Home AAA Server (HAAA).
- **Local Authentication:** Validates the session directly against the Enea AAA internal account database.

To ensure consistent billing and session tracking, all RADIUS Accounting-Requests received from the PGW are transparently proxied to the designated external HAAA. In some cases, the Accounting-Request is also copied to another AAA server.

To optimize performance and management, the architecture is divided into two functionally identical AAA proxy systems, each dedicated to a specific subscriber segment:

1. **Consumer:** The AAA system described in more detail in this case study.
2. **Corporate:** A dedicated Enea AAA environment tailored for enterprise-grade IoT and data services, not covered in further detail here.

THE CHALLENGE

Overcoming Inflexible APN Selection

CSP B's existing core systems lacked the necessary flexibility to manage complex APN Selection requirements. The operator required a highly programmable solution capable of executing sophisticated business logic on incoming RADIUS Access-Requests to drive precise APN assignments.

Key requirements for the new solution included:

- **Dynamic Authentication Logic:** The operator required the ability to determine the appropriate handling for each subscriber based on predefined policies. Specifically, the system needed to decide whether a request should be "Always Accepted," proxied to the correct HAAA for external authentication, or authenticated against the solution's local database.
- **Multi-Destination Routing:** The flexibility to proxy accounting messages to one or more HAAA nodes as well ass DPI and billing systems, based on predefined policy rules.

CSP B sought to implement an intelligent mediation layer to bridge the gap between their legacy core routing and the dynamic business logic needed to handle modern APN selection and proxying requirements.

THE SOLUTION

Enea AAA Server as AAA Proxy for APN Selection

To achieve the necessary flexibility and performance, CSP B selected the Enea AAA Server to serve as an intelligent AAA proxy for APN Selection. While many AAA platforms can deliver high transactions per second (TPS) for standard RADIUS signaling, executing advanced business logic for APN selection at scale requires a more sophisticated engine.

Performance and Scalability Requirements

To support the mass-market consumer segment, CSP B defined several high-performance benchmarks:

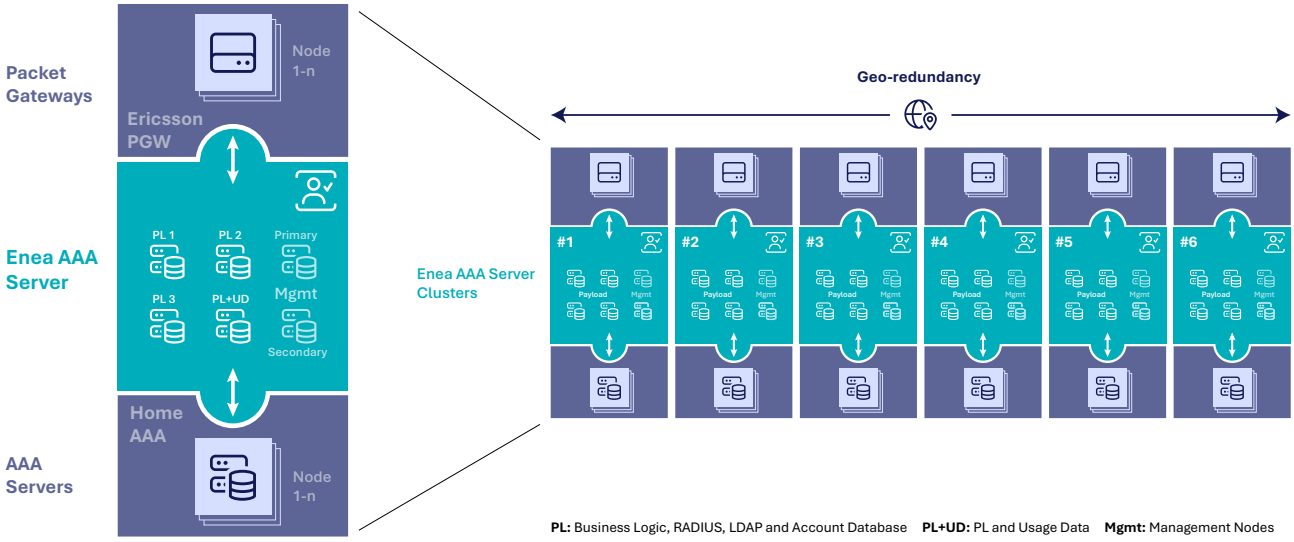
- **Subscriber Scale:** Support for 20 million monthly unique users and 12 million concurrent sessions.
- **Throughput:** Processing 36,000 TPS while simultaneously executing advanced business logic.

Virtualized Deployment Architecture

To meet these rigorous requirements, the Enea AAA Server is deployed as a **Virtual Network Function (VNF)**. The "Consumer" system comprises 36 VNF nodes organized into six clusters of six nodes each. An additional, functionally identical system with 18 nodes was deployed to support the "Corporate" service. For validation and testing, CSP B also maintains a 12-node Pre-production/Lab system.

Each cluster operates independently. Because the system is designed to be stateless for this use case, **geo-redundancy** is achieved without the need for complex inter-site synchronization, simplifying the overall architecture.

Cluster Configuration and Node Roles

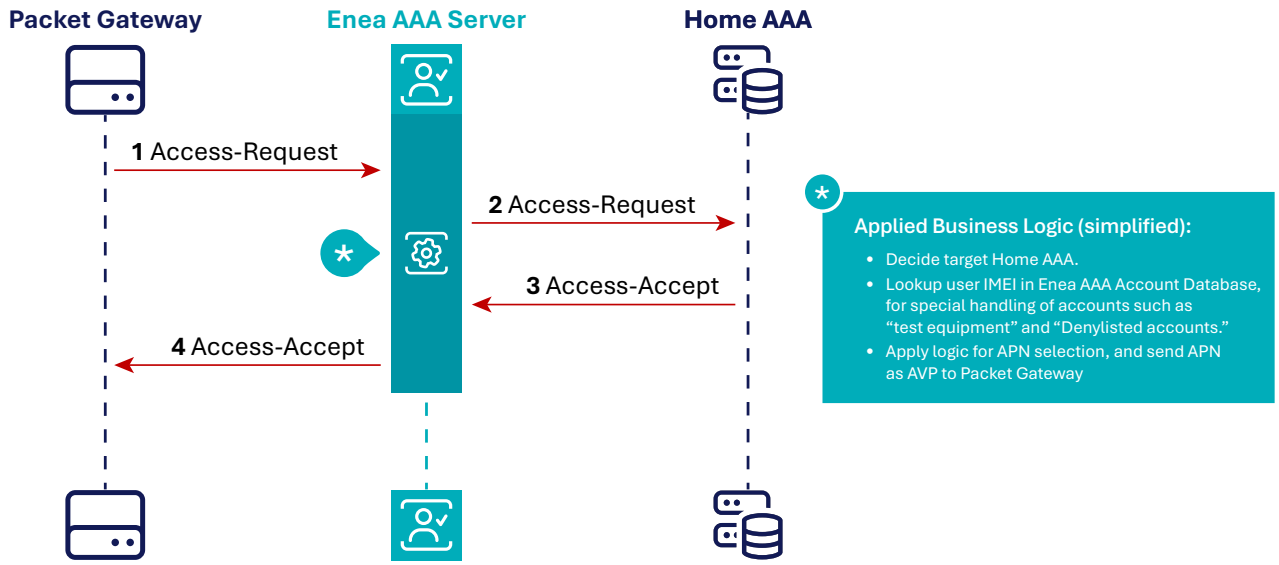


There are six Enea AAA Server clusters. Within each six-node cluster, functional roles are distributed to maximize performance and ensure continuous service availability:

- **Four Payload (PL) Nodes:** These nodes are dedicated to business logic execution, RADIUS signaling, LDAP queries, and the account database. The architecture is engineered for horizontal scaling, allowing for the addition of payload nodes as traffic volume increases. To optimize resource utilization, the fourth node in this group operates as a combo node, handling both standard payload processing and Usage Data (UD) functions.
- **Two Management (Mgmt) Nodes:** The primary management node is responsible for centralized system configuration, business logic updates, and daily administration. The secondary node serves as an **active redundant management node**, providing high availability (HA) across the cluster. To maximize operational efficiency, this secondary node remains fully accessible for daily tasks, such as log analysis, database queries, metric monitoring, and subscriber tracing.

APN Selection

The APN Selection process is driven by the Enea AAA Server's business logic engine, utilizing a combination of database lookups and advanced ruleset configurations. When the Enea AAA receives a RADIUS Access-Request from the Packet Gateway (PGW), the engine executes the logic to determine the correct Home AAA (HAAA) destination. Ultimately, the system assigns a specific APN, which is returned as an Attribute-Value Pair (AVP) in the Access-Accept message forwarded to the PGW.



Specialized Handling for Accounts and Devices

The Enea AAA provides granular control over specific account types and device models through its internal database (provisioned via GUI or CSV import). This allows the system to perform specialized handling for:

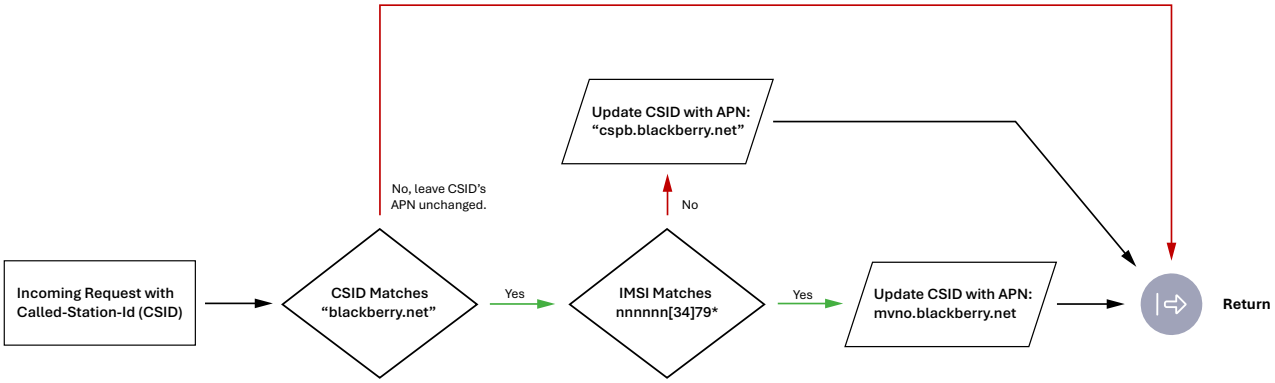
- **PLMN and Roaming Data:** Logic-based routing according to the origin network.
- **Restricted and Test Devices:** Denylisted devices, test IMSIs, and specific IMEIs.
- **Device Models and Firmware:** Utilizing a combination of the Type Allocation Code (TAC) and minimum Software Version (SV) to identify specific hardware and software revisions.

The business logic is designed to perform lookups against these tables in the Enea AAA internal database and take immediate action based on the results. This often leads to "Local Authentication," where the Enea AAA issues an Access-Accept or Access-Reject directly to the Packet Gateway without involving the Home AAA. This allows the system to resolve authentication for these special cases independently.

Programmable Rulesets and Pattern Matching

CSP B maintains full administrative control over the match tables and rulesets. While match tables handle basic use cases, the system leverages rulesets with pattern matching for complex, high-precision APN Selection.

Example Ruleset Execution



In this APN ruleset example, the Enea AAA Server first evaluates whether the Called-Station-Id matches "blackberry.net." If no match is found, the APN remains unchanged. If it does match, the system then applies the pattern *nnnn-nn[34]79** to verify the IMSI. If the IMSI matches this expression, the system returns the APN "mvnoblackberry.net"; otherwise, it returns "cspb.blackberry.net" within the modified Called-Station-Id attribute.

Note: Fort confidentiality we have anonymized APN names and replaced the first 6 digits in the IMSI with “n”.

The regular expression nnnnnn[34]79* perform matching according to this:

- Exact matching of the first 6 digits (nnnnnn) to match the MCC (country) and MNC (MNO Id) of CSP B.
- The 7th digit [34] matches either 3 or 4.
- The 8th digit matches exactly 7.
- 9* means zero or more 9 characters.

Extensible Hook Points

Beyond standard selection logic, the highly customizable rulesets allow CSP B to inject custom policy code at critical points in the signaling flow:

- **RADIUS Pre-Authentication:** Code execution prior to processing an authentication request.
- **RADIUS Post-Authentication:** Logic applied after the authentication decision is made.
- **RADIUS Pre-Accounting:** Logic applied before forwarding RADIUS Accounting messages.
- RADIUS Pre-Accounting-Copy: Custom logic executed before forwarding an accounting copy to an external AAA, analytics or billing server.

AAA Proxy Realms Configuration

The AAA Proxy Realms configuration, a core component of the Enea AAA Proxy package, manages the steering and handling of RADIUS Access and Accounting-Requests. This flexible configuration determines whether a request should be proxied to an external Home AAA (HAAA), or if it should be immediately accepted or rejected at the proxy layer.

Destination Mapping

The system utilizes pattern matching within the Realms configuration to identify the appropriate destination for each request. These destinations are organized into External Node Groups, which provide a layer of abstraction for managing multiple backend HAAA servers.

In addition to standard RADIUS Attribute-Value Pairs (AVPs), the Enea AAA can perform matching based on system-level attributes such as:

- The message type (e.g., Access-Request or Accounting-Request).
- The originating IP of the signaling packet.
- The configured name of the RADIUS client.

The system evaluates these filters in a **top-to-bottom order**, executing the first match found.

Accounting Management and Broadcasts

The Enea AAA provides granular control over accounting data to ensure billing integrity:

- **Accounting Broadcast:** Configurable within the Realm options, this setting can override the default proxy destination to ensure Accounting-Requests are distributed to multiple endpoints simultaneously.
- **Accounting Copy:** The system can be configured to send a duplicate stream of all accounting messages received from the PGWs to one or more external Node Groups. This is typically used for external analytics, auditing, or secondary billing systems without impacting the primary authentication flow.

RADIUS proxy with TPS Throttling

In high-scale deployments, network stability is often dictated by the capacity of the backend infrastructure. The Enea AAA Server's high-performance throughput usually exceeds the processing capabilities of legacy Home AAA (HAAA) systems. To prevent downstream service degradation, the Enea AAA includes TPS Throttling functionality. This allows the operator to set granular limits on outgoing RADIUS traffic, ensuring that the HAAA nodes are not overwhelmed during peak signaling bursts.

Advanced Operational and Integration Features

Several additional capabilities were implemented to enhance the management and extensibility of CSP B's environment:

- **Custom Counters:** Administrators can define custom counters within the rulesets to track specific signaling trends, such as the number of requests processed for a particular APN. These counters can then be analyzed via the internal metrics explorer or an external NMS such as Prometheus.
- **Batch Importing:** The configuration supports a custom batch-import utility. This enables the high-volume ingestion of subscriber accounts and match-table entries via CSV files, streamlining large-scale updates.
- **Comprehensive Unit Testing:** To ensure logic accuracy before deployment, the system includes a robust unit testing framework. This allows for the evaluation of APN Selection rulesets against test data. CSP B can perform batch unit tests via CSV uploads or integrate these tests into automated programmatic validation using the REST API.
- **Dynamic External Lookups:** The Enea AAA Server's programmable rulesets can be configured to perform real-time LDAP and SQL lookups, allowing authentication and selection decisions to be enriched by external subscriber data repositories.

System Interfaces

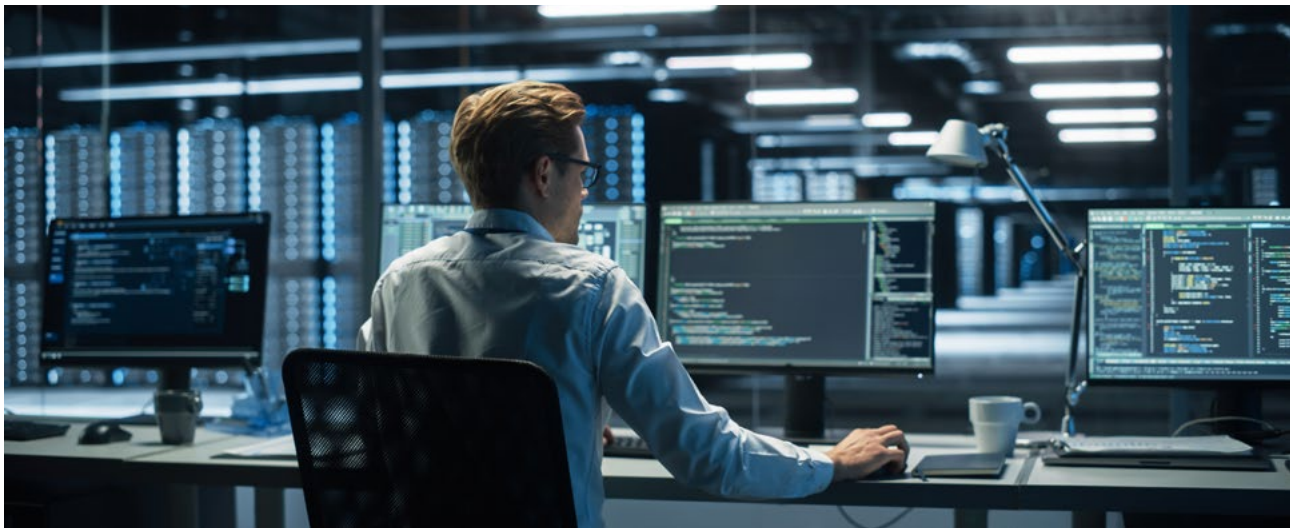
In this deployment, the Enea AAA Server acts as a high-performance hub, supporting the following interface protocols:

Inbound Interfaces:

- **RADIUS:** Processing Access and Accounting messages from the Packet Gateways (PGW).

Outbound Interfaces:

- **RADIUS:** Delivering Access-Accept/Reject responses to the PGWs and proxying signaling to the Home AAAs.
- **LDAP/SQL:** Facilitating external database queries via custom rulesets.
- **Usage Data:** Pushing Call Detail Records (CDRs) to remote SFTP servers for billing and auditing.



CSP C - TIER 1 LATIN AMERICAN MOBILE OPERATOR

Logics Mediation Layer with Policy-based Diameter Routing

CSP C, a leading Tier 1 mobile operator in Latin America, implemented a strategic Wi-Fi offloading initiative. By leveraging third-party Wi-Fi infrastructure—comprising over 35,000 Access Points (APs) in high-traffic locations such as hotels, airports, and shopping malls—CSP C significantly reduced the costs associated with expanding cellular coverage in congested areas.

THE CHALLENGE

Security Gaps and HSS Routing Complexity

The operator's legacy infrastructure utilized combined 3GPP AAA and HSS nodes (Combo AAA/HSS), which lacked support for encrypted IMSIs, creating a significant security gap. Furthermore, CSP C required a sophisticated, policy-based Diameter routing mechanism to intelligently direct authentication requests for entitled subscribers across ten distinct Combo AAA/HSS nodes.

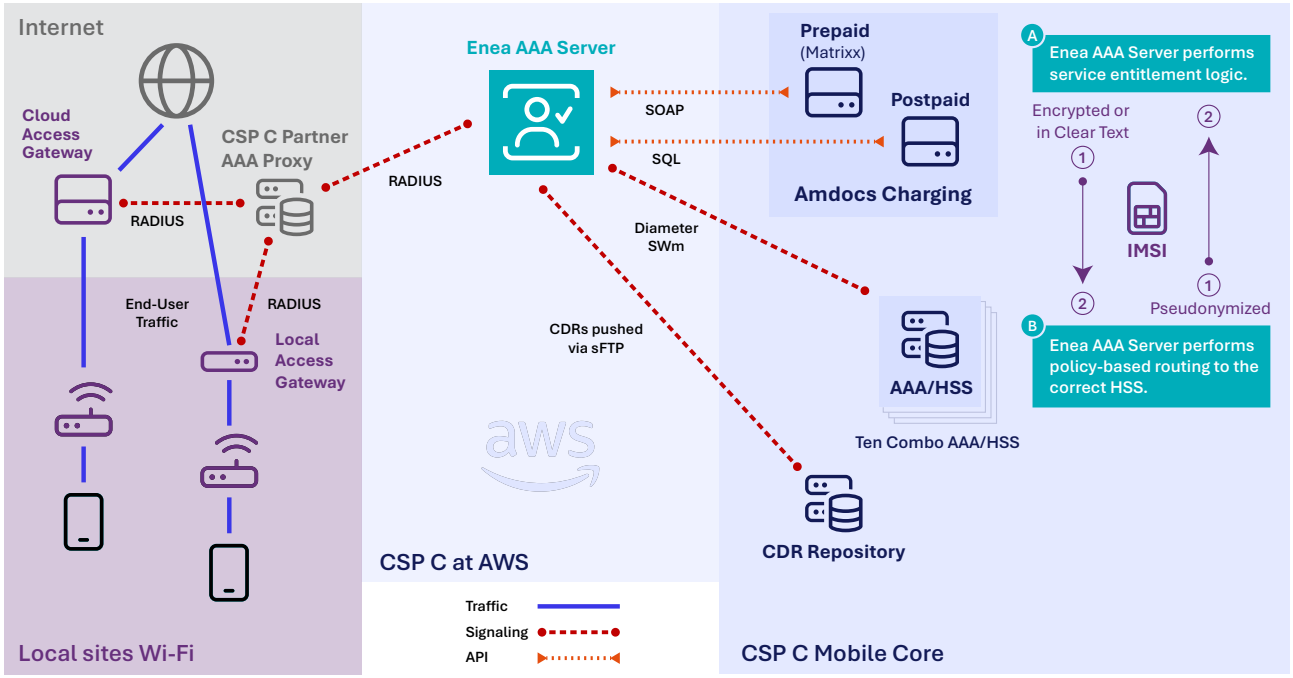
THE SOLUTION

Enea AAA Server as Logics Mediation Layer

Note: Overcoming Legacy Architectural Constraints

CSP C was burdened by an inflexible legacy 3GPP AAA that was tightly coupled with its integrated HSS function. This "Combo" architecture made a standalone AAA replacement impossible without a simultaneous—and commercially unviable—replacement of the HSS. Because the legacy platform lacked support for the standard SWx interface, the operator faced a significant integration hurdle.

To leverage the Enea AAA Server's advanced business logic and policy-based routing, CSP C chose a pragmatic architectural adaptation: utilizing the SWm interface between the Enea AAA proxy and the legacy Combo nodes, despite the non-standard nature of this specific signaling path (as SWm typically serves as the interface between the ePDG and the 3GPP AAA). While Enea strictly adheres to 3GPP standards, this deployment demonstrates how intelligent mediation can be used as a "surgical" intervention to modernize service logic in even the most rigid legacy environments.



The Enea AAA Server was deployed as an intelligent AAA Proxy with comprehensive support for encrypted IMSIs. Operating as a logical mediation layer, the system integrates entitlement logic and policy-based Diameter routing via a specialized two-step process:

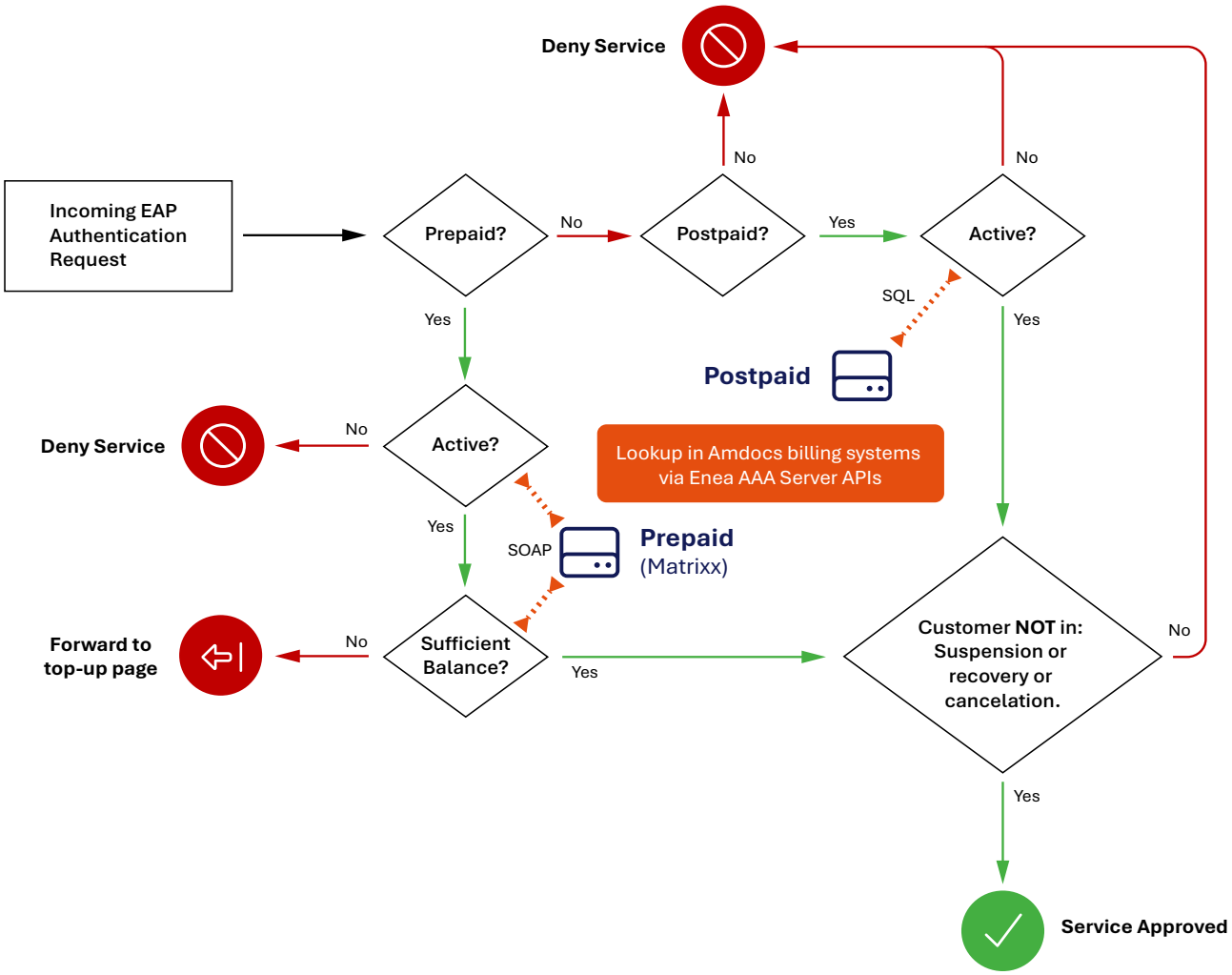
- **A – Entitlement Logic:** The Enea AAA Server validates service eligibility through real-time API lookups to CSP C's Amdocs Prepaid (Matrixx) and Postpaid billing systems.
- **B – Policy-Based Diameter Routing:** The server intelligently routes authentication requests to the appropriate AAA/HSS node based on subscriber identity.

Adaptive Execution Flow

The execution order of these activities is dynamically determined by the format of the received identity:

- **Cleartext or Encrypted IMSI:** Entitlement logic is performed first to ensure the subscriber is authorized before engaging the Combo AAA/HSS nodes.
- **IMSI Pseudonyms:** The process is reversed; the Enea AAA first performs policy-based Diameter routing to resolve the pseudonym and retrieve the permanent identity from the Combo AAA/HSS before triggering the entitlement logic.

Service Entitlement Logic



Prepaid Users

The Enea AAA Server leverages a SOAP API to verify account status and balance. Access is granted only if the subscriber has a sufficient balance and is not in a "suspended," "recovery," or "canceled" state. Users with insufficient funds are automatically redirected to a captive top-up portal.

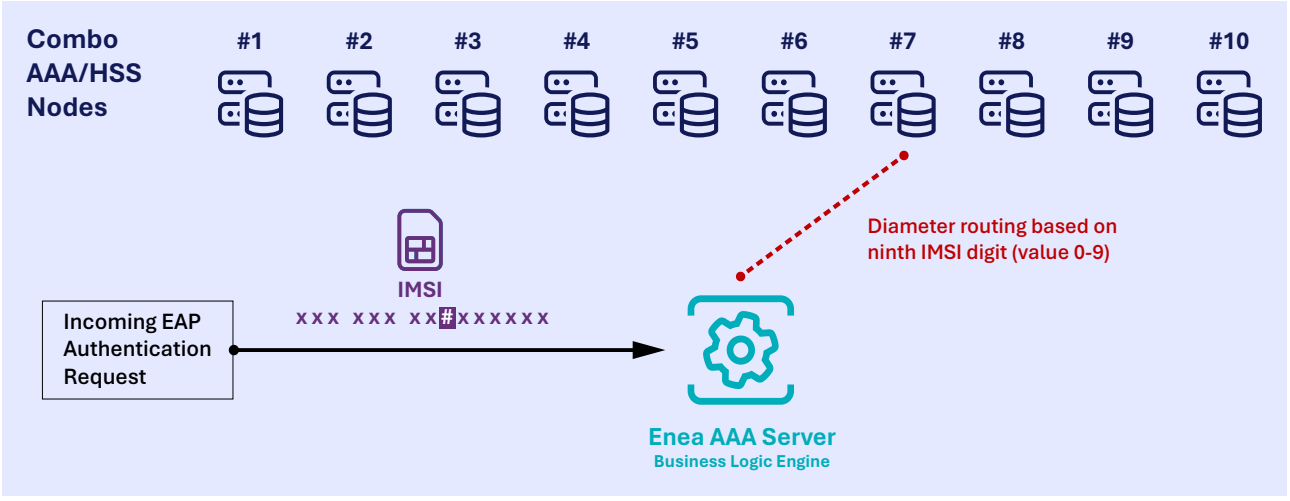
Postpaid Users

Utilizing an SQL interface, the Enea AAA Server confirms that the postpaid account is active and in good standing (not suspended or canceled) before granting network access.

Policy-based Diameter Routing

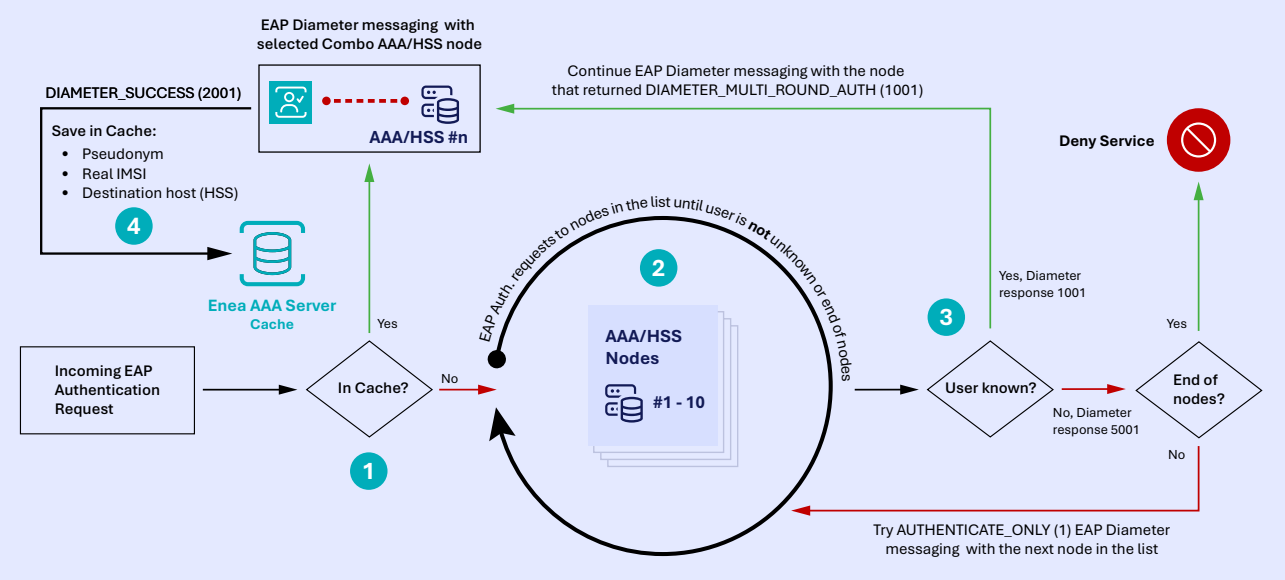
To manage its massive subscriber base, CSP C segments users across 10 separate Combo AAA/HSS nodes. The Enea AAA Server ensures intelligent routing based on the following scenarios:

Scenario 1: IMSI Received (Encrypted or Cleartext)



When the IMSI is available, the Enea AAA Server inspects the 9th digit of the IMSI to determine the destination. Through a dynamic GUI, CSP C administrators can map digits (0–9) to the specific AAA/HSS Destination-Host. To ensure high availability and load distribution, the system supports multiple hosts per digit using a round-robin algorithm.

Scenario 2: IMSI Received as a Pseudonym

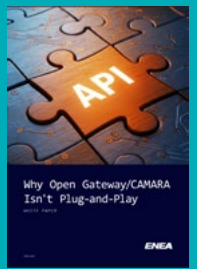


If an IMSI pseudonym is used, the 9th-digit routing logic cannot be applied. In this case, the Enea AAA Server follows a prioritized resolution process:

1. **Cache Lookup:** The Enea AAA Server queries its local cache to see if the pseudonym has a known mapping to a Destination Combo AAA/HSS host (AAA/HSS). If so, it starts EAP Diameter messaging with the selected AAA/HSS.
2. **Sequential Probing:** If no cache entry exists, the Enea AAA sends EAP Diameter Authentication requests to a preconfigured list of AAA/HSS nodes in a specific order.
    - The system uses the Auth-Request-Type AVP set to AUTHENTICATE_ONLY (1).
    - If an HSS returns DIAMETER_ERROR_USER_UNKNOWN (5001), the Enea AAA automatically tries the next HSS on the list.
3. **Discovery & Authentication:** This process continues until the server receives a DIAMETER_MULTI_ROUND_AUTH (1001) response, indicating the correct AAA/HSS has been found. The EAP Diameter messaging then continues with that AAA/HSS until the user has been authenticated.
4. **Caching for Performance and Session Persistence:** Once DIAMETER_SUCCESS (2001) is achieved, the Enea AAA caches the mapping of the pseudonym, the real IMSI, and the Destination Combo AAA/HSS.

Performance Note: By default, these mappings are cached for 8 hours. Since this duration is configurable via the Enea GUI, it allows CSP C to balance system performance with the frequency of HSS lookups.

The powerful combination of a robust business logic engine, flexible protocol adapters, and comprehensive API support positions the Enea AAA Server as an essential tool for solving 'real-world' operational challenges. Beyond mediation and interworking, these capabilities also empower operators to unlock new revenue streams through initiatives like GSMA Open Gateway (CAMARA). To explore why these APIs require an intelligent mediation layer to succeed, read our companion paper: Why Open Gateway/CAMARA Isn't Plug-and-Play.



CSP D - TIER 1 EUROPEAN MOBILE OPERATOR

RADIUS-as-a-Service for Mobile IP Enterprise VPN

CSP D, a leading Tier 1 European mobile operator, deployed the Enea AAA Server as a dedicated 3GPP AAA to support its Enterprise IP VPN RADIUS service. This solution—branded internally as RADIUS-as-a-Service (RaaS)—is embedded within their Mobile IP Enterprise VPN offering, allowing enterprise customers to securely access their private corporate networks directly from the CSP D mobile network.

THE CHALLENGE

Specialized High-End Enterprise Requirements

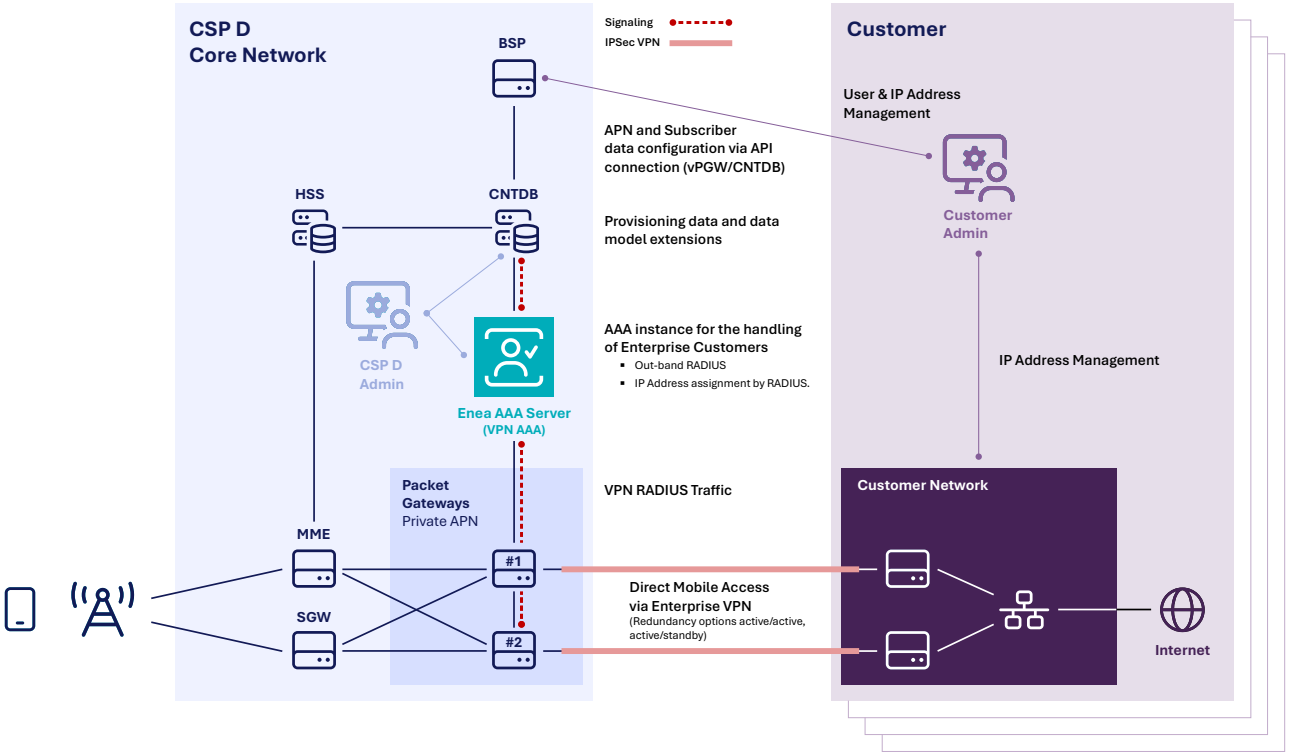
While CSP D's existing Enea AAA infrastructure was optimized for consumer and mass-market enterprise services, the high-end enterprise segment required more granular control. Key requirements included:

- Secure, direct access to private customer networks.
- Self-management capabilities for both static and dynamic IP address assignment.
- Specialized accounting handling to support VPN RADIUS session keepalives.

THE SOLUTION

Dedicated AAA Instance for Mobile IP Enterprise VPN

To meet these demands, CSP D implemented a dedicated Enea AAA Server instance tailored for RaaS. This instance provides robust access control, advanced IP Address Management (IPAM), and specialized accounting, ensuring enterprise subscribers maintain secure and persistent connections to their private networks.

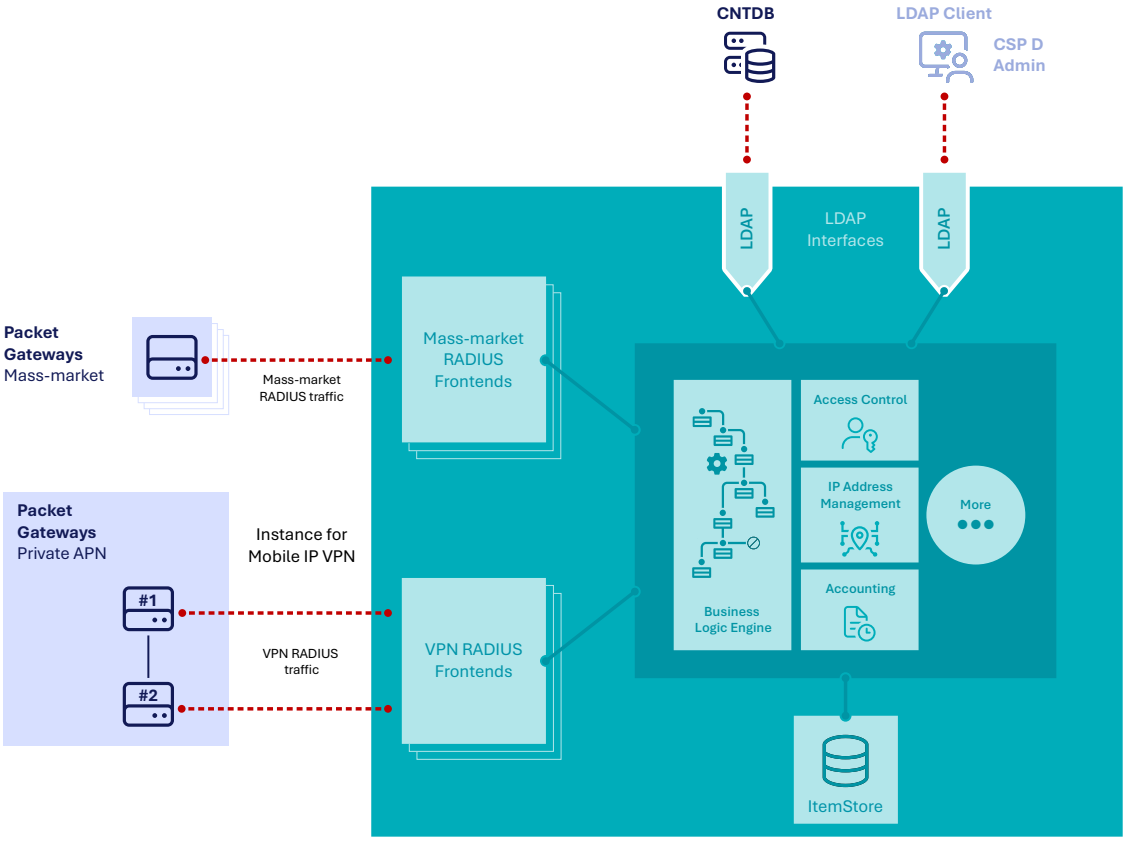


The architecture comprises three core elements:

- **Business Service Portal (BSP):** Provides the user interface for managing access control policies and IP configuration data.
- **Common Nokia NT Subscriber Database (cNTDB):** Serves as the persistent repository for all subscriber-related data.
- **Enea AAA Server:** Functions as the 3GPP AAA, executing the access control and IP configuration logic.

The solution integrates with the mobile packet core via the RADIUS protocol and leverages Private APNs to facilitate secure enterprise network access.

RADIUS Service Separation



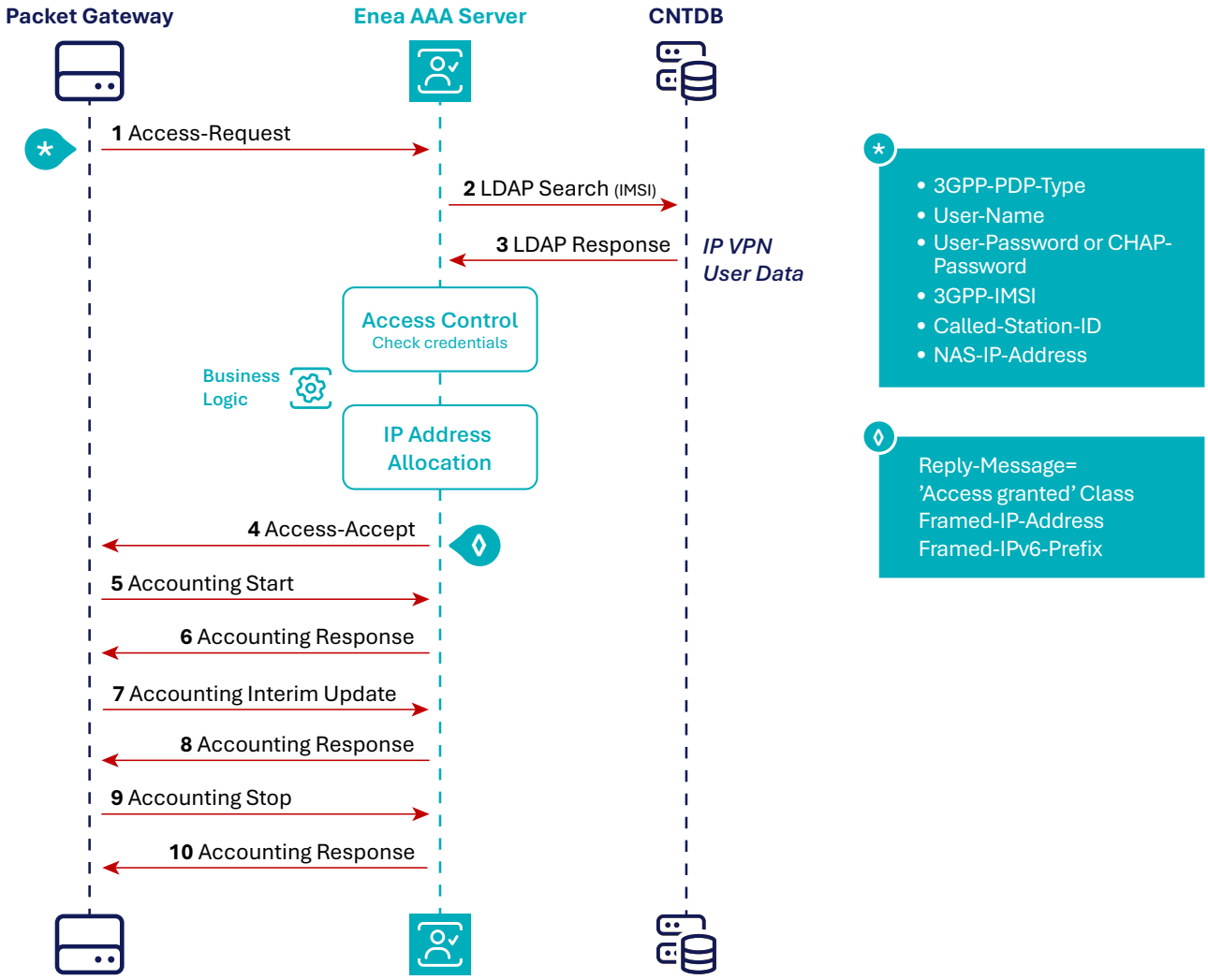
To ensure isolation and performance, a separate RADIUS service instance was introduced within the Enea AAA Server framework. This architectural separation allows the Mobile IP VPN traffic to be managed independently from mass-market traffic, ensuring excellent user experience for mission-critical enterprise sessions.

Service Capabilities

The Enea AAA Server Mobile IP VPN instance supports the following technical requirements:

1. **Access Control**
    - Support for both PAP and CHAP authentication protocols.
2. **IP Address Management (IPAM)**
    - Dynamic IP Assignment: IP pool selection is determined by a combination of the (alias) APN, Realm, and the (alias) PGW IP address. The system supports IPv4, IPv6, and dual-stack IPv4v6 pools.
    - Static IP Assignment: Supports IPv4, IPv6, and IPv4v6 addresses provisioned directly within the cNTDB.
    - DNS Management: Automated assignment of DNS server addresses.
3. **Accounting**
    - Processing of RADIUS Start, Interim, and Stop messages to support VPN session keepalives and auditing.

High-Level Call Flow



The Enea AAA Server processes Mobile IP Enterprise VPN access requests through a two-step logic engine:

1. **Access Control:** The system first validates the subscriber's credentials to grant or deny access to the private customer network.
2. **IP Address Allocation:** Once access is granted, the Enea AAA evaluates the incoming RADIUS Access-Request attributes, PDP context, and cNTDB data to apply the appropriate static or dynamic IP assignment logic.

Additionally, the Enea AAA manages RADIUS Accounting messages throughout the session to maintain keepalive status, ensuring the VPN tunnel remains active and monitored.

CSP E - TIER 1 NORTH AMERICAN MOBILE OPERATOR

HTTP/2 to Diameter Protocol Conversion

CSP E, a leading North American Tier 1 mobile operator, utilizes the Enea AAA Server as an Interworking Function (IWF) to bridge the signaling gap between its 5G Standalone (SA) core and its legacy mediation infrastructure. The Enea IWF performs high-performance protocol conversion between 5G HTTP/2-based end-points (N7 and N40) and the Diameter-based Gx and Gy interfaces required by the Hewlett Packard Internet Usage Manager (IUM).

THE CHALLENGE

The 5G Protocol Mismatch: Legacy Systems in an HTTP/2 Core

While CSP E's mobile core has evolved to support 5G SA, the operator continues to rely on the **HP IUM** to collect, aggregate, and normalize usage data for its billing systems. However, HP IUM reached End-of-Life (EoL) in 2021 and lacks support for the HTTP/2 RESTful protocols used by modern **5G Session Management Functions (SMF)**. This created a critical compatibility barrier between the legacy mediation layer and the next-generation core.

THE SOLUTION

Enea AAA Server as an Intelligent Interworking Function

The Enea AAA Server serves as a versatile mediation and protocol conversion layer, leveraging its powerful business logic engine to facilitate signaling between the 5G Session Management Function (SMF) and the legacy HP IUM. In this 5G architecture, the Enea Interworking Function (IWF) operates as an **HTTP/2 Server** for the 5G core and a **Diameter Client** for the HP IUM. Simultaneously, the solution provides essential mediation for 4G services, rewriting signaling messages to ensure seamless compatibility between the 4G Packet Gateway (PGW) and the HP IUM infrastructure.

Deployement:

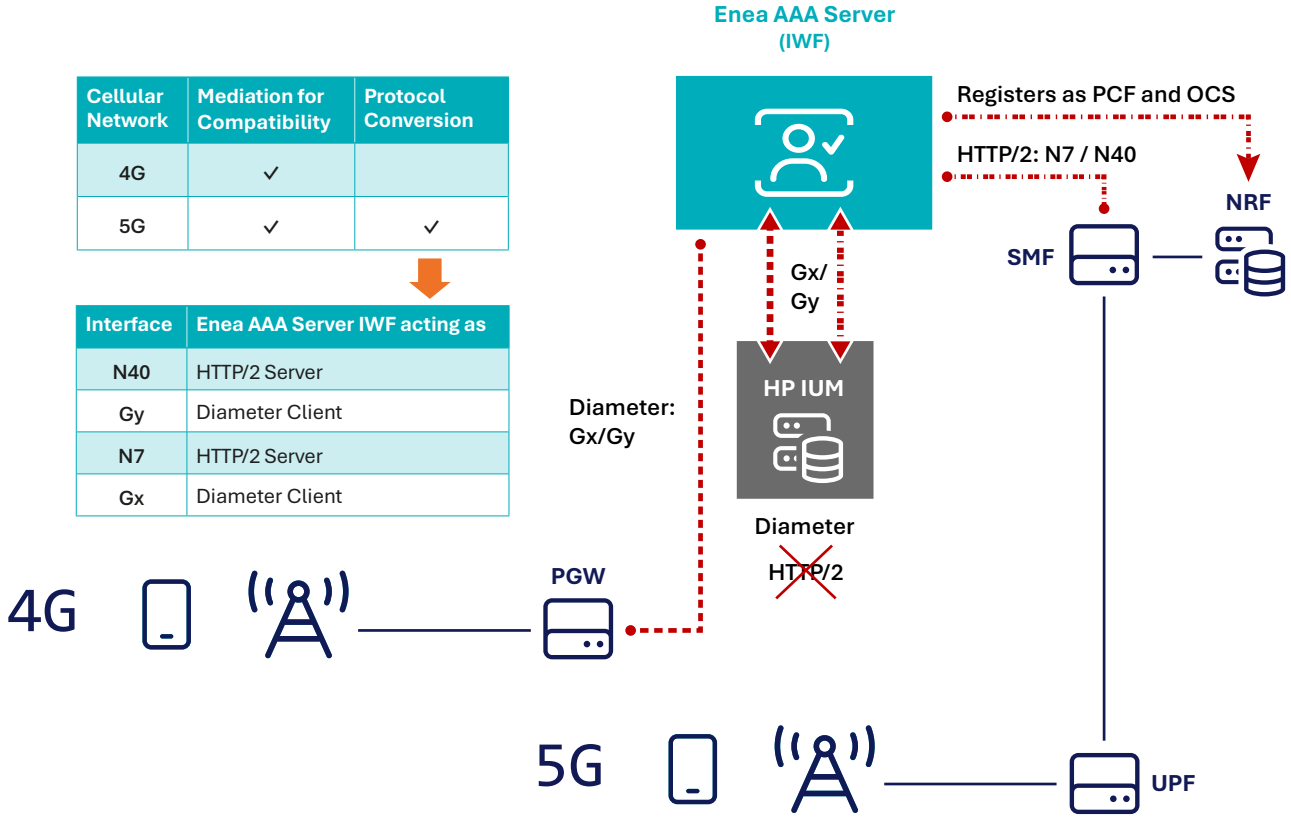
The Enea solution is deployed as a Cloud-Native Function (CNF) within a Kubernetes environment. To ensure high availability, the system is distributed across three regions, each featuring two geographically separate sites. Each site is dimensioned to handle the full traffic load for its respective region, providing robust local failover capabilities.

Key Technical Advantages

- **Selective Protocol Support:** The solution supports the specific subsets of N7 and N40 required by CSP E, performing 1:1 mapping between HTTP/2 JSON fields and Diameter Attribute-Value Pairs (AVPs).
- **Logic Abstraction:** The Business Logic Engine separates application logic from external interfaces. This allows CSP E to adapt to changing requirements or specific signaling behaviors via configuration updates, eliminating the need for core code patches or new product releases.

Cellular Network	Mediation for Compatibility	Protocol Conversion
4G	✓	
5G	✓	✓

Interface	Enea AAA Server IWF acting as
N40	HTTP/2 Server
Gy	Diameter Client
N7	HTTP/2 Server
Gx	Diameter Client

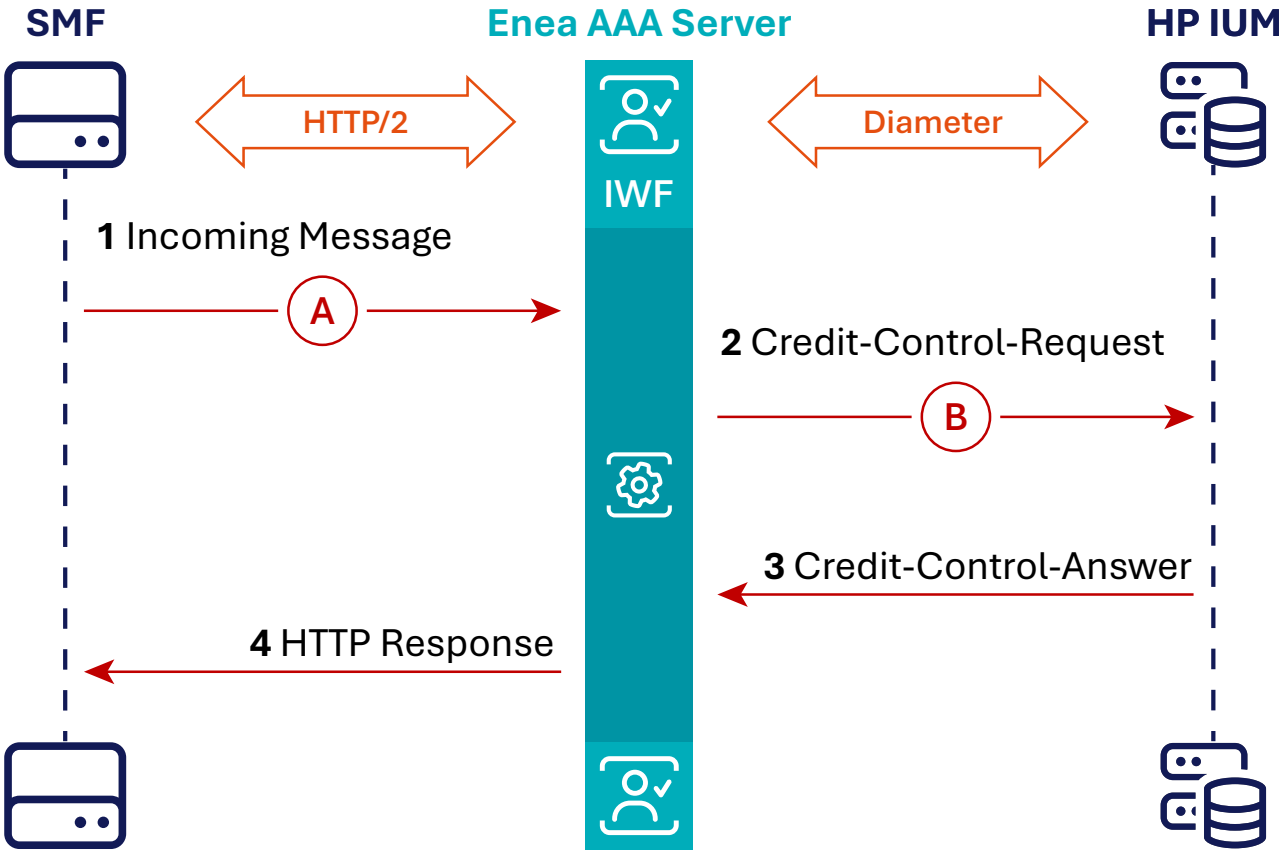


Mediation Examples

The flexibility of the Business Logic Engine allows CSP E to implement a wide range of custom signaling rules. Representative examples of these specialized behaviors include:

- **Suppression of CONTINUE Credit-Control-Failure-Handling:** To support the PGW's internal CONTINUE-RETAIN policy, the IWF suppresses any Credit-Control-Failure-Handling AVPs with a value of CONTINUE. By not sending this value in the reply, the IWF allows the PGW to execute its local policy, while all other values for this AVP are forwarded transparently.
- **Service-Identifier Translation:** Due to communication constraints between the SMF and HP IUM, the IWF translates 5G Service Identifiers into the specific Rating-Group/Service-Identifier pairs required by IUM.
- **Zero-Usage Filtering:** To prevent downstream processing errors in the legacy IUM, the IWF filters out 5G usage updates with a total volume of zero before they are proxied.
- **Context Management and Attribute Injection:**
  - ✓ **AF-Charging-ID Management:** The IWF stores the AF-Charging-Identifier received via Gx and injects it into subsequent Gy messages to satisfy HP IUM's requirements for session continuity.
  - ✓ **Access-Network-Charging-Identifier Injection:** Since the SMF does not transmit the Access-Network-Charging-Identifier, the IWF stores this value and inserts it into outgoing CCR-T (Terminate) messages to ensure the IUM receives a complete session record.
- **Synchronized Session Closure:** To maintain data integrity, the IWF ensures that the N7 policy session remains open until the corresponding N40 charging session is closed, ensuring that critical context from the policy layer is available for final charging updates.
- **Bitrate Normalization:** The IWF ensures bitrate values are delivered to the SMF in a consistent "bps" format, preventing issues with prefix conversion (e.g., ensuring "1024 bps" is sent instead of "1 kbps").
- **Result Code Mapping:** The IWF maps Diameter result codes (e.g., DIAMETER_SUCCESS) to appropriate HTTP status codes (e.g., 201 Created) to ensure the 5G core receives standard RESTful responses. Errors are mapped to corresponding HTTP status codes (4xx/5xx errors).
- **Bitrate AVP and value adjustment:** The IWF maps ***Max-Requested-Bandwidth-UL/DL*** from the HP IUM to the ***APN-Aggregate-Max-Bitrate-UL/DL*** format required by the PGW. It also adjusts special values (e.g., 0/0) to concrete, PGW-supported bitrates to ensure consistent QoS enforcement.
- **Gx update triggering:** IWF can trigger Gx Re-Auth-Requests (RARs) and thus request for Gx Update based on Gy traffic. This allows for faster updates to the session limits (e.g., bandwidth), based on Gy RARs and/or responses as they arrive from HP IUM.

High-Level Message Flows: Protocol Conversion



Request Flow (HTTP/2 to Diameter):

1. The Enea IWF receives an HTTP/2 signaling message from the **SMF (A)**.
2. The business logic engine translates JSON fields into appropriate Diameter AVPs and initiates a **Credit-Control-Request (CCR)** toward the **HP IUM (B)**.
3. Upon receiving a **Credit-Control-Answer (CCA)** from the IUM, the IWF maps the AVPs back to JSON fields and returns the appropriate HTTP status code to the SMF.

Note: If there's a field that cannot be translated 1:1, the same will be omitted from the outgoing diameter message.

In the following section, we delve into the critical protocol conversions performed by the Enea IWF. This process involves transforming incoming HTTP/2 signaling (A) from the SMF into the Diameter signaling (B) required by the HP IUM.

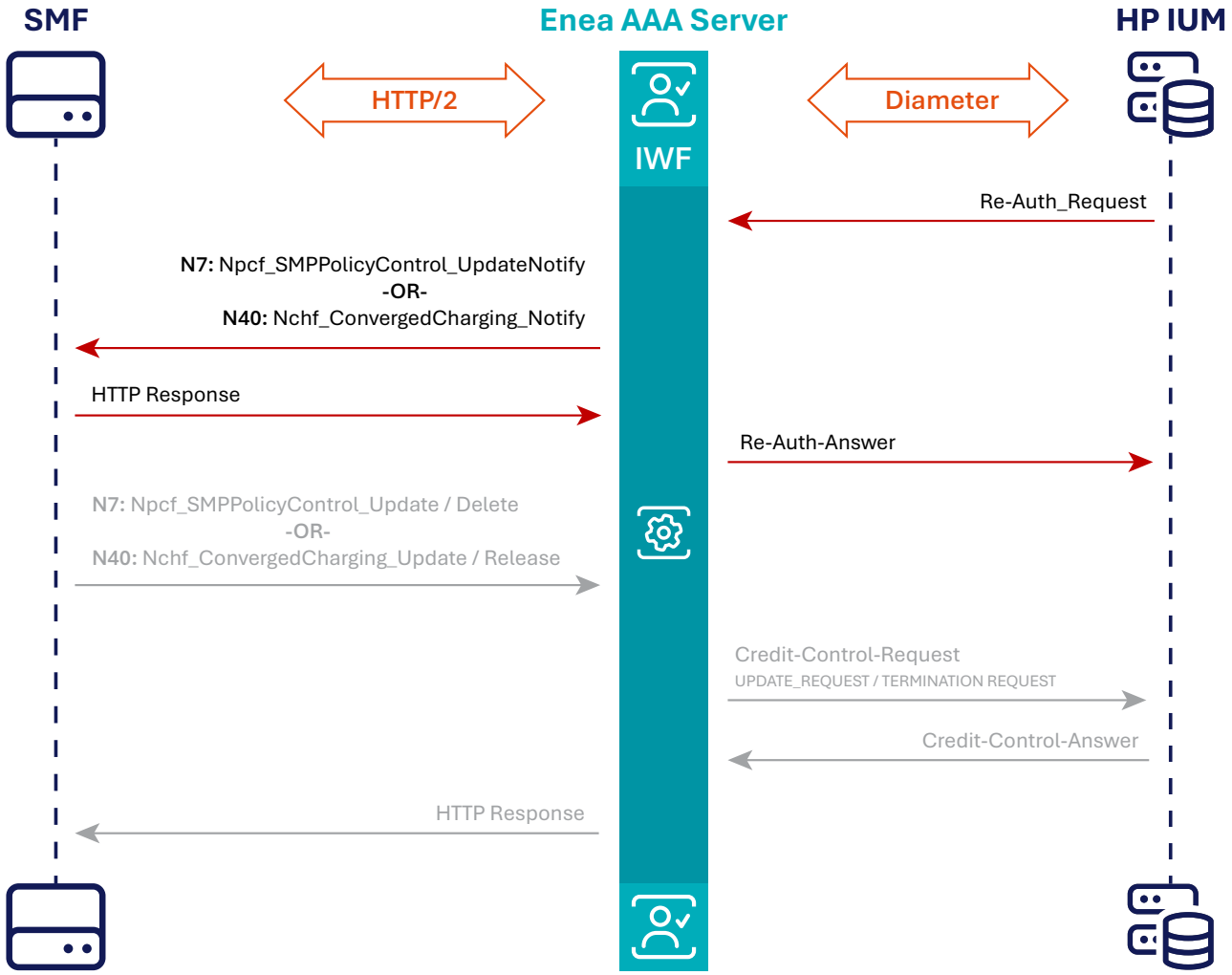
Protocol Conversion Details

Below table shows the most important conversions that are made by Enea IWF:

HTTP/2 (A) Diameter (B)

Service Operation	What it does	SMF ➔ IWF Message	IWF ➔ HP IUM Message
N40 Create	Provides means for the Network Function Consumer to create the resource of the charging session. It will result in quota authorization for service delivery on the destination HP IUM.	**N40:** Nchf_ConvergedCharging_Create	**Gy:** Credit-Control-Request (INITIAL_REQUEST)
N40 Update	Used to report usage and may request further quota authorization.	**N40:** Nchf_ConvergedCharging_Update	**Gy:** Credit-Control-Request (UPDATE_REQUEST)
N40 Release	Provides means for the Network Function Consumer to release the resource of charging session information.	**N40:** Nchf_ConvergedCharging_Release	**Gy:** Credit-Control-Request (TERMINATION_REQUEST)
N7 Create	Provides a request to create a Session Management Policy Association with the PCF to receive the policy for a PDU session.	**N7:** Npcf_SMPolicyControl_Create	**Gx:** Credit-Control-Request (INITIAL_REQUEST)
N7 Update	A request to update the Session Manage-ment Policy association with the PCF to receive the updated policy when the Policy Control Request Trigger condition is met.	**N7:** Npcf_SMPolicyControl_Update	**Gx:** Credit-Control-Request (UPDATE_REQUEST)
N7 Delete	Provides means for the Network Function Consumer to delete the Session Manage-ment Policy Association and the associated resources.	**N7:** Npcf_SMPolicyControl_Delete	**Gx:** Credit-Control-Request (TERMINATION_REQUEST)

Re-Auth-Request (RAR) and Notification Flow



When the HP IUM initiates a **Re-Auth-Request (RAR)** over Diameter, the Enea IWF triggers a separate notification flow to the SMF:

- **Charging Notifications:** A N40 Notify Service Operation (Nchf_ConvergedCharging_Notify) is sent to the SMF to communicate subscribed events.
- **Policy Notifications:** A N7 Update/Notify Service Operation (Npcf_SMPolicyControl_UpdateNotify) is triggered to update or delete PCC (Policy and Charging Control) rules and PDU session-related policy context.

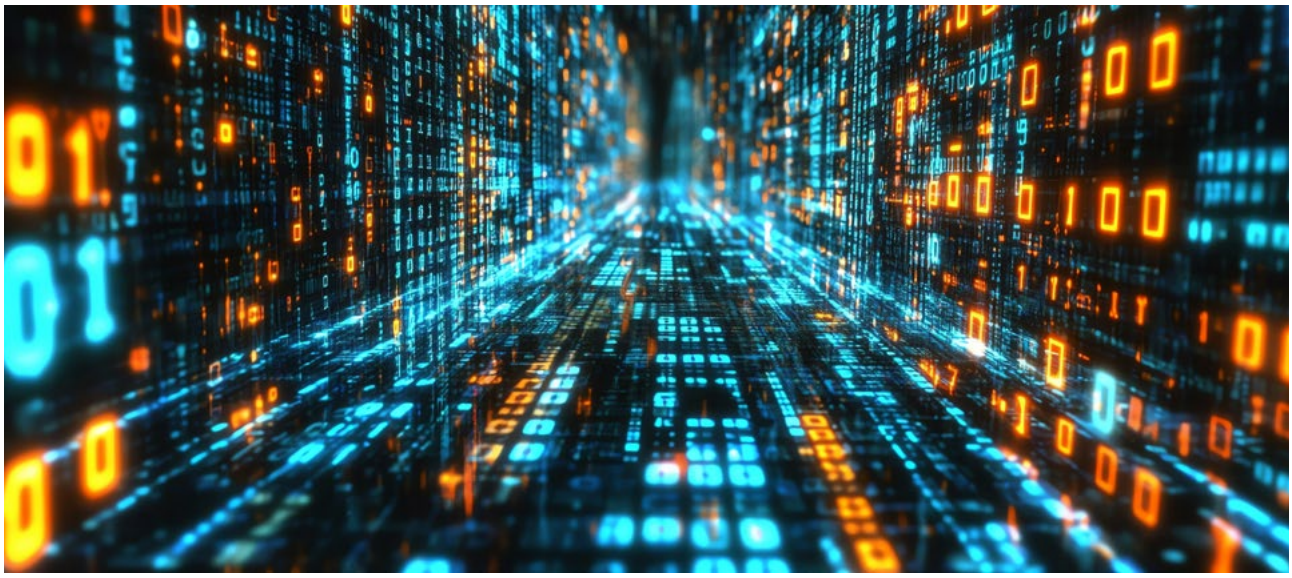
Once the notification is sent out to the SMF from Enea IWF, the expectation is that this will trigger an update or release operation on SMF. This will be processed as the completely separate call flow described above.

Note: If AVPs in the Re-Auth-Request are not sufficient to create the Notify request, the same will be omitted.

CSP F - TIER 1 EUROPEAN CABLE / FIXED OPERATOR

RADIUS-to-SQL Mediation for Migration to Central CGN

CSP F, a major Tier 1 European cable and fixed-line operator, leveraged the intelligent protocol mediation capabilities of the Enea AAA Server to consolidate its infrastructure. By providing a high-performance bridge between RADIUS-based signaling and SQL-based database environments, the Enea solution enabled a seamless migration to a centralized Carrier-Grade NAT (CGN) platform.



THE CHALLENGE

Bridging the SQL Compatibility Gap

Dual-Stack Lite (DS-Lite) is a critical transition technology for operators like CSP F as they migrate from IPv4 to IPv6 across xDSL, Cable, and FTTH networks. DS-Lite allows an operator to run an IPv6-only core while maintaining IPv4 internet access for subscribers by having the Customer Premises Equipment (CPE) wrap IPv4 packets within IPv6. The Carrier-Grade NAT (CGN) at the operator's core then unwraps these packets and assigns them a public IPv4 address for internet routing.

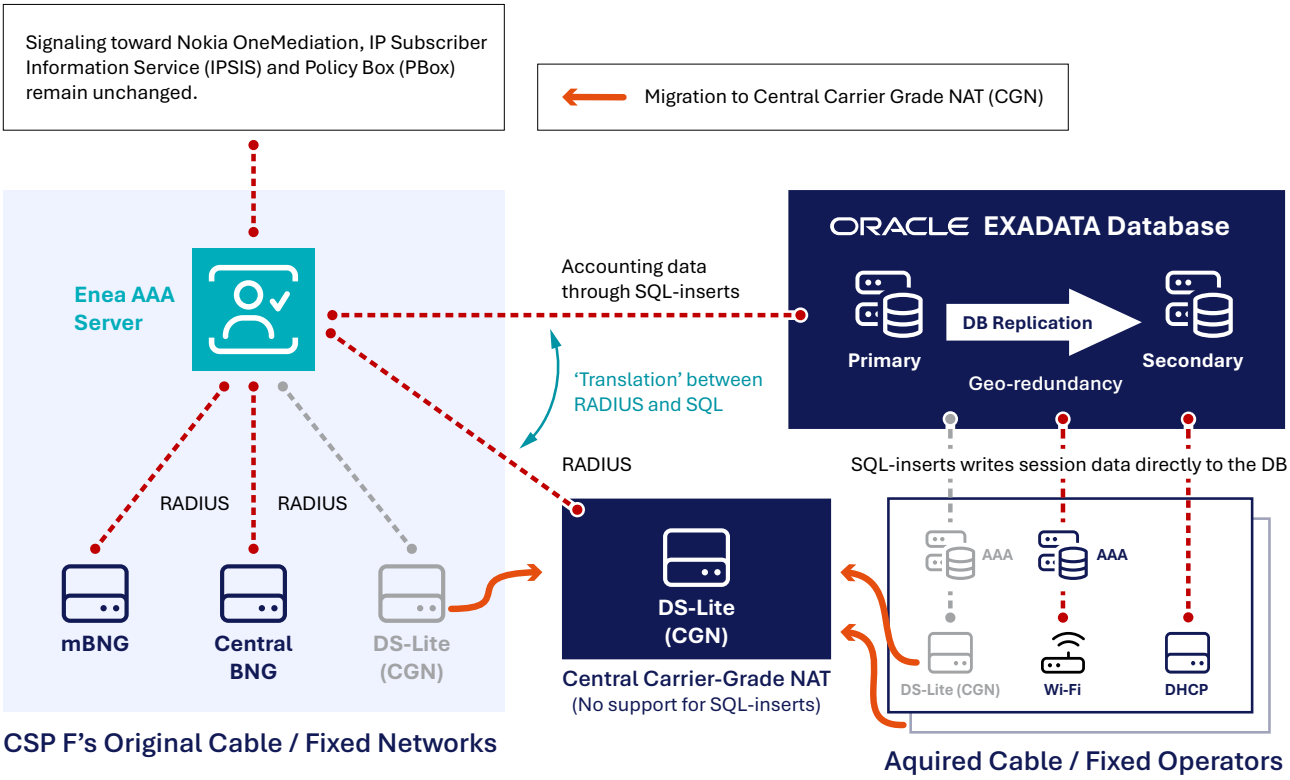
Following several acquisitions, CSP F sought to consolidate three independent CGN platforms into a single, centralized CGN solution. However, a significant technical 'showstopper' emerged: while the CGN systems at the acquired operators were capable of writing accounting data directly to the central **Oracle Exadata database** via SQL, the new centralized CGN platform—intended to harmonize the entire network—supported only the RADIUS protocol and lacked native SQL support.

Without a mechanism to transform RADIUS accounting data into SQL inserts, CSP F could not maintain the required session logging within its Oracle Exadata environment, effectively stalling the entire migration.

THE SOLUTION

Intelligent RADIUS-to-SQL Mediation

CSP F turned to the Enea AAA Server to serve as an intelligent **RADIUS-to-SQL translator**. Already serving as the central AAA platform for the operator, the Enea solution leveraged its flexible **Business Logic Engine** to perform real-time protocol transformation.



The Enea AAA Server now acts as a high-performance mediation layer that seamlessly transforms RADIUS accounting records into SQL inserts, regardless of the originating access technology (DSL, Cable, or FTTH).

Key Capabilities:

- **High-Throughput Mapping:** All RADIUS Accounting-Requests (Start, Interim-Update, and Stop) are converted into SQL INSERT statements in near real-time. The system maintains a 1:1 mapping, ensuring each accounting event is accurately reflected as a database record in the Oracle Exadata cluster.
- **Resilient Data Logging:** To ensure no accounting data is lost during database maintenance or network timeouts, the Enea AAA includes an internal caching mechanism. If the Oracle DB is temporarily unavailable, records are cached with a configurable expiration time (defaulting to two hours). The system automatically retries the SQL inserts once connectivity is restored.
- **Multi-Node Support:** Beyond the central CGN, the Enea AAA provides this same transformation logic for other network elements, including mBNGs and Central BNG nodes. The solution is highly configurable, allowing data to be written into separate tables for each node type such as mBNG and Central BNG or consolidated into a unified table based on CSP F's operational requirements.

Strategic Impact

By implementing this intelligent mediation layer, CSP F successfully overcame the technical limitations of its new CGN platform. The Enea AAA Server enabled the operator to unify its core network signaling by integrating the new centralized CGN alongside its existing **Nokia Mediation, IPSIS (IP Subscriber Information Service)**, and **Policy Box (PBox)** environments. This unified approach ensured a risk-free migration to a modernized, consolidated architecture while maintaining full continuity for critical downstream auditing and policy systems.

CSP G - TIER 1 EUROPEAN MOBILE OPERATOR

IoT Connectivity Control

CSP G, a leading Tier 1 European mobile operator, leverages the Enea AAA Server as an IoT Connectivity Control Function (ICCF), operating in concert with the existing Aeris IoT Connectivity Management Platform. Delivered as a comprehensive 'as-a-service' offering hosted on Amazon Web Services (AWS), the Enea solution utilizes the Enea AAA Server to manage the control plane, while Enea-deployed FortiGate next-generation firewalls handle the traffic plane.

THE CHALLENGE

Scaling Secure Connectivity for the SME "Long Tail"

As cybersecurity threats increase, secure cellular IoT connectivity has transitioned from a competitive advantage to a baseline requirement. However, the traditional method of delivering security via **Private Access Point Names (APNs)** does not scale for the "long tail" of small and medium-sized enterprise (SME) customers.

Limitations of Traditional Private APNs:

- **High Operational Costs:** Configuring and maintaining unique Private APNs for thousands of SMEs is resource-intensive for the mobile core.
- **Manual VPN Provisioning:** Establishing Enterprise VPNs between the Packet Gateway and customer networks often takes weeks and consumes significant engineering resources.
- **Rigid 1:1 Architecture:** Standard Private APNs typically support only one Enterprise VPN. Moving devices to a new VPN requires a complete re-configuration of the APN name on every physical device.
- **Localization Risks:** When using eSIMs for localization in countries with permanent roaming restrictions, IoT customers often lose control over IP addresses and security policies as the device is handled as part of the local MNO partner's network.

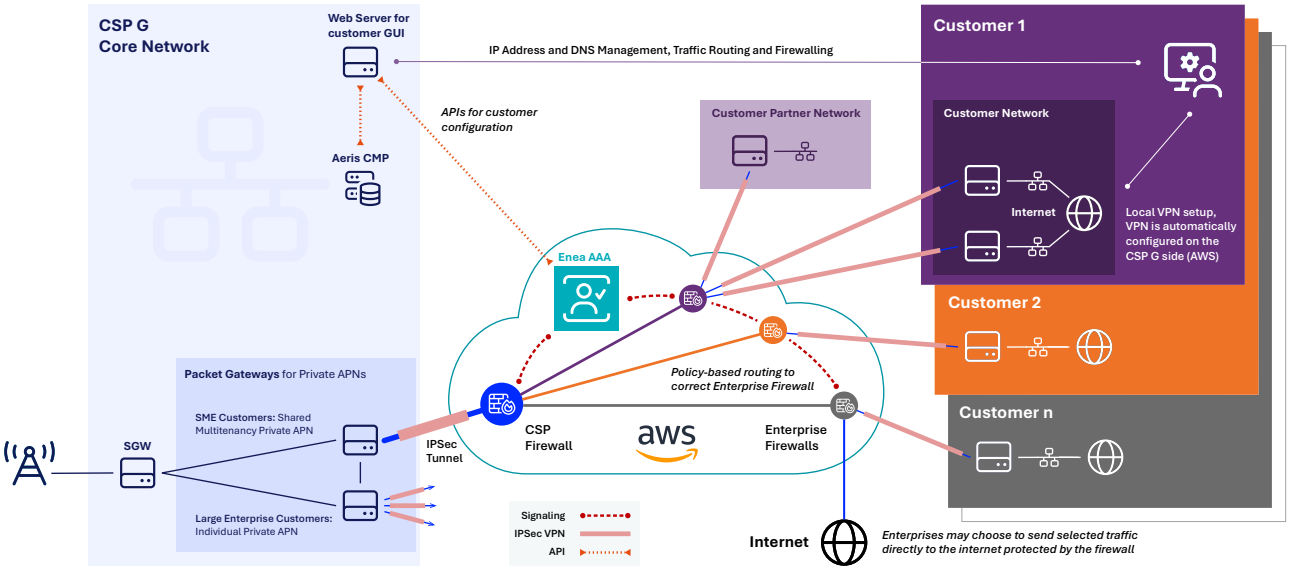
Furthermore, for the traffic going outside the Private APN directly to the internet, CSP G could previously only offer "blanket" firewall settings across all customers, rather than unique, per-customer security policies.

THE SOLUTION

Multi-tenant Private APN Innovation

To address these challenges, Enea offered its ICCF solution to CSP G leveraging the Enea AAA Server's built-in **Business Logic Engine** and **IP allocation through RADIUS.** This combination enables the **Multi-tenant Private APN** functionality—an industry-recognized Enea innovation that decouples the APN from the underlying VPN.

How it works

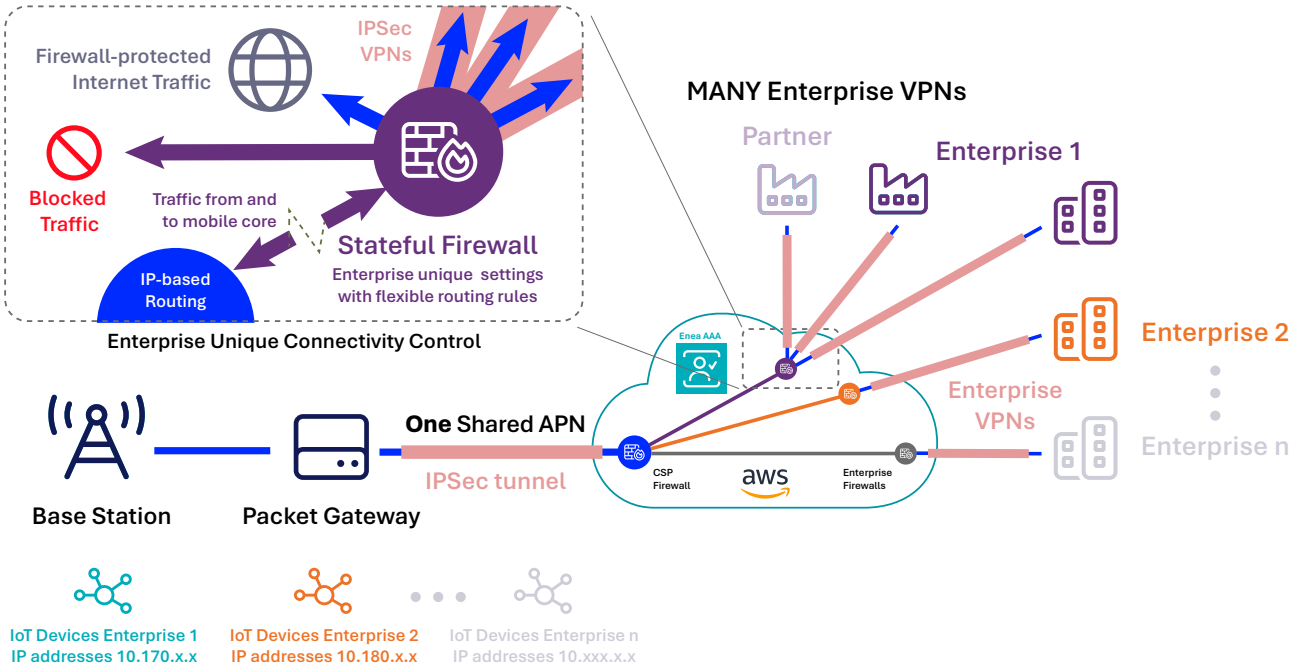


The Enea ICCF utilizes advanced **IP Address Management (IPAM)** and **Policy-Based Routing (PBR).** Because the Enea AAA is aware of which enterprise a specific IP address belongs to, it can intelligently route traffic to a dedicated **Enterprise Firewall** function within the ICCF solution.

One shared APN is routed to the Enea ICCF solution and then separated to many enterprises.

This allows thousands of independent enterprises to share a single APN while maintaining completely isolated security environments.

End Customer Self-Service Empowerment



Through a web-based self-service GUI provided by CSP G, IoT customers can directly manage their connectivity stack. While SIM management and related functions are handled via APIs to the Aeris CMP, the Enea AAA Server provides the underlying logic for:

- Software-Defined Traffic Routing to any Enterprise VPN destination or directly out to the internet, protected by the customer-unique Enterprise Firewall function.
- Custom Firewall Rules (Allowlists/Denylists and destination blocking).
- Automated Enterprise VPN Setup (reducing provisioning time from weeks to minutes).

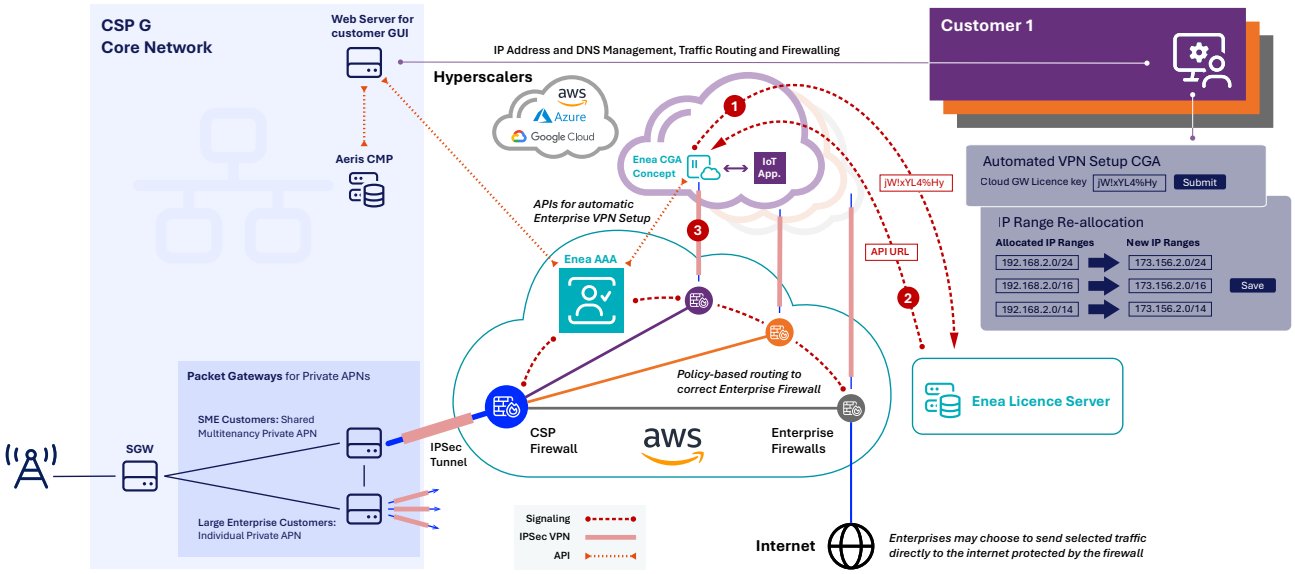
Key Comparison: Traditional APN vs. Enea ICCF:

Challenge	Traditional Private APN	Enea ICCF Solution
Setup Cost	High cost to maintain unique APNs at scale.	One shared APN for all SME customers.
VPN Provisioning	Manual setup; typically takes weeks.	Automated self-configuration in minutes.
VPN Scalability	1:1 relationship between APN and VPN.	Unlimited VPNs per customer.
Provide connectivity to partners	Since there can only be one Enterprise VPN, it is impossible to send selected traffic to a partner's Enterprise VPN.	With the support for multiple Enterprise VPNs, the partner can be included in what is more like a secure SD-WAN rather than a Private APN.
Device Re-config	Required if moving to a new VPN.	No re-config needed; APN name stays the same.
Firewall Control	Generic settings for all customers.	Dedicated firewall function per enterprise.
Localization	Loss of control to local MNO partners.	Consistent IP/Security via ICCF interworking.

Potential Future Extension for CSP G: The Enea IoT Cloud Gateway Appliance (CGA)

While the current ICCF solution successfully automates the CSP's side of the VPN connection, the enterprise customer is still responsible for configuring their own network endpoint. To address this final stage of complexity, Enea has developed the **IoT Cloud Gateway Appliance (CGA)** concept—a strategic innovation designed for hyperscalers such as AWS, Microsoft Azure, and Google Cloud.

This roadmap concept, which has been well received by CSP G and other IoT connectivity customers aligns with the significant trend of enterprise customers migrating their IoT application backends to the cloud. The CGA is designed to facilitate true **100% Zero-Touch Provisioning (ZTP)** by providing a pre-configured, cloud-ready appliance that can be instantly deployed within the customer's hyperscaler environment.



How the CGA Concept Will Work:

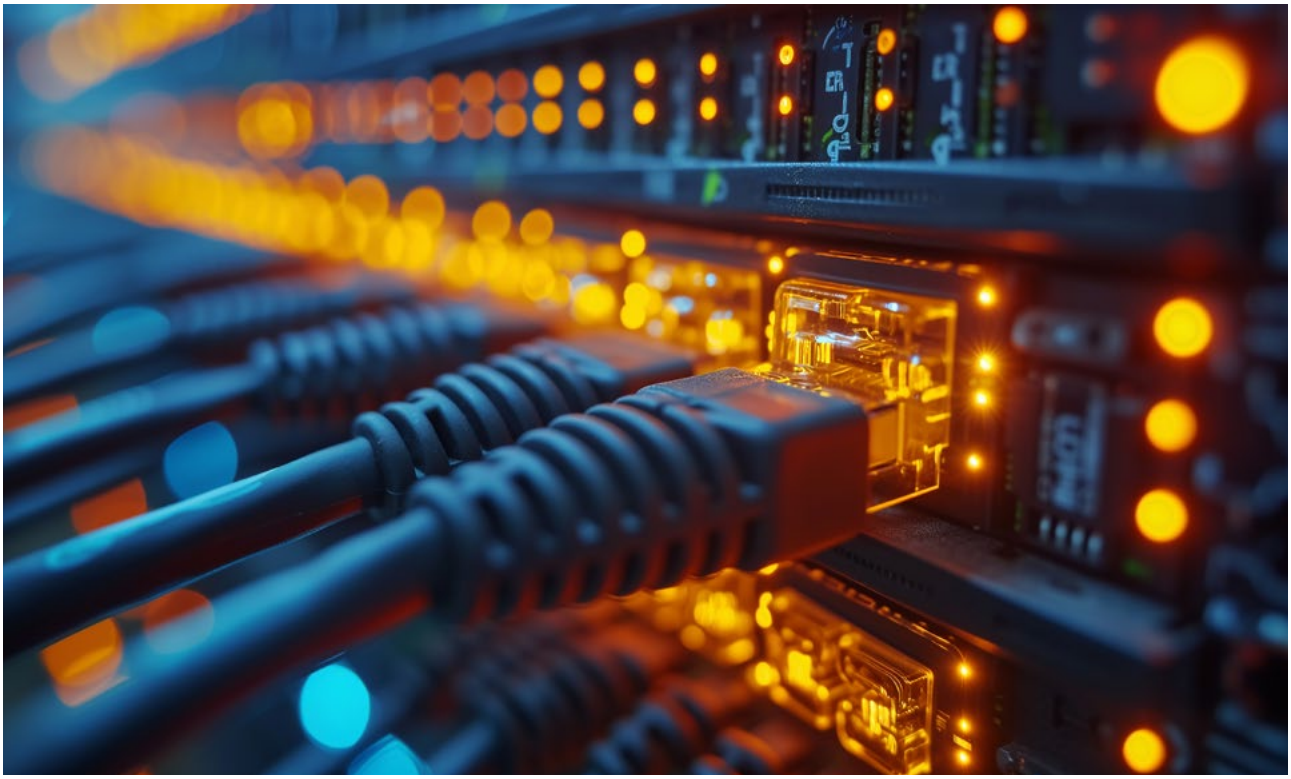
1. **License Allocation:** The CSP provides a CGA license key to the enterprise administrator.
2. **Instant Deployment:** The enterprise installs the CGA in their target cloud environment.
3. **Automated Activation:** Upon startup, the CGA validates the license key via the Enea License Server (1), which then replies with an API URL (2) triggering the Enea AAA Server API to automatically establish the VPN tunnel.

By introducing this concept, Enea is demonstrating a clear path toward a fully automated, SD-WAN-like experience for cellular IoT, where the VPN configuration is completely eliminated for the enterprise customer.

CSP H - LARGE ASIAN BROADBAND OPERATOR

Intelligent IP Address Management

CSP H, a large Asian broadband operator, leveraged the built-in IPv4/v6 DHCP server and business logic engine in Enea AAA Server to create an Advanced IP Address Management (IPAM) function tailored to their unique requirements. At the same time CSP H replaced its legacy systems for AAA and policy management with the Enea platform. Here we will focus on the IPAM aspect.



THE CHALLENGE

Legacy DHCP Server Couldn't Keep Up with IPv6 Requirements

The CSP H access network had grown organically over many years. Different regions used different operational models, subscriber databases, and address management practices. IPv4 services were delivered through a mixture of legacy DHCP platforms and locally managed address pools, while IPv6 deployment had been introduced incrementally through separate DHCPv6 systems tied to specific access vendors and Broadband Network Gateway (BNG) generations. Subscriber policy and authentication were handled independently by AAA infrastructure with limited integration to address allocation.

As subscriber growth accelerated and IPv6 adoption expanded, operational complexity increased significantly.

The operator faced several persistent problems:

- **IPv6 address planning** was fragmented across regions and access platforms.
- **DHCPv6 allocation behavior** differed between vendors and operational domains.
- **IPv6 Prefix Delegation**, where a client such as a home router, gets an IPv6 range and in turn allocates public IPv6 addresses to attached devices, were difficult to standardize.
- **Subscriber traceability** required correlating logs across multiple systems.
- **High availability was challenging** depending on manually managed failover procedures.
- **Scaling DHCP infrastructure** required increasingly complex pool partitioning and operational coordination.
- **Expanding address ranges** or introducing new subscriber policies frequently required maintenance windows.

The legacy DHCP servers, with two nodes in a primary-secondary configuration, suffered from the well-known 'split brain' issue where both nodes could consider themselves as the primary node if the connection between them was broken. Since they were optimized for performance, with only an in-memory database, the state of allocated IP addresses could in certain circumstances be lost all together. With IPv4 this had been a tolerable design flaw since the state in most cases could be re-established indirectly through RADIUS communication with the BNGs.

But with extensive usage of dual-stack IPv4/IPv6 came new requirements, especially with IPv6 Prefix Delegation. With IPv6 Prefix Delegation, re-establish state became too complicated, so CSP H looked for a 'split-brain-safe' DHCP function. Furthermore, CSP H business side had come with more advanced requirements related to IP management which pointed towards a more intelligent policy-based IP allocation approach with a hierarchical structure rather than the current flat structure.

THE SOLUTION

Policy-Based IP Allocation at the Network Edge

Traditional IP Address Management (IPAM) often relies on standalone DHCP servers that operate in isolation from subscriber identity. By integrating a **IPv4/v6 DHCP** Server directly into the **Enea AAA Server**, the process of assigning an IP address is transformed from a basic network function into a **policy-driven event** orchestrated by the **Business Logic Engine.**

> **The Enea AAA Server's built-in DHCP capability represents a shift from static IP assignment to Intelligent IPAM, where the Business Logic Engine ensures that every IP allocation is a policy-enforced decision.**

Key Strategic Advantages

1. **The "Single Source of Truth":** This approach ensures 100% synchronization between a subscriber's identity and their assigned IP. This is vital for Lawful Intercept (LI), accurate billing, and troubleshooting.
2. **Policy-Based Precision:** Unlike standard DHCP servers, the Enea Business Logic Engine can drive IP allocation based on real-time criteria such as:
   - **Subscriber Segment:** Assigning different IP pools for Consumer, Corporate, or Wholesale users. No allocation for subscribers on deny-lists (payment pending, banned etc.).
   - **Network topology and regions:** The IP allocation logic had to consider from what network equipment and region the DHCP request originated.
   - **Prefix IPv6 Delegation:** Is the client, e.g. a Home router, entitled to get a whole block (prefix) of IPv6 addresses (e.g., a /56 or /64 prefix) to provide IP allocation for attached devices? If so, what prefix size?
   - **DNS parameters:** Customized DNS settings for different subscriber types.
3. **Hierarchical IP-Allocation structure:** Facilitates administration across different user groups and locations.
4. **Lower Signaling Latency:** Co-locating DHCP with AAA eliminates the "extra hop" to an external server. The IP is assigned the moment the subscriber is authorized, reducing the **Time-to-Online**.

The operator also wanted to modernize its architecture toward active-active regional operation, eliminating the 'split-brain' issues, while preserving strict operational control over address ownership and subscriber policy.

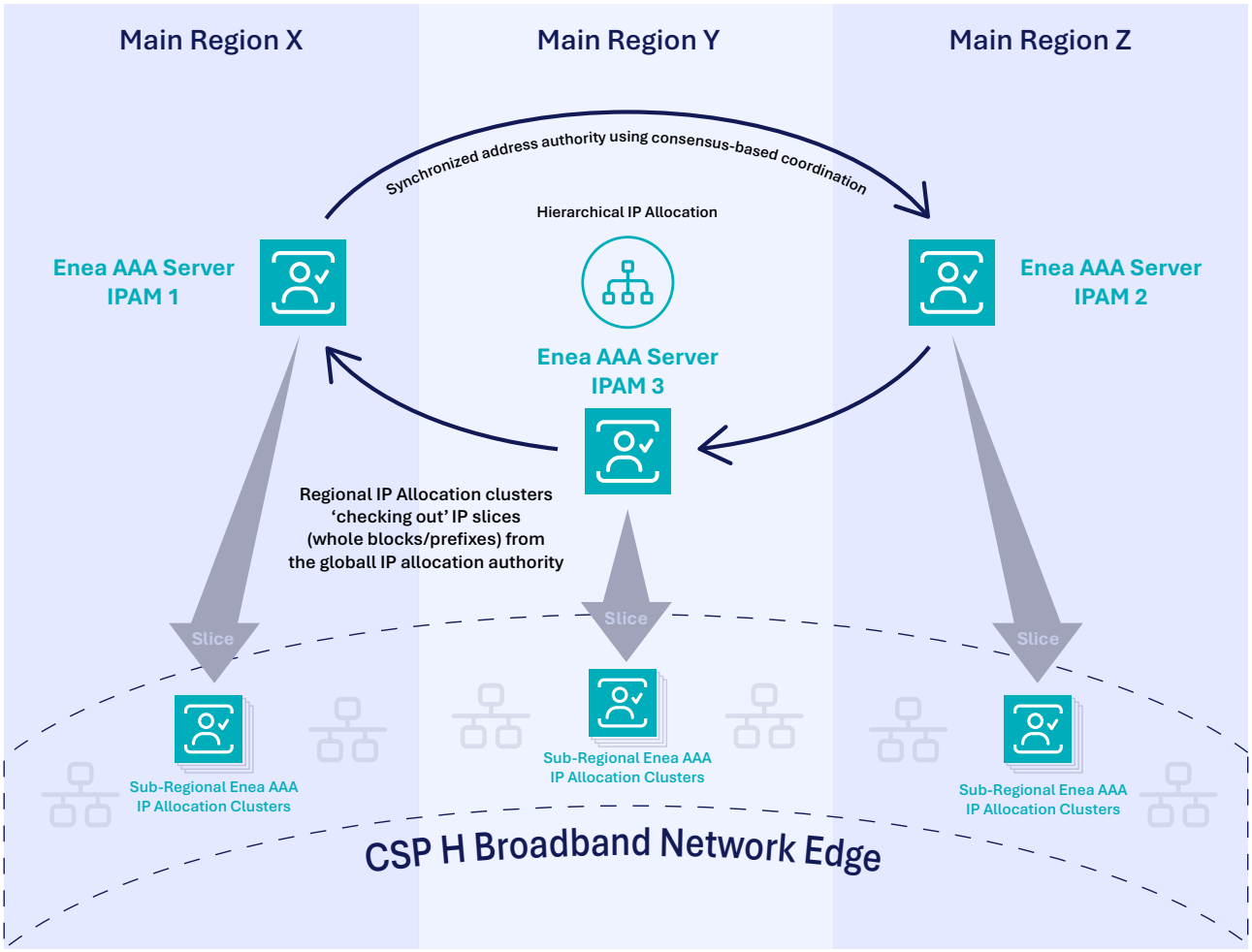
At the core of the deployment was a consensus-based distributed IPAM architecture. Instead of relying on isolated DHCP servers with locally managed pools, the new system established a globally authoritative hierarchical allocation model aligned with CSP H's network topology.

Address space was organized hierarchically according to the operational structure:

- Region,
- BRAS / BNG,
- Subscriber Segment,
- and Service Policy.

This hierarchy allowed the operator to directly map address ownership to the physical broadband network while maintaining clear aggregation boundaries for routing, operations, and reporting.

The system introduced delegated regional allocation clusters located close to broadband edge infrastructure. Regional allocators received delegated IP allocation slices from a globally synchronized address authority using consensus-based coordination.



This architecture solved two major problems simultaneously:

1. **Regional IP Allocation:** Local subscriber allocations could be performed with very low latency and high scale.
2. **Global Address Ownership:** IP coordination remained strictly consistent and conflict-free across the entire network.

Unlike the previous DHCP failover mechanisms, which relied on split pools and asynchronous lease replication, the new platform provided deterministic allocation guarantees through **distributed consensus**. This eliminated duplicate allocations during failover scenarios and enabled true active-active operation across geographically redundant sites.

CSP H no longer needs to statically partition address pools between servers or regions. Instead, allocation capacity expands dynamically as regional clusters request additional delegated slices from the global hierarchy. Address utilization has improved significantly, while operational overhead associated with manual pool management has been greatly reduced.

Integrated AAA capabilities further simplifies operations. Subscriber identity, authorization policy, IPv6 prefix delegation behavior, and service classification are now evaluated within a single policy framework.

The Enea AAA's integrated DHCPv6 engine supports both IA_NA (Identity Association for Non-Temporary Address) for WAN connectivity and IA_PD (Identity Association for Prefix Delegation) for residential networking. By utilizing the Business Logic Engine, CSPs can dynamically manage prefix sizes based on subscriber profiles, ensuring efficient address utilization.

Relay metadata from BNGs — including relay link-address, Interface-ID, and subscriber identifiers — allowed the Enea AAA Server to automatically determine the correct allocation hierarchy and subscriber policy for each request.

This enabled consistent enforcement of:

- **Segmentation:** Residential versus business and wholesale policies.
- **Service-level IP Pool Selection:** Dynamically assigning subscribers to specific IP pools that trigger distinct contention ratios and QoS priorities within the network core.
- **For IPv6:** Identity Association for Non-Temporary Access - IA_NA (home router's IP) versus Identity Association for Prefix Delegation - IA_PD (the home network block) allocation behavior.
- **Topology-aware prefix** delegation strategies.

CSP H also gains much stronger subscriber traceability. Because address management, lease state, and subscriber identity are unified within the same distributed system, operational teams can quickly correlate subscriber sessions, delegated prefixes, access nodes, and authentication records without stitching together data from multiple legacy platforms. This simplified tracking for regulatory compliance.

From an operational perspective, one of the largest improvements is the elimination of maintenance-related service disruption. Address ranges can be expanded dynamically within the hierarchy without interrupting active subscriber sessions. New BNGs and regional access domains could be introduced simply by extending the address hierarchy and policy tree rather than deploying isolated DHCP infrastructure.

The new Enea IPAM solution provides:

- Geo-redundant active-active operation.
- Topology-aware hierarchical IPv6 management.
- Low-latency regional IP allocation.
- Integrated subscriber policy control.
- Carrier-grade fault tolerance.
- Unified architecture designed specifically for large-scale broadband networks.

For CSP H, the transition was not merely a DHCP replacement project. It became a foundational modernization of subscriber identity, address management, and broadband service control for the IPv6 era.

About Enea

Enea is a global specialist in advanced telecom and cybersecurity software, with a vision to make the world's communications safer and more efficient. Through continuous innovation, our solutions help customers optimize, secure, and monetize their global communication services, enabling seamless connections between people, businesses, and connected devices worldwide. We serve 300 customers across 100+ countries, including telecom operators, cloud communication providers, governments, and cybersecurity vendors. More than 3 billion people rely on Enea technologies every day. Headquartered in Stockholm, Sweden, Enea is publicly listed on NASDAQ Stockholm.

For more information: www.enea.com

Author
Johan Terve, Senior Director Marketing, Enea

Contributors & Reviewers:

Jonas Andén, Director Managed Service and Support

Marko Ergotić, Senior Software Architect

Martin Hedenfalk, Senior Solution Architect and Engineering Teamlead

Jonas Lagerquist, Director Product Management

Josip Medved, Senior Solution Architect

Nikolina Pepić, Senior Software Architect

Juan Carlos Reynoso, Director Technical Sales & Delivery

Andrew-Jay Séguin, VP Tribe Data Management Applications

Pontus Söderström , VP Tribe Service Management Platform

ENEA