



Open Source Telecom Signaling

PAiCore Technology SMS Signaling Firewall

Reigniting telecom innovation and sustainable profitability via open source signaling solutions



SMS Signaling Firewall

Product Overview

The PAiCore SMS Signaling Firewall secures telecommunications infrastructure by neutralizing signaling threats at the interconnect edge. Operating inline at the SCCP layer of the SS7/SIGTRAN protocol stack, the platform intercepts unauthorized signaling queries and malicious routing attempts before they reach the core network or compromise subscriber data.

Designed specifically around the GSMA FS.11 specification for messaging security, the firewall enforces a zero-trust, five-stage decision chain on all incoming interconnect traffic. By validating originating identities, filtering unauthorized Mobile Application Part (MAP) operations, capping transaction rates, and detecting subscriber harvesting behaviors, the SMS Signaling Firewall protects subscriber privacy against tracking and spoofing while securing operator interconnect revenue.

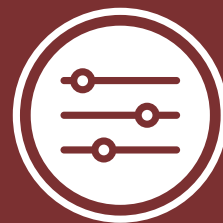
Key Features



GSMA FS.11 Standard
Compliance



Own-GT Anti-Spoofing
& Partner Screening



Category 1 MAP
Operation Filtering



SRI-SM / MT-FSM
Harvesting Detection

Use Cases

Subscriber Identity & Location Privacy Protection



Prevents unauthorized location tracking and stops malicious actors from harvesting subscriber IMSIs or monitoring user movements across interconnect routes.

Interconnect Revenue Protection & Perimeter Security



Neutralizes grey routes, invalid-origin routing, and unagreed interconnect queries by restricting signaling access strictly to authorized roaming partners and compliant operation limits.

SMS Signaling Firewall Features



Origin & Entitlement Verification

Own-GT anti-spoofing plus a deny-by-default partner allowlist confirm every message is from who it claims to be, and that a roaming agreement exists.



Partner Allowlist & Deny-by-Default Control

Restricts incoming interconnect traffic exclusively to declared roaming partners using strict Calling Party Address (CgPA) prefix matching, rejecting unauthorized origins immediately.



Category 1 Operation Blocking

Blocks high-risk Mobile Application Part (MAP) operations (such as profile modifications or IMSI/location retrievals) that lack explicit bilateral agreements, inspecting multi-component messages to eliminate evasion attempts.



Per-Origin Rate Limiting

Caps transaction frequencies per origin GT and operation code (opcode) to prevent high-speed network sweeps, utilizing memory-bounded token bucket structures to mitigate application-layer signaling floods.



Behavioral Anomaly Detection

Flags the SRI-SM / MT-FSM query-to-delivery ratio that exposes subscriber identifier harvesting disguised as ordinary routing traffic.



Subscriber Identity Protection via SMS Home Routing

Integrates alongside PAiCore SMSC to service routing queries in place of the HLR/HSS, replacing sensitive subscriber IMSIs and serving MSC addresses with temporary Correlation IDs in compliance with 3GPP TR 23.840.



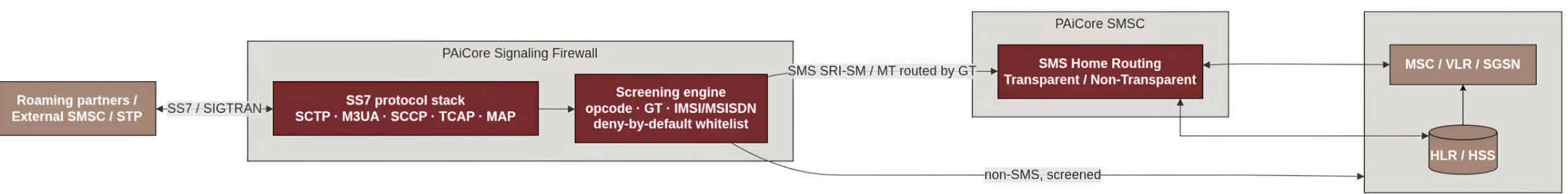
Open Source Telecom Signaling

Appendix – Technical Information



Architecture & Interconnection

The firewall operates transparently as a Signaling Transfer Point (STP) with security logic, intercepting traffic at the Global Title Translation (GTT) hook of the SCCP layer. Permitted traffic is forwarded directly, preserving end-to-end dialogue correlation without adding per-conversation state.



How It Works: The Decision Chain

Every message is evaluated inline, in a fixed, deny-by-default order. The first rule that fires short-circuits the chain and decides the outcome, no rule firing means the message is allowed through untouched

Step	The Question	Technical Rule	Condition	Verdict / Action
1	Is it who it claims to be?	Own-GT Anti-Spoofing	CgPA in home operator range arriving from interconnect	DROP
2	Does it have an agreement?	Partner Allowlist	CgPA does not belong to a declared partner	REJECT
3	May it ask that?	FS.11 Category 1	Blocked opcode without bilateral exception	REJECT
4	At what rate?	Rate Limiting	Transaction limit exceeded for (CgPA, Opcode)	DROP
5	Does it make sense?	SRI-SM / MT-FSM Ratio	Harvesting/inventorying pattern detected	ALERT / DROP / REJECT
Default	No rule fixed	Default Pass	Traffic satisfies all security controls	ALLOW