



Open Source Telecom Signaling

Release Notes

for SMSC CT Edition v3.1.0+cte

Reigniting telecom innovation and sustainable profitability via open source signaling solutions



SMSC

CT Edition v3.1.0+cte Release Notes

Continuous innovation remains at the core of PAiCore Technology, and this new release of the SMSC Core Technology (CT) Edition v3.1.0+cte delivers a significant leap in performance, reliability, and routing precision.

At its core, this version introduces advanced traffic orchestration, an even more intuitive management interface, AI-powered SMS protection, and superior traceability through enhanced CDR reporting and real-time logging.

LATEST VERSION: v3.1.0+cte
RELEASE DATE: April 21, 2026
IMPROVEMENTS: 12

Enhancements & New Features vs Previous Version

- **Advanced Message Priority Management**

- **Multi-Protocol Priority Queues:** Dedicated **High**, **Medium**, and **Low** priority queues are now integrated across SMPP, HTTP, SS7, and Diameter gateways, enabling precise traffic segmentation and delivery.
- **Dynamic Throughput Reallocation:** A new scheduling algorithm ensures maximum resource utilization. If high-priority traffic is below its quota, the system automatically reallocates available throughput capacity to lower-priority queues. This ensures the SMSC consistently maintains 100% of the configured **Messages Per Second (MPS)**.

- **AI-Powered SMS Protection:**

- Integrated **OpenTextShield**, an advanced security layer leveraging the Multilingual BERT (mBERT) architecture. This enables real-time, **AI-driven** detection of **SMS spam** and **phishing** attempts across 104+ languages.

- **UI/UX & Operational Enhancements**

- **Service Provider Management:** Configuration for SMPP and HTTP Service Providers has transitioned from modal overlays to **dedicated full-page** views. This expansion provides a more robust environment for managing complex parameters and improves overall navigation.
- **HTTP Custom Parameters:** HTTP Service Providers now support default custom parameter configurations, allowing outbound messages to be automatically populated with required provider-specific values.
- **Log Analysis Filtering:** To streamline troubleshooting, the "Analyze Logs" module now **defaults to a full-day view** (00:00:00 to 23:59:59) instead of the current server time. This provides immediate visibility into the day's activity without requiring manual filter adjustments.

- **Signaling & Message Handling**

- **Configurable Message Reference Length:** Introduced a toggle to switch between **8-bit** and **16-bit** message references during the concatenation (split-message) process. This ensures that all partitioned messages—whether via HTTP or SMPP (TLV payload)—strictly follow the configured reference logic, guaranteeing **reassembly integrity** and **consistent delivery during retry** cycles.
- **Custom DLR Data Coding Scheme (DCS):** Added a configuration flag to define a **default Data Coding Scheme (DCS)** for SMSC-generated Delivery Receipts, ensuring encoding compatibility across diverse service providers and gateways.

- **Broadcast Module Improvements**

- **Executor Tracking:** Introduced an execution tracking field within the campaign list, providing full auditability by identifying the user responsible for each broadcast.
- **Provider Access Control:** Implemented provider-level permissions, enabling administrators to enforce routing restrictions by mapping specific Service Providers to user during onboarding.
- **Fixed Sender ID:** Enabled dedicated Sender ID assignment, ensuring users are restricted to pre-authorized identifiers within the Broadcast module.

Enhancements & New Features vs Previous Version

- **CDR & Reporting Enhancements**

- **Friendly Name Identification: CDRs** now feature **Friendly Account Names** alongside Network IDs, significantly improving the readability and traceability of message records.
- **CDR Logging Accuracy:** Improved the reliability of CDR reporting by ensuring that failed delivery attempts correctly reflect the specific destination ID involved, even when a subsequent retry through a different route is successful.