Enabling Lawful Interception for Fraud Detection Across Mobile and Fixed Networks with Cubro EXA64100

CASE STUDY

Published at Cubro, September 2025

Please refer to the latest version of this document on our website to ensure you have the most up-to-date information.

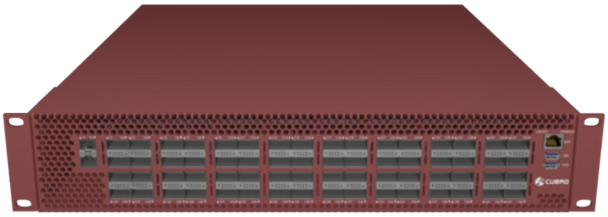
Industry » Service Provider

Executive Summary

Fraudsters often use mobile phones, fixed-line calls, or instant messaging apps to target victims. To detect and stop them early, authorities needed a way to analyse communication patterns across the country's telecommunications networks.

Cubro's EXA64100 provides a robust, compliant and scalable foundation for national fraud detection systems. Standardising data collection across mobile and fixed-line networks enables telecom operators, government agencies, and system integrators to work together efficiently, ensuring effective fraud detection while maintaining full regulatory compliance.

Overcoming CDR Collection and Compliance Challenge in Lawful Interception



Cubro EXA64100

- Data collection: The system needs to collect Call Detail Records (CDRs) from three major telecom providers (both mobile and fixed-line).

- Fraud detection: CDRs are to be forwarded to the law enforcement big data analysis system, where suspicious behaviour can be identified.

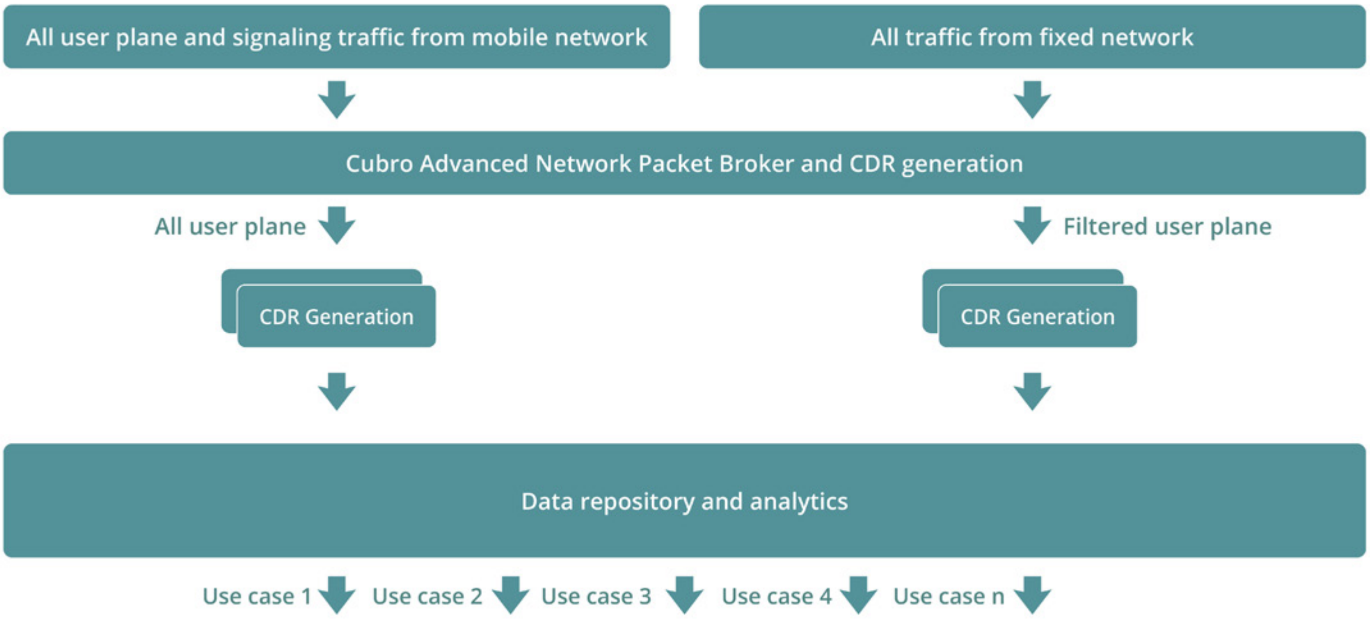
- Role of telecoms: Telecom companies are responsible for creating the CDRs; they will not store or process the data.

Roles and responsibilities

Three parties are involved in the Legal Interface. Telecom providers provide the data, Cubro distills the data into CDRs, and authorised government agencies store and analyse the data.

Party	Role
Telecom Providers	Allow access to the mobile and fixed network for Cubro. Provide fixed network point codes and Circuit Identification Codes (CICs).
Cubro	Distill raw network traffic into standardised CDRs; ensure accurate field population; guarantee secure and compliant CDR delivery to government systems.
Authorised government agencies	Access CDR data for analysis, fraud detection, and law enforcement, in accordance with legal mandates.

Cubro’s Solution with advanced network packet broker EXA64100


All user plane and signaling traffic from mobile network
All traffic from fixed network
Cubro Advanced Network Packet Broker and CDR generation
All user plane
Filtered user plane
CDR Generation
CDR Generation
Data repository and analytics
Use case 1
Use case 2
Use case 3
Use case 4
Use case n

Cubro provided the EXA64100 Network Packet Broker (NPB) as the infrastructure backbone for this project.

- The NPB collects raw traffic from both mobile and fixed-line networks.
- Filters and formats the relevant data into CDR fields.
- CDRs are handed over to the government law enforcement big data system for analysis.

The telecom provider provided the corresponding fixed network point codes and Circuit Identification Codes (CICs), which Cubro used to accurately populate the CDR fields for the fixed-line communications. All collected data is stored in a standardised CDR format, ensuring uniformity across both mobile and fixed networks, as required.

Each CDR contains both mobile and fixed network fields. When a session is captured from a mobile network, the fixed network fields are left blank, and vice versa. While the system may capture large amounts of session data, including potentially irrelevant sessions, all data is retained. The big data system filters and identifies which sessions are actually relevant for fraud detection.

Cubro acts as a trusted partner for system integrators, providing responsive support to resolve technical challenges and simplify deployment.

Key Benefits of the Cubro Solution

1.High-performance data collection - The EXA64100 handles massive volumes of network traffic from multiple mobile and fixed-line networks without dropping data, ensuring all relevant sessions are captured.

2.Accurate CDR population - Cubro uses telecom-provided point codes and CICs to accurately fill all fixed-line fields, ensuring reliable data for analysis.

3.Compliance - Cubro enables lawful interception without mass surveillance, keeping telecom operators and authorities compliant with legal requirements.

4.Scalability and flexibility - The solution works for both mobile and fixed networks, and can adapt to new communication apps and fraud patterns.

5.Retention of all data for smarter analysis - Even seemingly irrelevant session data is captured and retained, allowing the big data system to filter intelligently, improving fraud detection accuracy over time.

6.Trusted partner for system integrators - System Integrators rely on Cubro to actively respond to technical challenges, making deployment faster and more reliable.