Network Forensics

LIMA Introduction

new needs need new solutions

Group 2000

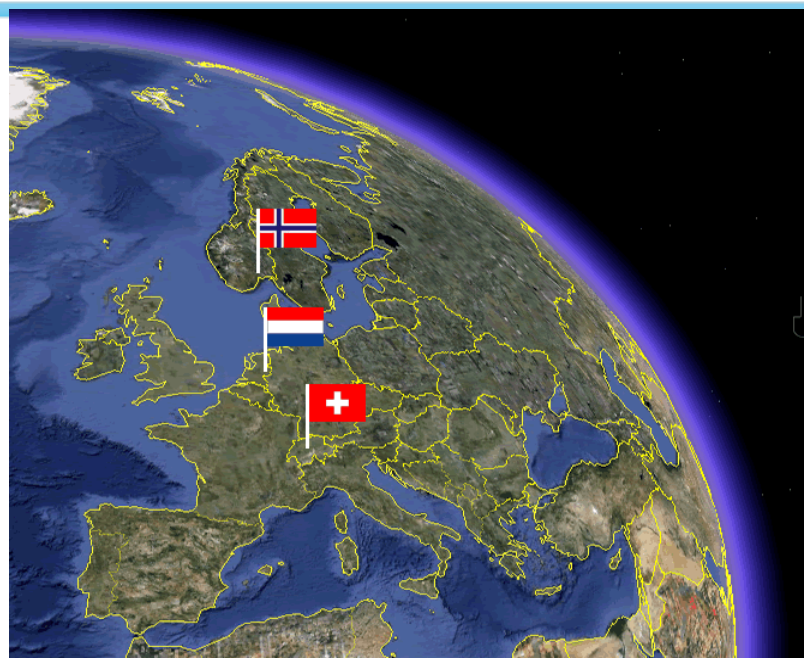
Founded in 1978

Independent, privately owned company

Stable financial position

70 employees

Headquarters in the Netherlands



Offices in the Netherlands, Norway, Switzerland and USA

In-house development and 24x7 Customer Care

ISO certified & full ETSI member

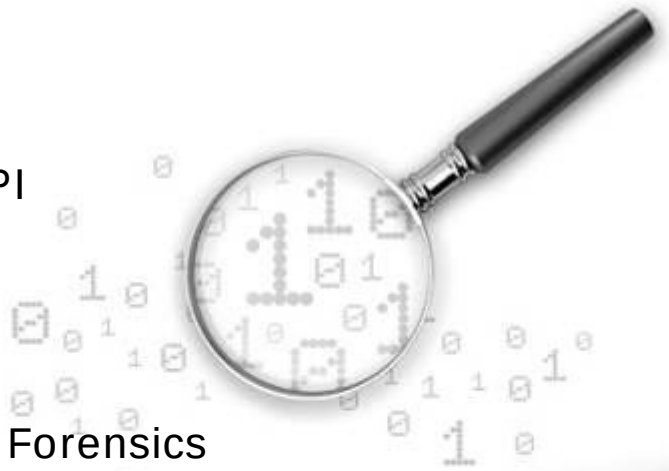
Group 2000 product lines

ICTS product line

- System integration at Telecom Operators
- Ample experience with major European operators
- Flexible and cost effective, yet telco-grade

Network Forensics product line

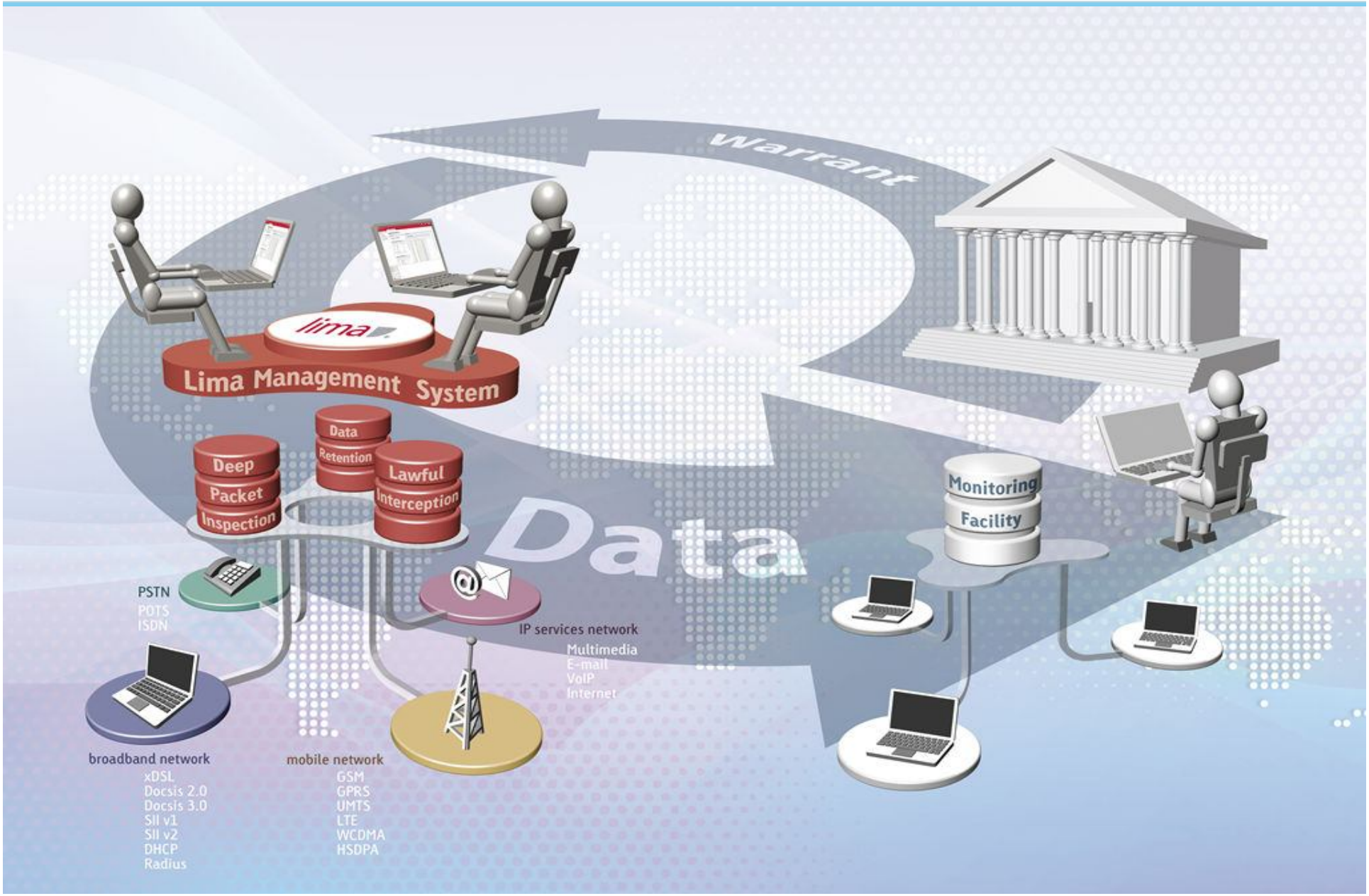
- Lawful Interception, Data Retention, DPI
- Experience > 20 years



LIMA

- Group 2000 platform suite for Network Forensics
- Deployed in > 20 countries at Telco's and ISP's

LIMA environment



LIMA configurations

Voice over IP

- AcmePacket Net-Net
- Cisco PGW 2200
- Cisco BTS 10200
- SipWise OpenSER
- Italtel iMSS
- Nortel CS2000
- Siemens HiQ 8000

LIMA configurations

GSM, GPRS, UMTS

- MSOFT X3000
- UMG 8900

- Nokia OLCM
- Nokia LIG

- LI-IMS

- LIMA GTP monitor

LIMA configurations

IP/SII – DHCP, Radius

ARRIS

CASA

cisco

Juniper NETWORKS

lima lawful interception®

Email

OPENWAVE

synacor

lima lawful interception®

LIMA configurations

PSTN

- Ericsson AXE
- Ericsson LI-IMS

- Nortel DMS 100

- SS7 monitor

IMS

P-CSCF, I-CSCF, S-CSCF
HSS, ATS, PES, AS
AGCF, SBC

LIMA Handover specifications

GSM	**ETSI TS 201 671 v2.5.1**
3G	**ETSI TS 201 671 v2.5.1 – Annex B** **TIIT v1.1.0** **ETSI TS 102 232** **3GPP TS 33.108**
GTP monitoring	**ETSI TS 102 232 v1.3.1** **IRI records according to ETSI TS 201 671 v2.5.1**
Circuit Switched	**ETSI TS 201 671 v2.5.1** **ETSI ES 201 671 v3.2.1**
IP VoIP Multimedia	**ETSI TS 102 232 v1.3.1** **ETSI TS 102 233 v1.2.1** **ETSI TS 102 234 v1.4.1** **ETSI TS 102 232-1 v2.2.1** **ETSI TS 102 232-3 v2.1.1** **ETSI TS 102 232-4 v2.1.1** **ETSI TS 102 232-5 v2.1.1** **ETSI TS 102 232-6 v2.1.1** **TIIT v1.1.0**
Email	**ETSI TS 102 233 v1.2.1** **ETSI TS 102 232-2 v2.1.1** **TIIT v1.1.0**

LIMA Platforms

LIMA Management System

- Unified LI Management for all types of traffic and networks
- Interfaces to network equipment to enable end-to-end interception
- Operator friendly interface; no network knowledge required for LI user
- Distributed setup; can be deployed across networks or countries

LIMA Mediation

- Converts intercepted traffic into handover standards (e.g. ETSI)
- Correlates intercepted events and data

LIMA Data Retention

Retention Store

- Third party technology for storage
- COTS hardware
- At least 20% compression rate
- Ingestion rates of 100+ million records/day

Integrated solution

- Module in LIMA MSv3
- ETSI HI-interface optional

LIMA MS v3

Web-based system for end-to-end control

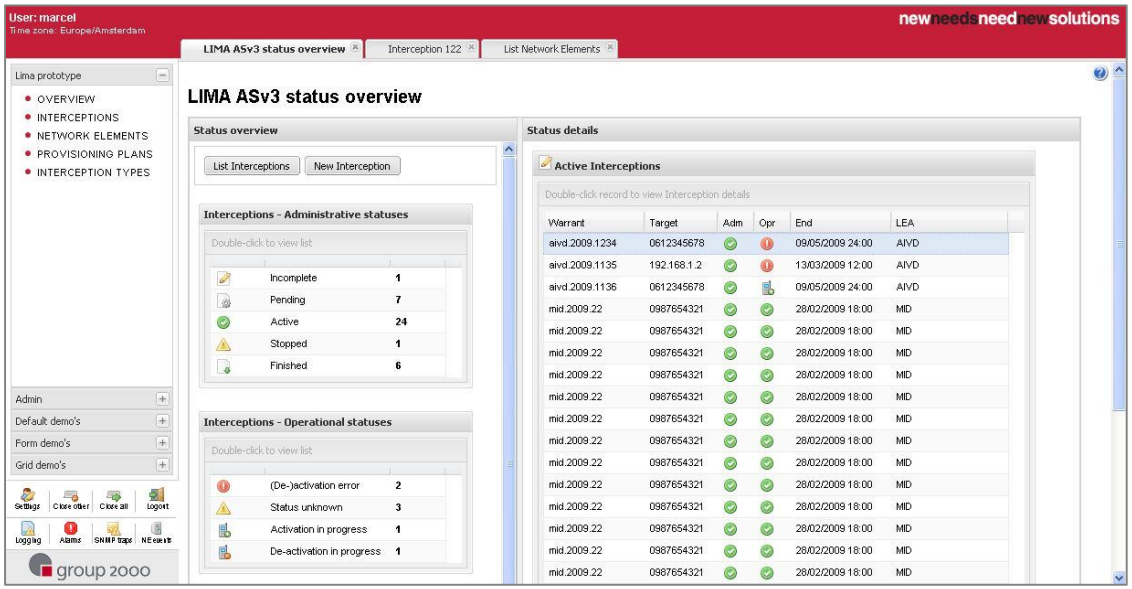
Warrant Administration

Network Element management

Automatic distribution

Integrity checking

Extensive logging
- IDR
- Events
- Alarms
- Auditing



LIMA MS v3

One solution manages all networks

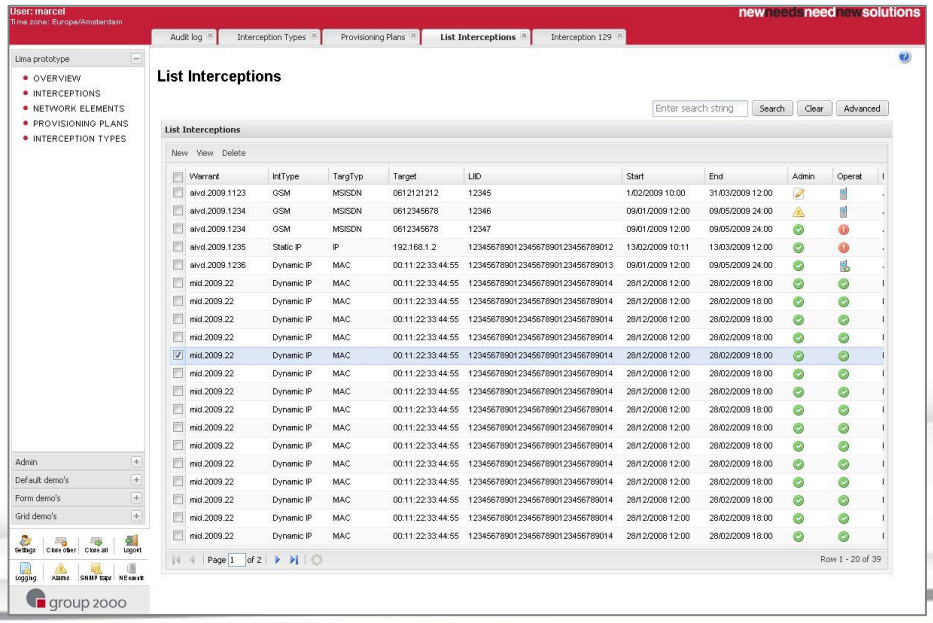
Simultaneous support for different types of interceptions

Easy to use interface

Clear status overview

Problem analysis by
drilling down into
details

Multi-lingual user interface



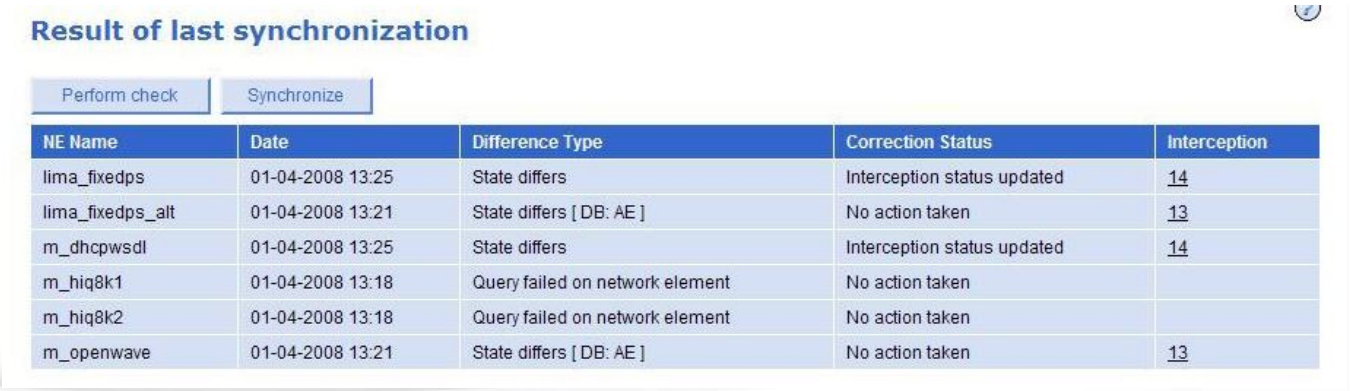
LIMA MS v3 integrity monitor

Interception integrity!

Monitor interceptions on network elements during their entire life time

On scheduled intervals interceptions are
checked against the LIMA MS database

Automatic repair of inconsistent interception measures



Result of last synchronization

Perform check | Synchronize

NE Name	Date	Difference Type	Correction Status	Interception
lima_fixedps	01-04-2008 13:25	State differs	Interception status updated	14
lima_fixedps_alt	01-04-2008 13:21	State differs [DB: AE]	No action taken	13
m_dhcpwsdl	01-04-2008 13:25	State differs	Interception status updated	14
m_hiq8k1	01-04-2008 13:18	Query failed on network element	No action taken	
m_hiq8k2	01-04-2008 13:18	Query failed on network element	No action taken	
m_openwave	01-04-2008 13:21	State differs [DB: AE]	No action taken	13

(sample screen)

LIMA MS v3

User Management based on Sun Open-SSO

Definition of users and user groups

Secure environment

Fine-grain control on access to data and functions for user groups

Security groups

Access to warrants can be shielded off between user groups

Possible to securely handle different sets of warrants in single system

Security and Auditing

Comprehensive audit logging

All actions of users and systems are recorded

Access to audit logging based on user rights

Direct and filtered access from GUI modules

- Interceptions
- Network elements

LIMA MS Distribution Layer

Intelligent Interception distribution

Provisioning of network elements, in the right order, with the right information, on the right time.

- All switches (e.g. GSM network)
- Only specific network elements (e.g. Fixed network)
- Handling of interception identifiers (e.g. generated by NE)
- Based on events (e.g. SIP call, DHCP lease)
- Adhere to Warrant Start and Warrant End Dates

Handles fault scenarios such as failing network elements or network connections

Intelligent repair of failing interceptions

Supports dynamic provisioning for dynamic network identities such as IP addresses based on DHCP, Radius or SIP information

LIMA MS Provisioning Modules

Provisioning modules

Interfacing LIMA Management System with 3rd party equipment.

- Softswitches (Huawei, Siemens, Nortel, Cisco, Ericsson, Italtel, ...)
- SGSN/GGSN (Nokia, Huawei, Starent, Ericsson, ...)
- CMTS 's (Cisco, Arris, Casa, ...)
- Mail Servers (OpenWave, Synacor, ...)
- SBC's (AcmePacket, ...)
- Edge Routers (Cisco, Juniper, ...)
- Class 5 switches (Nortel, Ericsson, ...)
- ....

Allow LIMA MS to interface with any network element

LIMA MS options

Optional modules for extension of functionality

Reporting and Statistics

Reports about number and types of interception

Provisioning interface

Allows LIMA MS to be controlled by external system (e.g. LEMF)

Electronic HI-1 interface

Digital interfaces for warrant handling (not applicable to all countries)

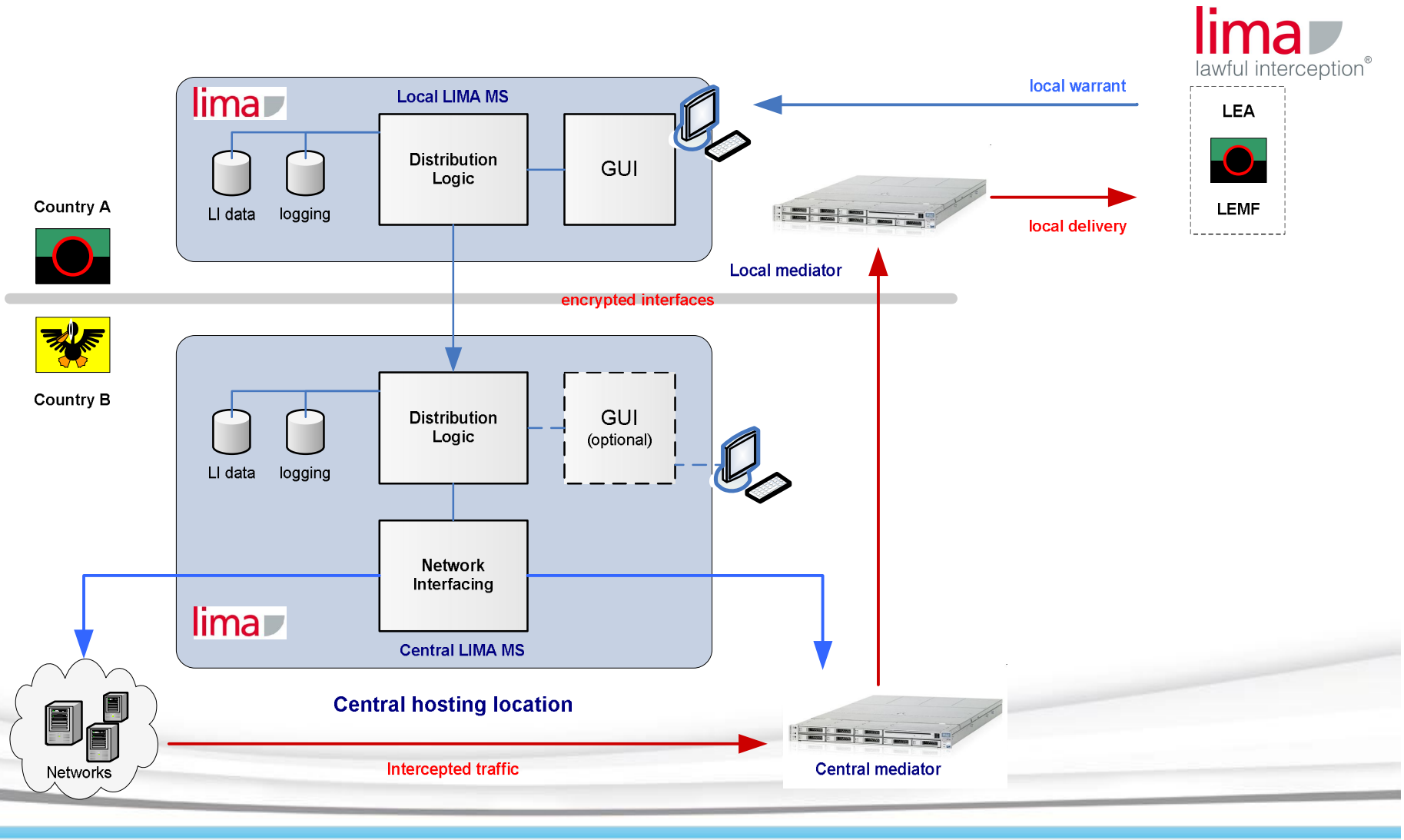
Billing

Automatic generation of invoices

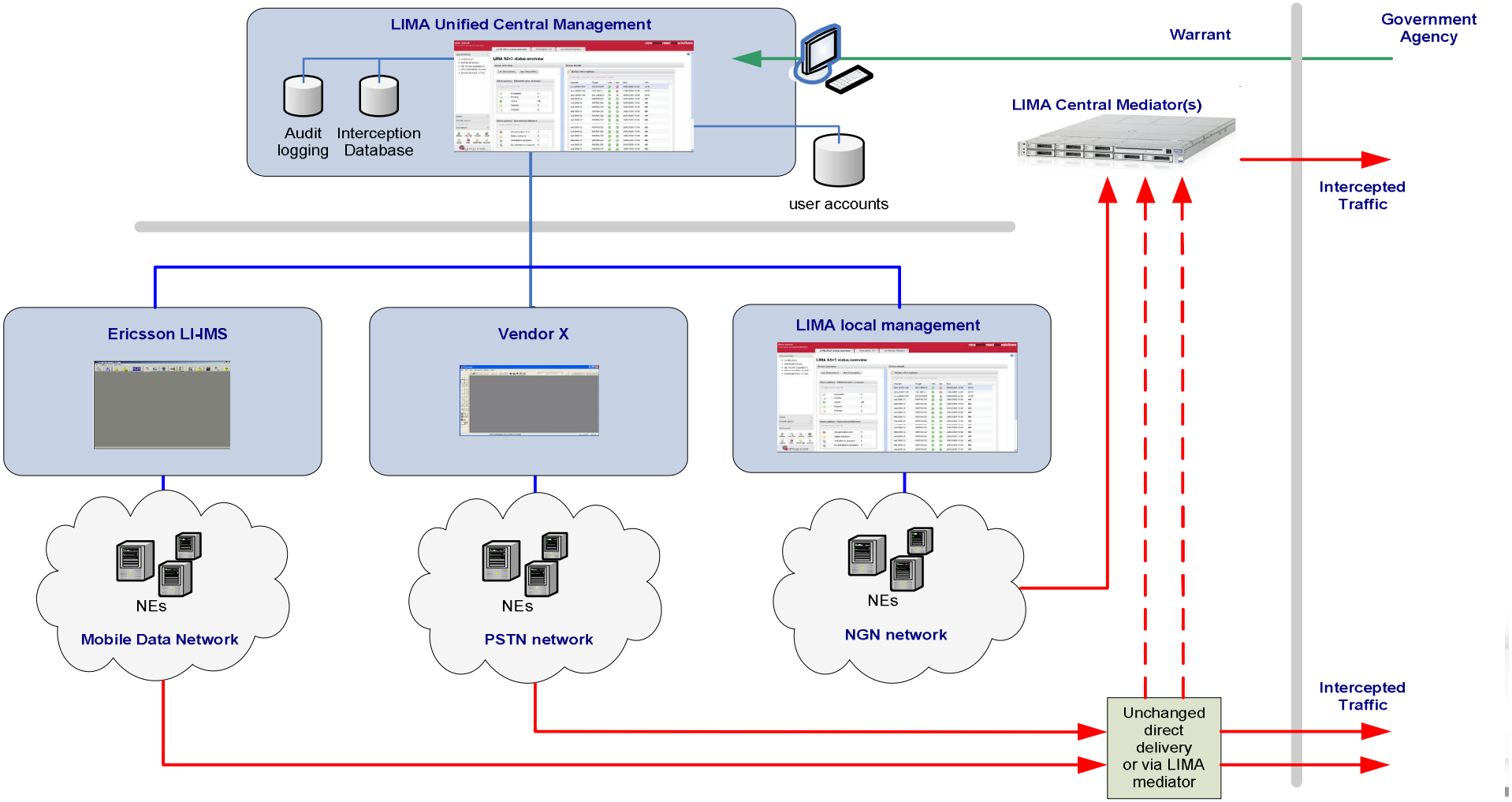
Customer specific configuration

Configuration of fields for specific value or lengths

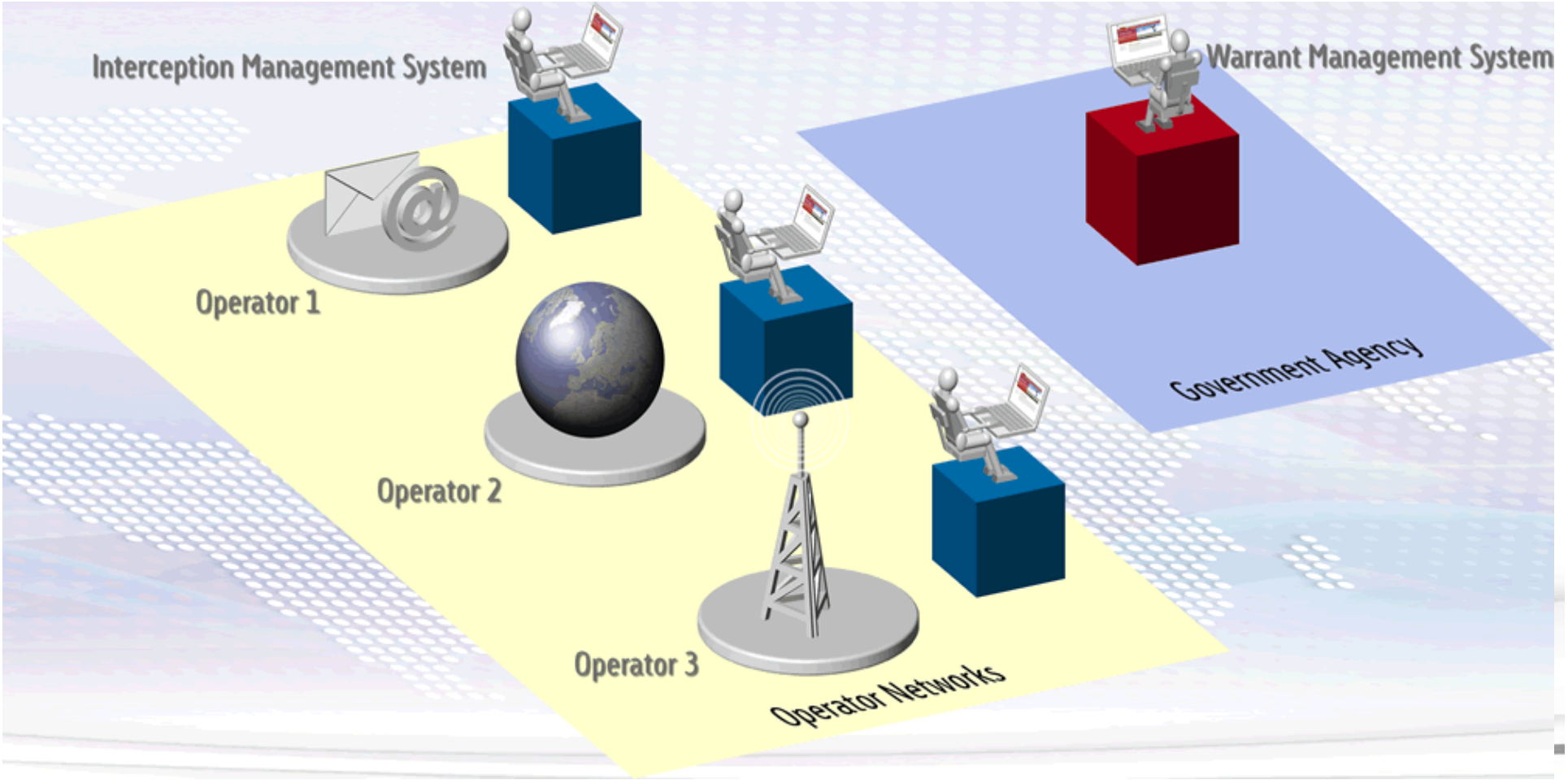
LIMA MS Cross country Deployment



LIMA MS – Unifying multiple networks



Distributed setup – government controlled



group 2000

Network Forensics

LIMA Introduction