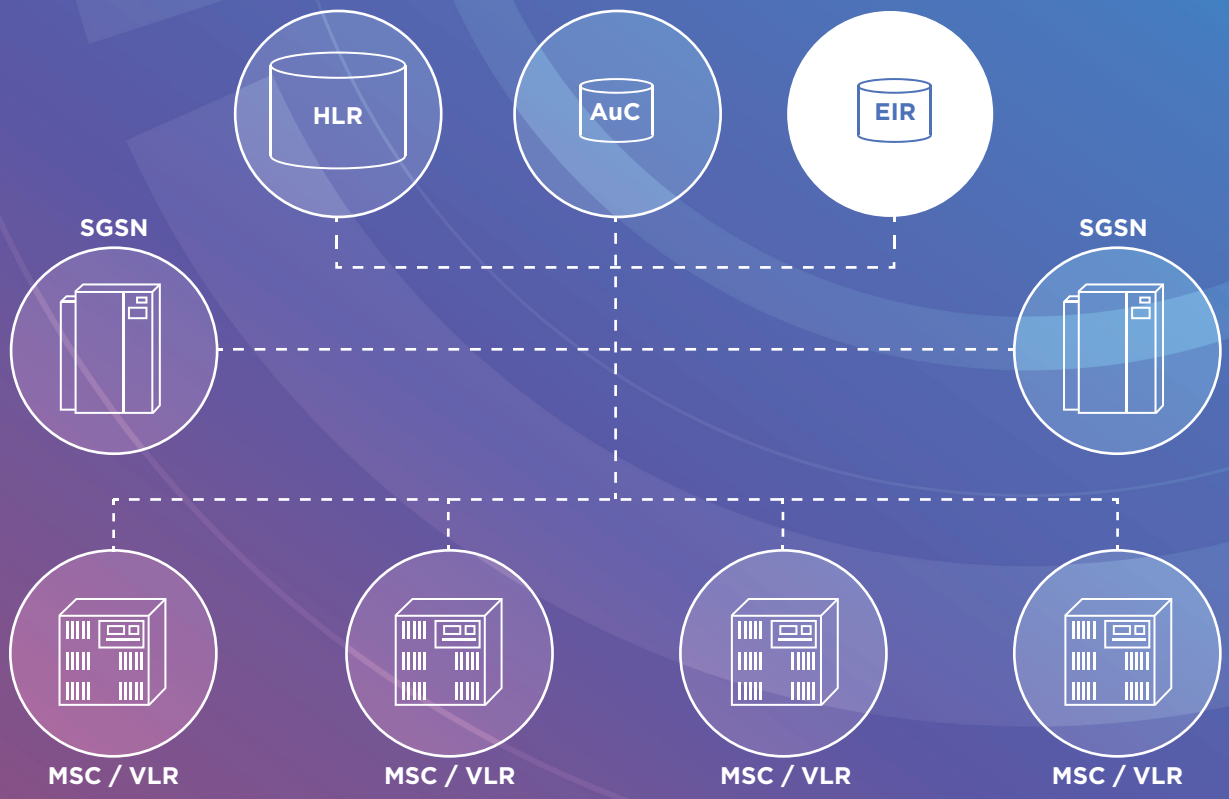
Network **Security** Solutions

PolyNet EIR
(Equipment Identity Register)
Where Security Meets Connectivity



EIR, or Equipment Identity Register, is a database used in telecommunications and mobile networks to store information about mobile devices, primarily their International Mobile Equipment Identity (IMEI) numbers. These databases enable network operators to verify the authenticity of IMEI numbers, thus ensuring that only authorized devices are allowed on the network. PolyNet EIR offers complete EIR functionality implemented in a dependable and customizable hardware and software framework to enhance the security and integrity of your mobile network.

Benefits

- **Security and network integrity:** Reduces the risk of compromised, counterfeit or non-compliant devices connect to the network
- **Customer protection:** Helps prevent the use of stolen or lost mobile devices, and detect device cloning for fraudulent purposes
- **Enhanced tracking and reporting:** Tracks and reports the location of devices with blacklisted PEI numbers, monitors device usage and detects suspicious activities
- **Better network performance:** By ensuring that only authorized devices connect to the network, PolyNet EIR helps maintain network performance and prevent congestion
- **Regulatory compliance:** Helps mobile operators comply with government and industry regulations and policies
- **Cost-effective and simple integration:** Requires minimal server room space, and its expenditure structure (CAPEX-OPEX) is customizable

POLYNET Perfect Timing

Network **Security** Solutions

PolyNet EIR Technical Data

Specifications

- Various black/white/grey lists can be configured for different service purposes
- Lists can contain standalone IMEIs as well as IMEI ranges
- Standalone IMEI number and/or range can be deleted/inserted from/into a certain list
- Both 14- and 15-digit IMEIs are handled
- Full handling of Check IMEI functionality
- Configurable triggers for alarms
- Functionality-related and transaction related logging and archiving
- Periodic IMEI Database backup
- Periodic reporting of transaction statistics. Separate statistics for hitting black, white and grey lists
- IMSI-dependent rules for screening the lists. Rules can be defined for IMSI prefixes to determine the sequence for searching IMEIs in lists
- For security and traceability purposes all subsystem communications and direct database / list interventions are checked and logged
- Custom-database is applied for 10x faster access than commercial DBs
- Central provisioning of clusters with loadsharing

Capacity

- Ten different IMEI lists - including “black”, “grey”, “white”, and “unknown”
- Altogether 50 million possible entries (IMEI ranges or standalone items) in the 10 IMEI lists
- 100 IMSI prefix rules to describe “IMSI prefix – IMEI” combinations
- Traffic capacity, SS7 on E1:
- Two bidirectional signaling links per card
- Each link handling 32 transactions/sec (calculating with 40% effective usage of a 64 kbps channel)
- One signaling card: 64 transactions/sec altogether
- Maximum 4 cards in one machine (PC); scalable
- The SS7 limitations do not apply for SIGTRAN. There is no practical transaction speed-limit for the application itself.

Configuration Requirements

A fully duplicated system requires two 19” industrial grade PCs, containing:

- redundant HDD (e.g. 160 GB SATA)
- redundant power supply
- passive motherboard with 6-10 slots to fit several SGA-47 cards
- active processor board
- processor: Intel Core2 Duo – or similar
- memory: 4 GB

For SS7 connections SGA-47 interface cards are required;
SIGTRAN connections can be handled by any industrial grade Ethernet cards.

PolyNet Telecommunications Consulting and Contractor Ltd.

Bojtar utca 17, Budapest, 1037 Hungary | Phone/Fax: +36 1 250 7726 | www.polynet.hu | Email: info@polynet.hu