

GSMK Oversight®
Signalling Network
Intrusion Detection & Analytics System

GSMK Oversight®

High-Performance Intrusion Detection and Analytics System

Protect your Signalling Network's Achilles Heel.

With the technical foundation of the SS7 protocol going back to the 70s, today's increasing network complexity and the transition to new signalling technologies like Diameter and GTP still require strict policies and new tools to prevent fraud, hijacking or service disruption and espionage.

Oversight® is an essential part of your state-of-the-art signalling network management and allows high-performance live analytics and threat management of interconnect traffic across signal transfer points, diameter agents, GTP firewalls, carriers, and signalling technologies.

Inherent system vulnerabilities of SS7, Diameter and GTP have recently been publicly exposed, opening the door for systematic violation on a global scale.

Basic filtering or firewalling of SS7, Diameter and GTP interconnect messages to counteract intruders is neither sufficient for protecting operators from the financial impacts nor can it guarantee the network's integrity in terms of data security or GDPR compliance.

Without dedicated detection and protection beyond basic filtering, the existing SS7, Diameter and GTP core infrastructure can no longer be trusted:

► Subscriber privacy violations and data theft

Subscribers can be located down to street level and the location can be continuously tracked. IMEI and IMSI can be read out, including call status and hardware information.

► Illegal interception of calls and messages

Messages can be read and calls can be forwarded to unauthorized third parties using a number of alternative methods, including manipulation of subscriber data and crypto key exfiltration.

► Billing fraud

The financial impact on billing fraud is highly relevant. Possible manipulations of subscriber data include unauthorized pre-paid to post-paid conversion and USSD-based attacks on credit transfers.

► Denial of service (DoS)

Targeted attacks via ISD/DSD or general overloading of signaling links have recently gained in popularity and impact critical data connections (critical infrastructure) as well as voice services.

System Key Features

- Carrier-grade SS7, Diameter and GTP intrusion detection
- Scalable system architecture
- Compatible with redundancy requirements
- Centralized remote management
- Graphical UI - intuitive system handling
- Nodes based on Erlang/OTP
- Element profiling
- Resilience 99.999% uptime
- Carrier grade SLA, CARE, Incidents
- Full SCTP/M3UA/M2PA support
- M2PA support
- Anonymised reports to comply with GDPR
- High flexibility in rules and actions
- Full OSS and cloud orchestration support

The Solution

As a renowned industry leader in the field of strong encryption and network security, GSMK developed the Oversight system to enable comprehensive detection of signalling network anomalies and continuous monitoring and alarming.

The Oversight system architecture provides seamless integration into existing signaling structures and complies with redundancy requirements within load balanced setups.

System Design

The Oversight network security system, building on a modular and scalable approach, consists of the Oversight Manager, which constitutes the centralized backend, as well as a number of a number of *Oversight Detector* nodes according to the number of interconnect STP or DEA nodes to be secured.

Software

The Erlang/OTP-based software and runtime environment enable a highly parallel, fault-tolerant, real-time non-stop system with maximum availability and scalability for reliable attack detection and parametrization.

Analysis and visualization

A major step into state-of-the-art analysis is the right graphical representation of raw data. Only then data becomes information and complex systems can be handled without time-consuming trainings.

The backend system provides a state-of-the-art HTML5-based user interface (Oversight Frontend) enabling intuitive and centralized system management. Visualizations allow different levels of operation, e.g. filter configuration, filter grouping, graphing, logs, reports, alarming and system administration.

Deployment

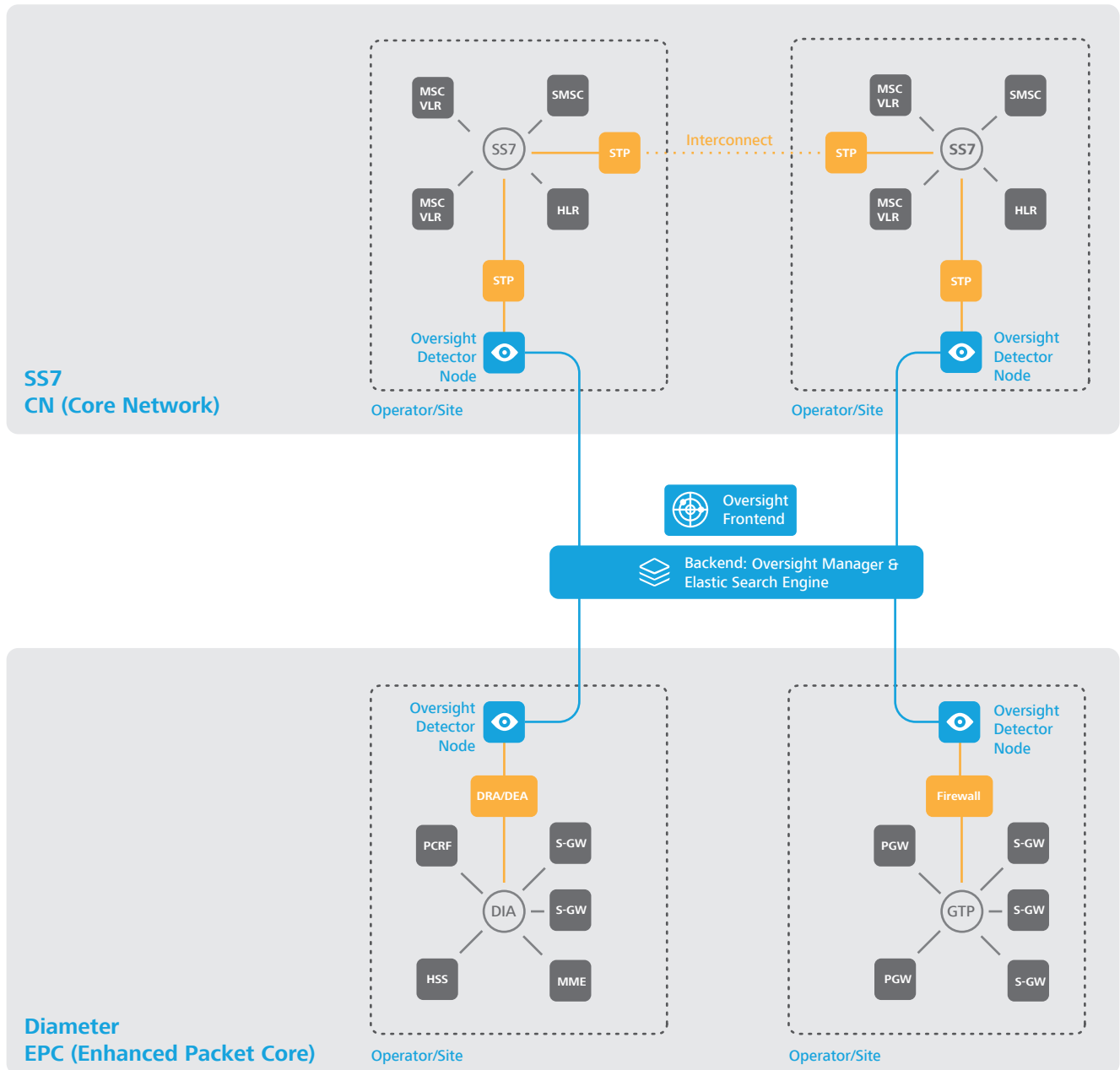
GSMK supports its customers before, during and after deployment with an advanced requirement analysis, full deployment support, training, system swing-in calibration and tailor-made SLAs.

Lab Version

Lab versions are available for testing and maintenance purposes.

Oversight System Architecture

Multi-technology, multi-site, multi-operator, 5G ready

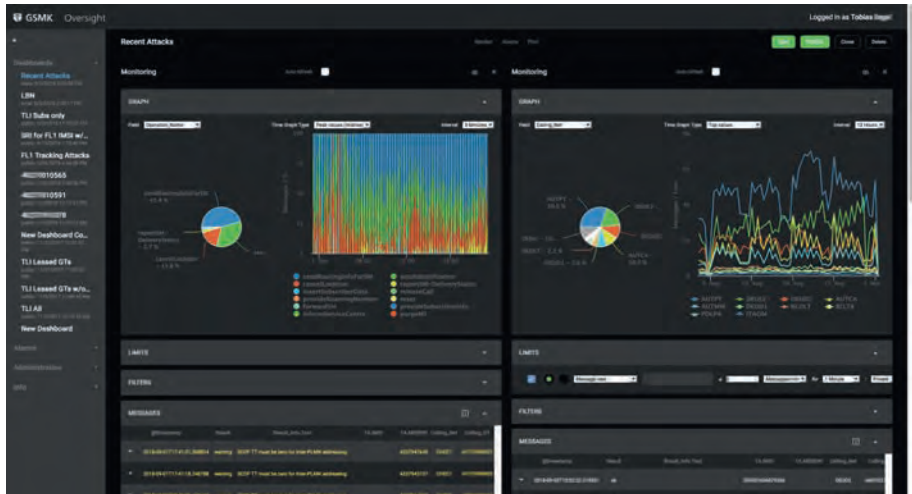


Oversight User Interface

Information visualization and system management

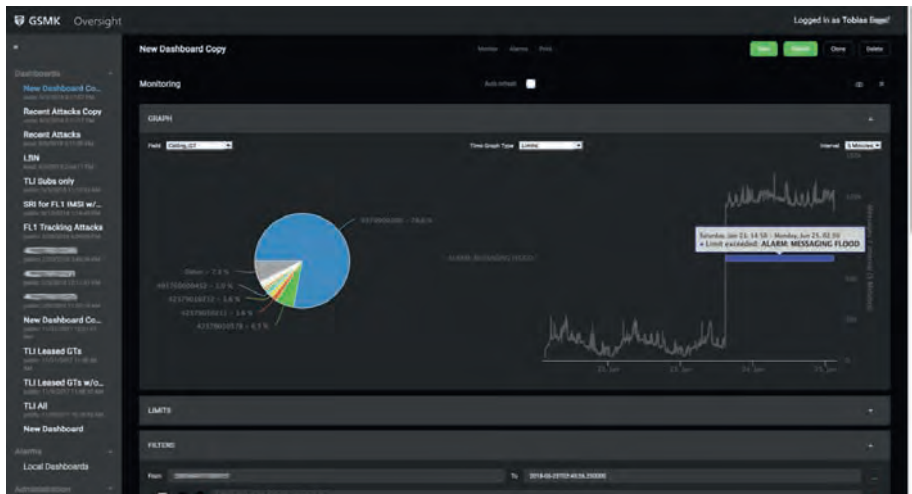
Oversight Frontend

Dashboard-based information architecture



Oversight Frontend

Filters, trigger levels and alarming



Oversight Frontend

In-depth data inspection



Oversight Hardware

Information visualization and system management

Oversight Detector Node

High-grade appliance
HP ProLiant, Generation 10



System Monitoring

GSMK backend systems support health monitoring via frontend and SNMP (RFC 1157, RFC 3410) for centralized monitoring solutions.

Oversight Manager

Scalable High-End-Server for mission-critical applications



System Monitoring

GSMK backend systems support health monitoring via frontend and SNMP (RFC 1157, RFC 3410) for centralized monitoring solutions.

GSMK - Gesellschaft für Sichere Mobile Kommunikation mbH
Marienstrasse 11
10117 Berlin
Germany

Phone + 49-30-24 62 500-0
Telefax + 49-30-24 62 500-1
www.gsmk.de

This document is provided for information purposes only, and the contents hereof are subject to change without notice. This document is not warranted to be error-free, nor subject to any other warranties or conditions, whether expressed orally or implied in law, including implied warranties and conditions of merchantability or fitness for a particular purpose. We specifically disclaim any liability with respect to this document, and no contractual obligations are formed either directly or indirectly by this document. This document may not be reproduced or transmitted in any form or by any means, electronic or mechanical, for any purpose, without our prior written permission.

The product names and logos mentioned in this document are trademarks or registered trademarks of their respective owners. © V2_08.2018_M

This document is GSMK Classified Information and not for general circulation.



Regional Representative / Distributor