

Monitoring Centre - Collection, Storage and Analysis of Intercepted Communication

The Klarios® Monitoring Centre (MC) is a comprehensive platform for filtering, collecting, storing, analysing and presenting data and voice communication collected from various types of telecommunication networks.

The Klarios® MC supports law enforcement and intelligence agencies in their endeavours to maximise the results of their investigative efforts.

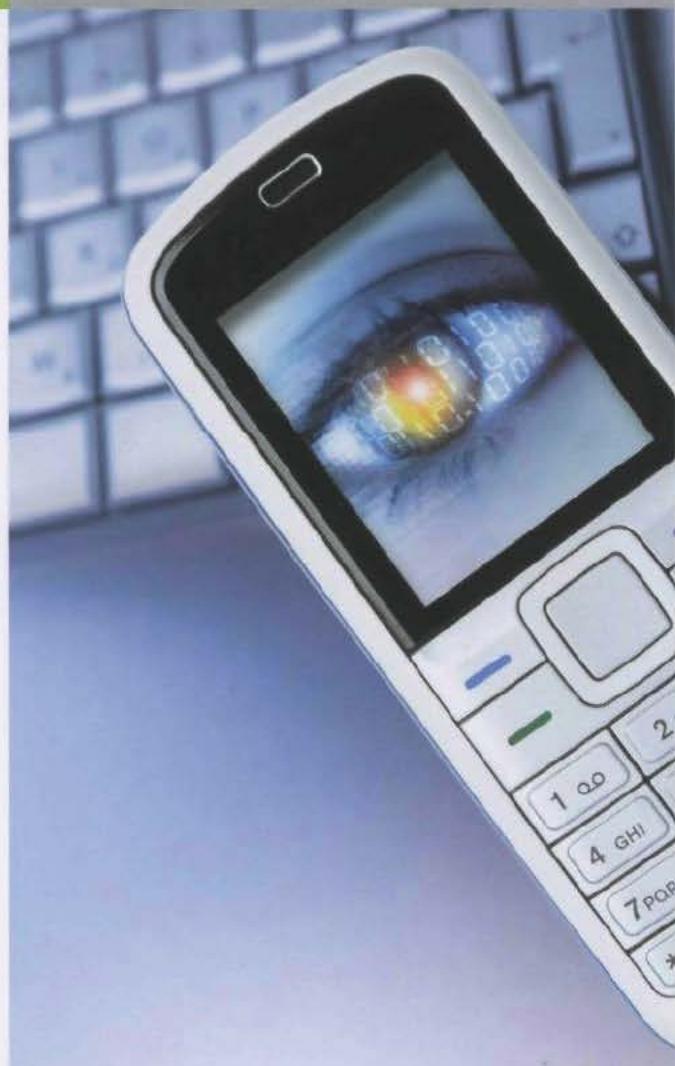
Key benefits of the Klarios® Monitoring Centre are:

- Flexible and modular architecture allowing deployment in different types of service provider networks (PSTN / ISDN, VoIP, NGN, ISP)
- Ergonomically optimised user interface simplifying the process of evaluating, searching and transcribing communication content
- Advanced search functions allowing users to focus only on relevant content
- Content pre-filtering and automatic classification using integrated data analysis tools
- Centralised administration of target provisioning and user access rights; customised workflows adapted to specific legal / regulatory requirements; extensive reporting and auditing capabilities
- Field-proven solution based on 15 years of experience and close cooperation with satisfied customers worldwide

Technical characteristics:

- Compliant with ETSI, 3GPP, CALEA and various national handover standards for legacy circuit-switched telephony and IP data delivery
- Interoperability tests regularly conducted with leading network equipment vendors
- Scalable in terms of data collection / processing bandwidth and number of system users (content evaluation and analysis clients)
- Open decoding platform enabling development of new decoders for a wide range of IP applications
- Optional indexing and processing engines providing automatic analysis of large volumes of unstructured data
- System components designed to protect the system against external intrusion and intercepted malicious content

Klarios® 2.0



ATIS Klarios® Monitoring Centre
Turnkey solution – preconfigured and tested for seamless integration with network infrastructure

Klarios® | Monitoring Centre

Klarios® Monitoring Centre – Collection, Processing, Storage and Analysis

A System Architecture

The Klarios® Monitoring Centre comprises:

- Front-end – connects with handover interfaces of service provider networks; a wide range of handover standards are supported
- Core system – storing, managing and processing intercepted communication
- Back-end – clients for i) evaluating intercepted and processed content; and ii) administration of the Monitoring Centre

A wide range of functional options complete the tool-set available to law enforcement and intelligence agencies in order to increase productivity and optimise the results of their investigative efforts.

All systems are delivered rack-mounted with monitoring / configuration consoles and are equipped with UPS units to protect the Monitoring Centre against power failure.

B Front-end

Characteristics:

- Collection of intercepted communication from ISP, PSTN / ISDN, 3G, Next Generation and VoIP networks
- Conversion / mediation of differing delivery formats into a uniform format
- Modular and scalable

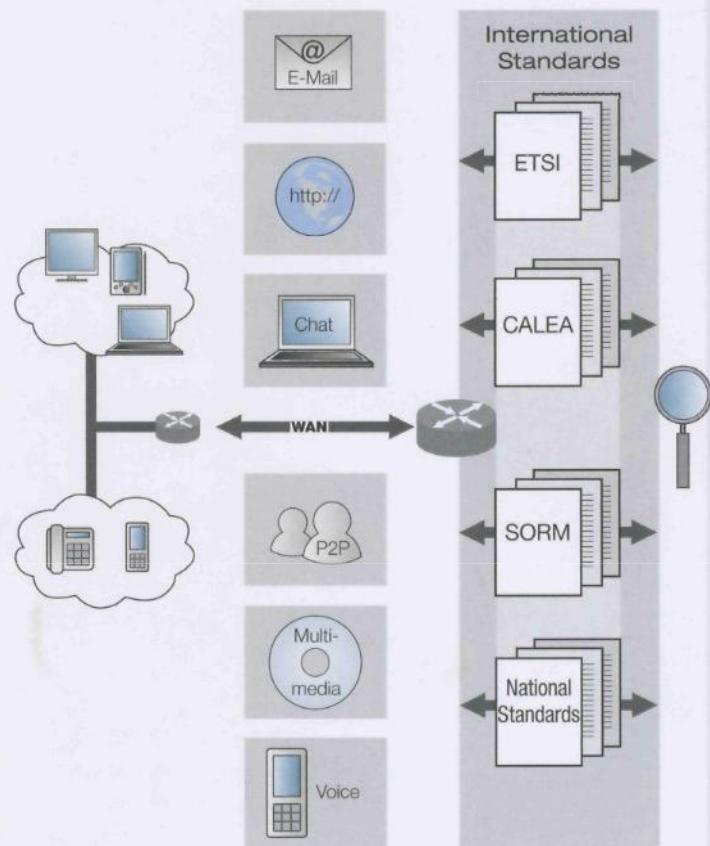
The Klarios® MC front-end family includes the following modules:

MCMX / MCMN

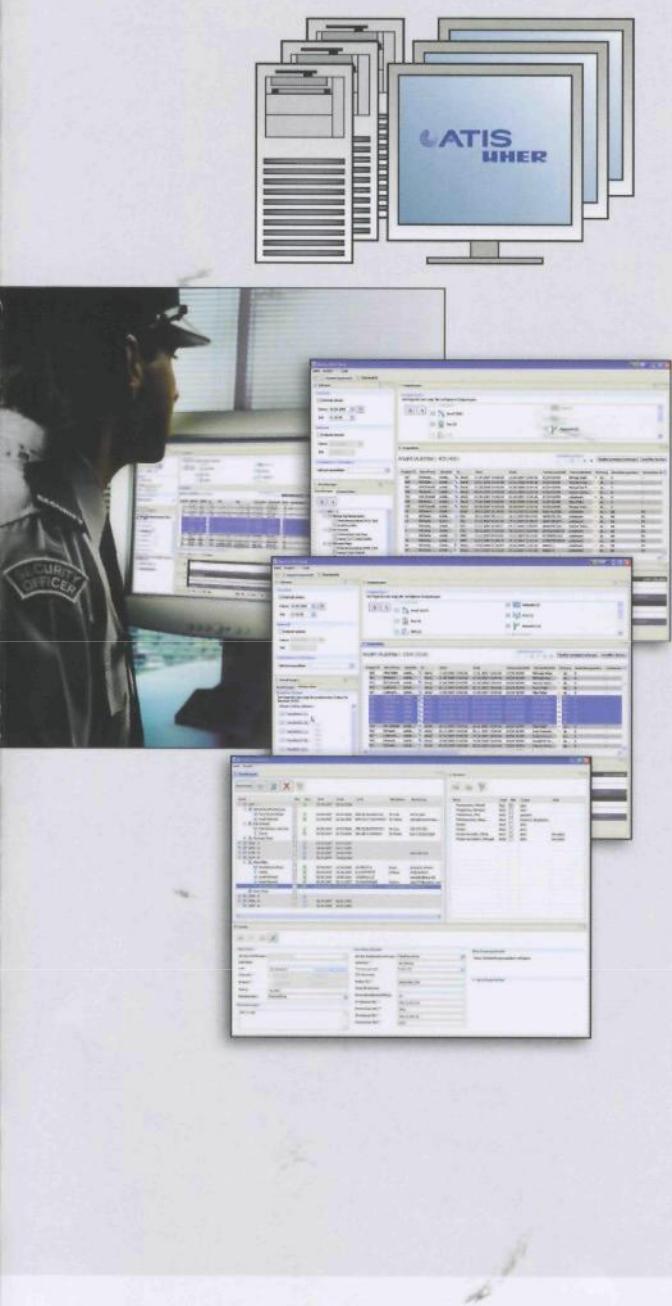
Front-end for legacy circuit-switched telephony. Receives communication content via E1 links, decodes the signalling protocols, classifies calls and forwards the content over (internal) IP networks (LAN / WAN) to storage servers. Available in a basic version with 2 E1 interfaces (MCMX) or in a modular chassis version (MCMN) for up to 16 E1 interfaces.

CAR Handler

Conversion of all intercept-related information (IRI) received by the Monitoring Centre into the standard used in Klarios® databases.



Klarios® 2.0



APIX

The latest member of the ATIS front-end family is used for collecting all communication content delivered in IP format (VoIP, e-mail, internet, etc.)

C Core System

CDBS

At the heart of the Klarios® MC, the Central Database Server (CDBS) controls and manages mission-critical system information/data, including references to all communication recorded (objects) as well as user access rights and logs.

Main functions of the CDBS:

- Storing all references to content intercepted and providing search and navigation capabilities to users
- Managing roles and access rights for system users and administrators
- Auditing, logging and reporting all system activities
- Managing and monitoring all modules of the Klarios® Monitoring Centre

To meet the highest requirements in terms of system availability, resilience and scalability, various database cluster configurations are available (optional).

F3S

Large data volumes require:

- sophisticated storage systems and content ageing solutions;
- optimised use of available storage capacity; and
- minimised total cost of ownership (capital and operational expenditure) per unit of storage.

Klarios® F3S (Flexible Scalable Storage Solution) is:

- able to support virtually all storage platforms;
- independent of specific vendors; and
- independent of the rapid pace of change in the underlying storage technology market (storage media).

Technical Details

Monitoring Centre

IDEc

The Internet Decoding (IDEc) is a state-of-the-art solution for demodulating and decoding a wide range of data communication protocols. Our objective is to reconstruct intercepted internet sessions as seen by the intercepted subscriber.

Supported protocols include fax, SMS and commonly used modem and internet (application) protocols:

Decoding

- E-mail (SMTP, POP3, IMAP)
- Web (HTTP, webmail)
- VoIP
- Chat (IRC, ICQ, Yahoo Messenger, MSN, AIM)
- News
- FTP
- P2P
- AOL

Demodulation

- PSTN (supports most of the analogue modem standards)
- ISDN (including Multilink PPP)
- Fax (analogue and FRITZ!Card; mixed analogue-ISDN)
- SMS, MMS, ring tones
- SMS over PSTN / ISDN

Other protocols can be developed upon request.

D Back-end

The graphical user interface of the Klarios® Monitoring Centre is tailored to meet the requirements of law enforcement and intelligence agencies. For this purpose, a rich set of user-friendly features is available to investigating officers, including:

- rapid searching in intercepted communication content and IRI;
- setting content processing priorities (allocating resources for certain targets);
- defining alarms triggered by certain activities of user-defined targets;
- easy and intuitive navigation within the content of intercepted sessions; and
- access to comprehensive summarising statistics of intercepted sessions (e.g. which applications were used by the intercepted target).

For more detailed information, please do not hesitate to contact ATIS.

E Functional Options

Several evaluation and analysis tools can be added to the Klarios® Monitoring Centre. Possible options include:

SCP – Signal and Content Processing is a flexible and scalable platform used for the purpose of filtering and analysing signals collected by the Monitoring Centre.

Characteristics and features:

- Library of software-based processing modules running on a number of processing instances (servers)
- Facilitates the automated analysis of a broad range of voice and data signals
- Speaker and language recognition, phonetic word indexing and protocol analysis

IDA – Intelligent Data Analysis platform provides the law enforcement and intelligence agencies with advanced functions for conceptual search and information retrieval within the data collected. Available features:

- Keyword search
- Linguistic processing
- Automatic data / content clustering
- Classification based on predefined or automatically generated taxonomies

GIS – Geographical Information System

Klarios® GIS allows geographic surveillance of targets in mobile networks. The GIS user interface shows the locations of the mobile subscribers being monitored and their movements between different locations on digitised maps.

ADRI – ATIS Retained Data Investigator

Klarios® ADRI supports direct connection to the retained data repositories and:

- supports ETSI standardised handover or proprietary interfaces;
- provides a wide range of data analysis, mining, correlation, mapping and presentation tools;
- enables deep evaluation of query response data delivered by data retention systems; and
- represents a full end-to-end data retention solution based on state-of-the-art modular storage and indexing platforms.

AIMS – ATIS Interception Management System

is a software module which enables law enforcement and intelligence agencies to manage complex network topologies in multi-vendor and multi-service-provider environments. AIMS offers a centralised provisioning interface to enable and disable target interception directly from the Monitoring Centre's system administrator client position.