STAR-GATE™

Intelligent Delivery

Compliance with CALEA and ETSI Delivery and Administration Standards

USA
Tel: +1-703-818-2130
Fax: +1-703-818-2131
E-mail: marketing.citi@cominfosys.com

Israel
Tel: +972-3-766-4119
Fax: +972-3-766-4747
E-mail: marketing@icominfosys.com

http://www.cominfosys.com

In this product description…

Introducing ***STAR-GATE***™:
Compliance with Lawful Interception Standards

As communication technologies expand, so do the regulations that control the communication surveillance activities of law enforcement agencies. Among the most sweeping of recent legislation are the CALEA/ETSI Lawful Interception (LI) standards, which mandate the telecommunication industry to provide electronic surveillance services for law enforcement agencies. LI standards started with circuit switched networks and now legalization of Internet surveillance is taking place worldwide. Operators of Internet Protocol (IP) networks will soon be also required to provide communication interception services for law enforcement agencies. Ensuring compliance with LI requirements can present great technical, legal and financial obstacles.

STAR-GATE was created specifically to overcome these obstacles. Drawing upon Comverse Infosys' expertise and years of experience in the design of communication surveillance products, STAR-GATE offers an effective, reliable and cost-efficient solution to LI requirements.

STAR-GATE supports both circuit switched and packet data networks. The requirements of IP networks are similar to those placed on circuit-switched operators: to extract all the communication traffic of users who have been targeted by law enforcement. The implementation, however, is quite different.

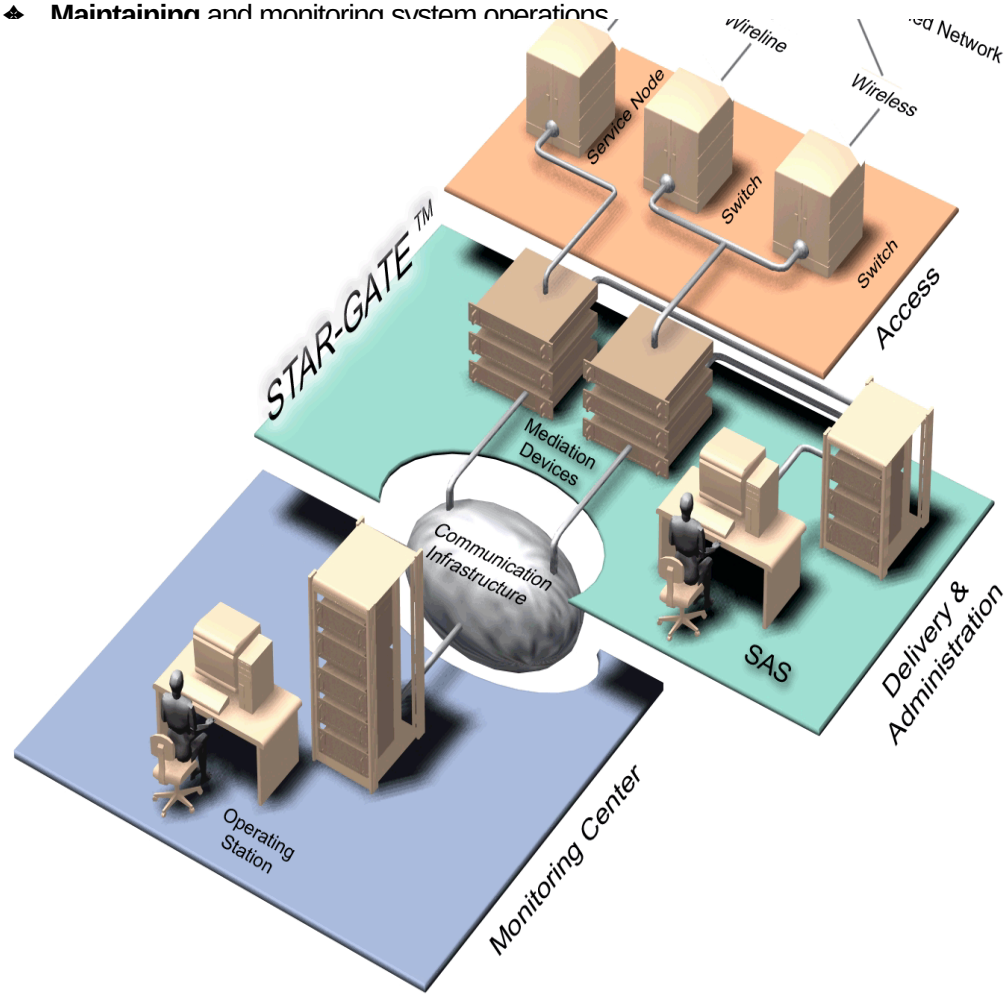
STAR-GATE provides telecommunication carriers and operators with the complete solution to LI regulations by unifying the legal obligations of both the access/delivery and administrative functions in a single product. These two functions are covered by STAR-GATE's two principle subsystems:

- **The Mediation Device [MD]:** Performs the delivery function of communication surveillance.
- **The Surveillance Administration Subsystem [SAS]:** Assigns targets and oversees system administration, maintenance and security.

Each MD can serve either circuit switched or packet data networks. The SAS is a unified, network independent solution. The same SAS can serve all kind of networks and switches. Together, these two subsystems perform the full range of tasks necessary to deliver intercepted communications to the appropriate law enforcement agency accurately, securely and in compliance with the law. The basic tasks include:

- **Collecting** intercepted data from the switch.
- **Converting** messages into the required Legal Interception (LI) Standard format.

- **Delivering** intercepted communications to the appropriate law enforcement agency.
- **Defining** target assignments and the destination parameters of law enforcement agencies.
- **Controlling** system security and monitoring system activity.
- **Maintaining** and monitoring system operations.



STAR-GATE's leading-edge technology provides the following features and benefits:

- A ***comprehensive solution***, STAR-GATE covers both administrative and delivery functions, supports multiple networks and switches and supports all data delivery protocols.

- An ***open and flexible solution***, STAR-GATE's modularity and scalability enable you to expand to meet any capacity requirement and can be easily upgraded to meet the needs of new technologies.
- A ***cost-effective solution***, STAR-GATE minimizes costs associated with backhaul, network engineering and operations.
- A ***legally compliant solution***, STAR-GATE complies with all regulations that govern communication monitoring and can be customized to meet specific regional regulations.

Comprehensive Solution

By unifying the delivery and administration duties of communication surveillance in a single product, STAR-GATE offers a comprehensive product that serves both functional and administrative needs.

In addition, STAR-GATE provides an end-to-end solution for the delivery of intercepted communications since it supports:

- **Wide Range of Protocols:** STAR-GATE provides full support for various call content and call data protocols. Furthermore, regardless of the protocols used by the switch STAR-GATE completes the mission of translating the data to the LI-standard interface and delivering it to the appropriate agency.
- **Multiple Switches:** Each STAR-GATE Mediation Device (MD) can be connected to several switches concurrently, even if the switches are of different types or versions. Multi-switch support reduces initial setup costs and simplifies deployment by offering capacity management that is unavailable with switch-only solutions. The enhanced capacity can be deployed efficiently in a regional framework that adheres to the published configuration guidelines.
- **Multiple Networks:** STAR-GATE supports all existing circuit-switched networks - wireline PSTN, ISDN, wireless GSM, CDMA, TDMA and packet data networks - GPRS for GSM, GPRS for TDMA, 1XRTT for CDMA, EDGE and UMTS. In addition, the product provides an excellent LI solution for fixed packet data networks, such as Internet Service Provider backbones.

- **Multicasting:** The MD can deliver intercepted call data and content to up to six different law enforcement agencies simultaneously, even if each agency requires a different delivery protocol.
- **Combined Content Delivery:** If the switch sends separated content, the MD combines it and delivers the integrated content to the law enforcement agency's collection module. STAR-GATE's MD eliminates the need for additional switch hardware to perform this function.

Open and Flexible Solution

In order to keep pace with the dynamic and ever-changing telecommunications industry, the communication surveillance system must be open and flexible. STAR-GATE features these flexible benefits:

- **Adaptable Design:** STAR-GATE's open architecture operates independent of switch type, model or software version and is smoothly integrated into any environment. In addition, STAR-GATE can be easily customized, upgraded and adapted to meet the demands of new communication protocols and technologies.
- **Scalable Capacity:** STAR-GATE's modular design is fully scalable to meet any capacity requirement. MD sites can be added as new switches are added to the network, and the central Surveillance Administration Subsystem can be expanded to support more users, targets and MD sites as the network grows.

Cost-effective Solution

With STAR-GATE, the details of complying with LI standards are left to the communication surveillance experts at Comverse Infosys. STAR-GATE ensures full legal compliance, decreasing expenses associated with network design and engineering.

In addition, STAR-GATE's centralized network design diminishes costs associated with backhaul and operations. Since all data can be routed and distributed through a central location, you save on systems expenses. Centralized operations also present savings with respect to personnel, training, reduces initial setup costs and simplifies deployment by offering capacity management that is unavailable with switch-only solutions.

Legally Compliant Solution

Comverse Infosys closely monitors legislation that regulates communication surveillance so that you can rest assured of being in complete compliance with the law.

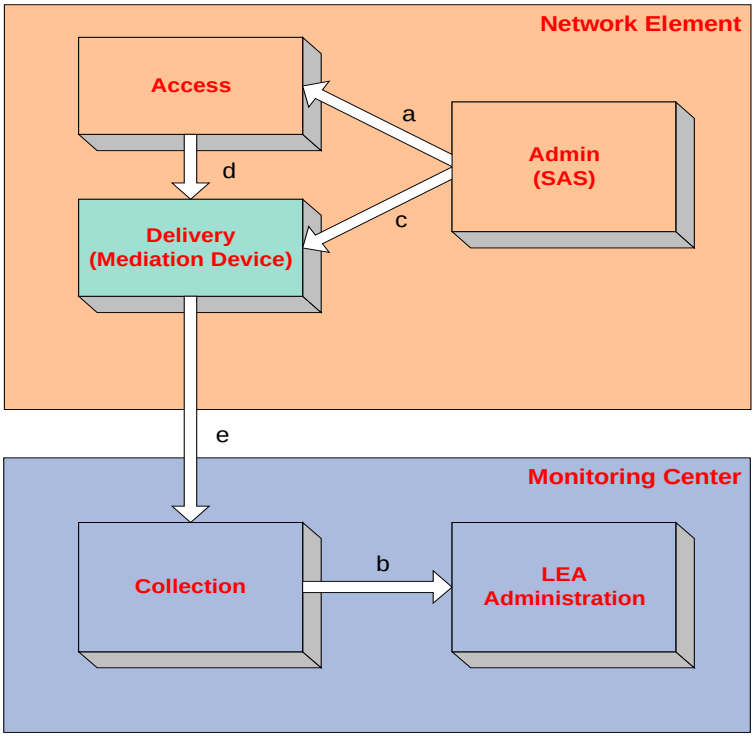
STAR-GATE ensures full LI-standard compliance not only by converting messages into the required protocol, but also by supporting supplementary services. The following are examples of how the STAR-GATE Mediation Device (MD) fills in the missing pieces to help the switch comply with LI standards:

- The MD supports most standard call content protocols, such as PRI or ISUP for circuit-switched networks, FTP or GTP* for packet data networks.
- The MD can extract post cut-through DTMF signals from the call content and retransmits them with the call data.
- If the WAN connection is down, the MD can provide buffering for data until it can be delivered successfully.
- The MD correlates Call Content and Call Data using predefined call identifiers.

Compliance with CALEA

The following diagram illustrates the functions of communication surveillance as illustrated in the J-STD-025 model. The telecommunication carrier is responsible for delivery regulations, while the law enforcement agency is responsible for the collection regulations.

TIA J-STD-025 Network Reference Model:



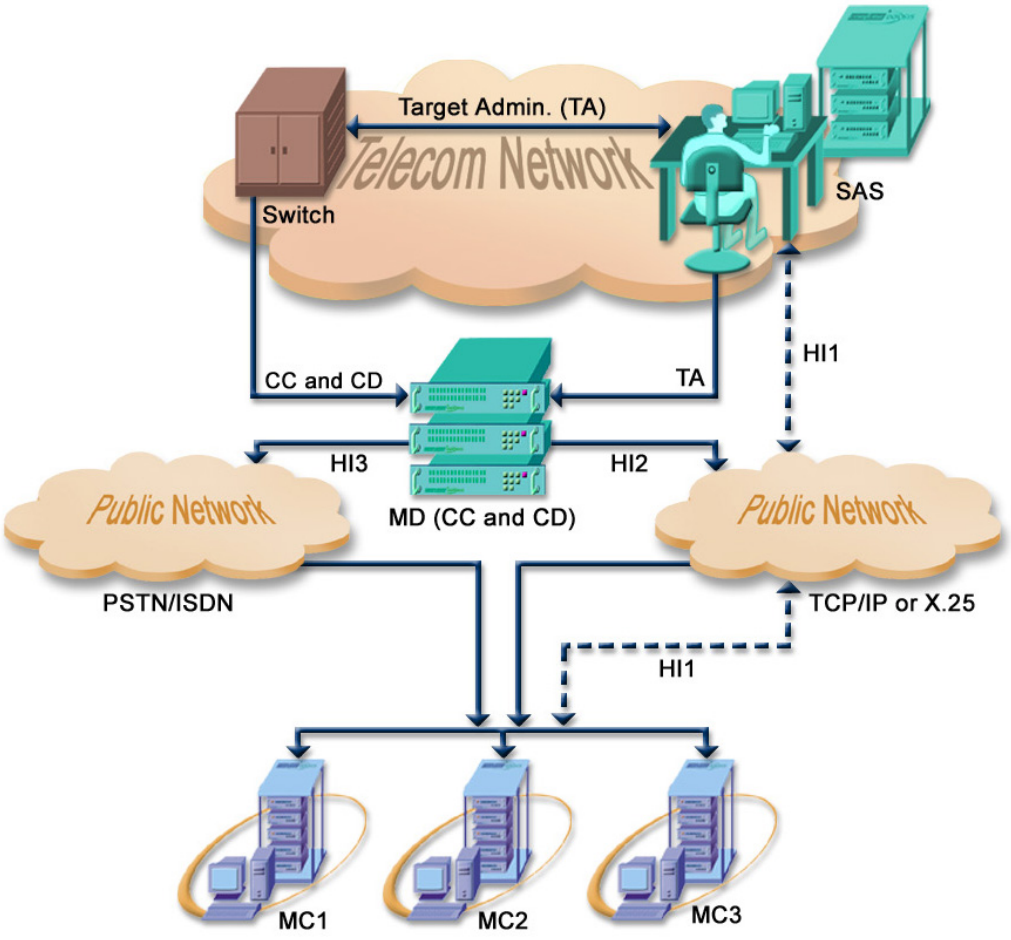
The STAR-GATE system is fully compliant with the following delivery and administration requirements:

- Telecommunication Industry Association Interim Standard (TIA) J-STD-025
- Surveillance Administration System Generic Requirements GR-2975-CORE
- TR-45.2 J-STD-025 + Enhance Surveillance Services

Compliance with ETSI

The STAR-GATE system is fully compliant with ETSI ES 201 671, which regulates the handover interface for the lawful interception of telecommunication traffic.

According to ETSI standards, the generic handover interface adopts a three port structure such that administrative information (HI1), intercept related information (HI2) and the communication content (HI3) are logically separated.



Entities of ETSI-Compliant Surveillance

The switch provides the CC and IRI at the internal network interface. For both information types, mediation functions may be used, which provide the final representation of the standardized handover interfaces. HI1 interface is optionally provided by SAS.

Functional Description

STAR-GATE™ is comprised of two main subsystems:

- **The Mediation Device:** performs the delivery functions of communication surveillance.
- **The Surveillance Administration Subsystem:** Assigns targets and oversees system administration, maintenance and security.

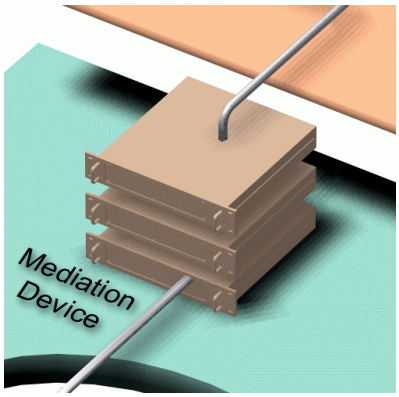
The data flow architecture and main features of both of these systems are discussed in detail in this section.

Mediation Device

The STAR-GATE Mediation Device (MD) performs the delivery functions of communication surveillance for a wide range of network switches and network environments. It is comprised of three functional components:

- **Switch Interface System:** An integrated adapter to the switch, designed for a specific switch type and software version.
- **Kernel:** The nucleus where most of the MD functions are performed.
- **Output Formatter:** An integrated output formatter module, customized specifically for LI standards, to convert the switch proprietary message format to the required LI format.

The Mediation Device:



Architecture and Data Flow of Mediation Device

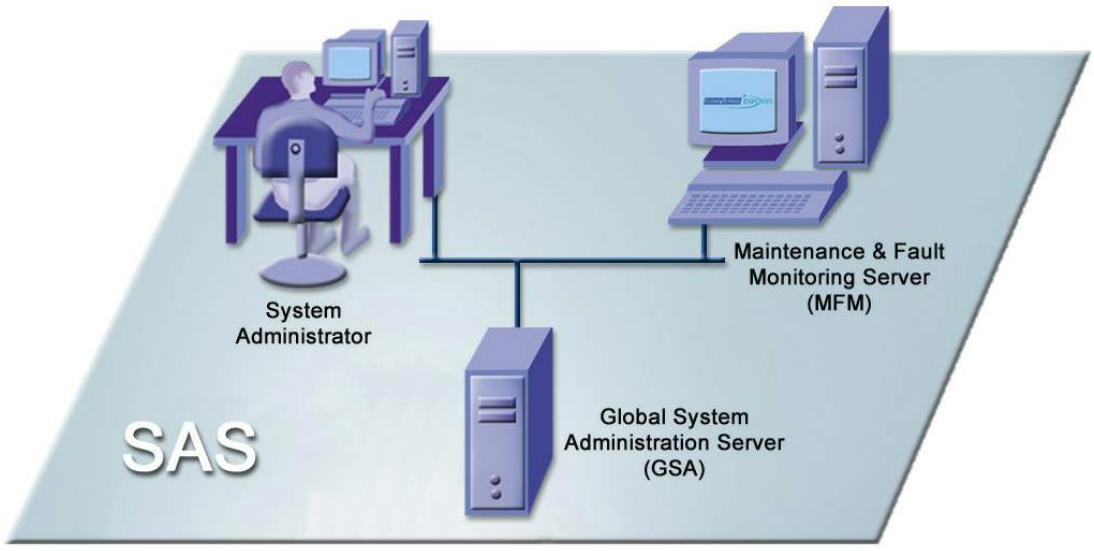
STAR-GATE's mission is to deliver intercepted communications to the appropriate law enforcement agency accurately, securely and in compliance with LI standards. The STAR-GATE Mediation Device (MD) completes this mission by mediating between the switch, the law enforcement agency and the Surveillance Administration Subsystem (SAS). The data flow is illustrated below:

1. **Network Interfacing:** The MD receives intercepted information from the switch. The information is collected by the MD drawer and can include both call content and call data.
2. **Conversion:** The MD converts the collected data format to the LI-standard format required.
3. **Delivery:** The MD delivers the data directly to the appropriate law enforcement agency. The data are sent via the LAN to the site router and then to the collection module at the law enforcement agency.
4. **Target Provisioning:** The MD sends and receives administrative data to and from STAR-GATE's Surveillance Administration Subsystem (SAS). These data are sent via a WAN connected to the site router and include information such as target assignments and management instructions.

Surveillance Administration Subsystem

The Surveillance Administration Subsystem (SAS) provides centralized control over system administration and system maintenance. The SAS is comprised of two modules:

- **Global System Administrator Server (GSA):** Controls system administration, target assignments and security functions.
- **Maintenance and Fault Management Server (MFM):** Oversees system operations and controls system maintenance.



Surveillance Administration Subsystem

Global System Administrator Server

The Global System Administrator Server (GSA) provides centralized control over system administration, target allocation and security functions.

The GSA features an intuitive graphical interface based on standard Windows conventions. Among the application's highlights is a search feature that enables you to quickly access users and targets. The GSA application also enables you to back up all user and target information with removable media.

STAR-GATE's flexibility enables a variety of GSA deployment options to suit particular needs. One central GSA can administer all network switches. Alternatively, several GSA units can be situated regionally. Furthermore, additional GSA units can added to an SAS site for load sharing and redundancy.

The following sections explain the GSA functions.

System Administration

The GSA enables you to define users and their information access rights in order to guarantee smooth and secure operations. Several types of users can be defined, including a System Administrator and Target Administrator. Each user's access and actions can be limited to fulfilling specific tasks.

The administrative features of the GSA include:

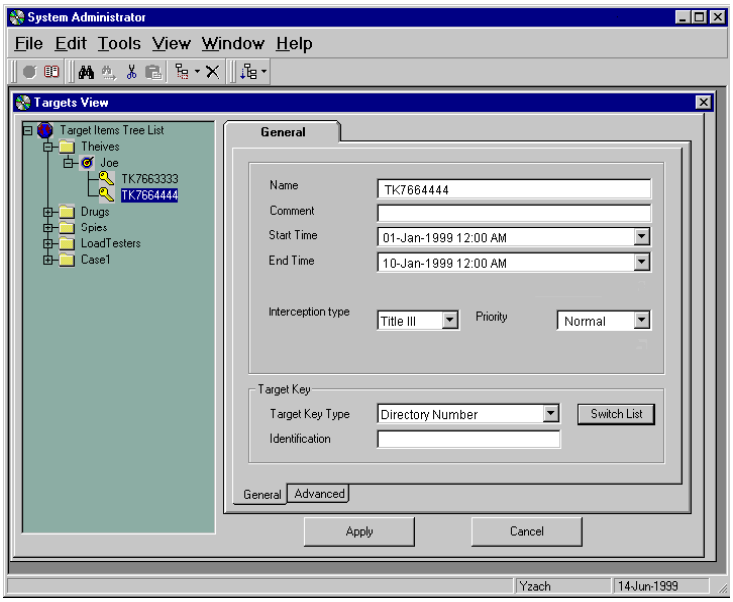
- **Remote Access:** The GSA can be controlled with remote dial-up connections, enabling authorized administrators and security officers 24-hour, secure access to the system. Configurable security restrictions limit remote administrators to specific, predefined tasks.
- **Generation of Reports:** System activity is easily monitored with the generation of reports. The GSA can issue reports on the operations of the entire system, on particular targets or on particular users. Reports can be printed, saved and exported to other applications.

Target Administration

The target allocation functions of the GSA enable the accurate and efficient transfer of intercepted data. A Target Administrator defines information about switches, targets and law enforcement agencies. This information includes:

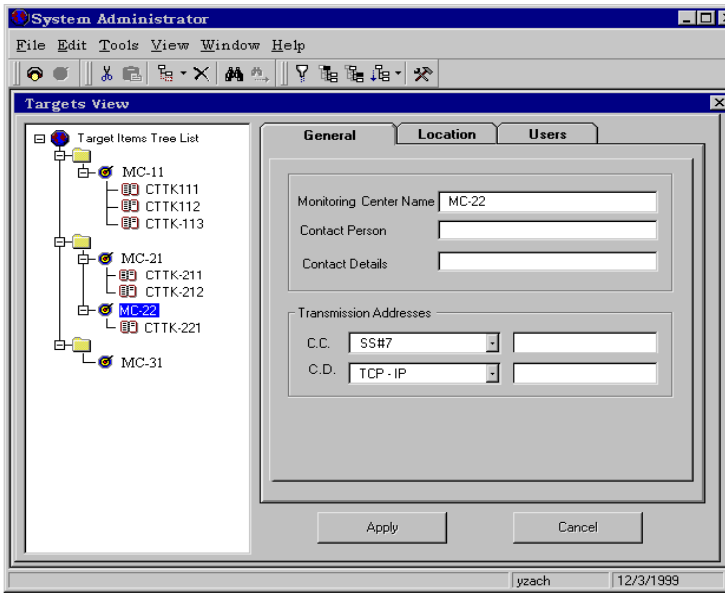
- **Territory Data:** Divides switches into regions, enabling the GSA to determine which switches should monitor particular targets.
- **Target Data:** Defines and distributes actual targets for surveillance. Target data include a target number, delivery information, and warrant restrictions. Warrant restrictions can include time and date limitations and can specify surveillance type - both Call Content and Call Data or Call Data only. The GSA distributes the targets to the appropriate Mediation Device and switches and monitors and logs the distribution process. The Mediation Device automatically provisions the switches with the target data and warrant restrictions.

Defining Targets:



- **Law Enforcement Agency Data:** Defines the destinations where intercepted data are sent. Required destination information includes the network address and protocol used by the law enforcement agency. The entries can also include supplementary data, such as contact information and comments.

Defining Law Enforcement Agency Parameters:



Security Functions

The GSA provides uncompromised security features to ensure data confidentiality and grant access to authorized personnel only. These features include:

- **Controlling Data Access:** The GSA ensures the confidentiality of both target information and intercepted data. Access rights defined by the System Administrator apply to files, network connections and database tables. SAS can also operate with any firewall programs that can be provided as part of the network design.
- **Monitoring System Activity:** All operator actions and most system activities are recorded in a log file, called an "audit trail". Information in this file includes the operators' access to resources and information changes.
- **Transfer Encryption:** Encryption between the Mediation Device and the System Administration Subsystem (SAS) or between the Mediation Device and the collection facility is ensured by network equipment that supports the necessary protocols.

Maintenance and Fault Management Server

The Maintenance and Fault Management Server (MFM) provides a base for monitoring the operations of the entire network. The MFM also controls configuration and software upgrades of units throughout the STAR-GATE system.

Operations Monitoring

The MFM continually receives event information from the other units in the system. Event information includes the unit source, description of event and a time stamp. In addition, the MFM regularly contacts system units to gain operation information. Based on this data, the MFM constructs a "picture" of the system and its status. Using an intuitive graphical interface, the MFM creates a visual representation of the entire surveillance system, with each site represented by an icon. The display is color-coded according to current status, giving the Maintenance Engineer an immediate grasp of overall system operations.

Highlights of MFM operations monitoring include:

- **Effortless Navigation:** The Maintenance Engineer can quickly and easily gain a broad view of the entire system or a microscopic view of the operations of individual units. By clicking the site icons in the visual representation of the system, the Maintenance Engineer can zoom down through the different subsystem levels. This feature enables the Maintenance Engineer to see everything from the "big picture" to detailed information about individual cards and channels.
- **Remote Access:** The MFM can be controlled via remote dial-up connections, enabling an authorized Maintenance Engineer 24-hour access to the system. Configurable security restrictions can limit the Maintenance Engineer to specific, predefined tasks. In addition, the MFM can be configured to page a Maintenance Engineer when defined events are generated. The paged message can include a code indicating the type of event.

Configuration and Control

The MFM provides a central location to control the STAR-GATE system, enabling the Maintenance Engineer to shutdown, reboot and modify the configuration of any system unit. The MFM also enables the Maintenance Engineer to run diagnostic tests on individual units.

Software Upgrades

As new telecommunication standards and software versions become available, the STAR-GATE system may require upgrades. The MFM provides a central location to control software upgrades throughout the system. The MFM distributes the new software version to the specified unit, issues a reconfiguration command and monitors and logs the process.

Contact Information

Contact us at any one of our offices below for more information:

Comverse Infosys Inc
Worldwide Headquarters
Tel: +1-516-677-7300
Fax: +1-516-677-7197
Toll Free: 1-800-967-1028
E-mail: marketing@cominfosys.com

Comverse Infosys Technology Inc.
Tel: 1-703-818-8002
Fax: 1-703-818-2131
E-mail: marketing.citi@cominfosys.com

Comverse Infosys Ltd.
Tel: +972-3-766-4119/5258
Fax: +972-3-766-4747
E-mail:marketing@icominfosys.com

Comverse Infosys UK, Ltd.
Tel: + 44 (0) 1923 717347
Fax: +44 (0) 1923 717377
E-mail: andrew_dawson-maddocks@comverse.co.uk

Comverse Infosys Hong Kong
Tel: +852-2574-7192
Fax: +852-2904-7676
E-mail:marketing-hk@icominfosys.com

Comverse Infosys GmbH
Tel: +49 6172 941799
Fax: +49 6172 488038
E-mail: franz.woelflick@netsurf.de

Comverse Infosys Brazil
Tel: +55 11 3039-7373
Fax: +55 11 3039 7333
E-mail: marketing@icominfosys.com

Comverse Infosys Netherlands

Tel: +31 - 79 - 36 -33 -111
Fax: +31 –79 - 36 -33 -110
E-mail: marketingnl@icominfosys.com