SUBSENTIO
To Notice Secretly

About Subsentio®

Subsentio, LLC. is trusted by both the private and the public sectors to perform lawful intercept. Based in Centennial, Colorado the company has national, regional and rural service provider clients.

Subsentio provides Lawfully Authorized Electronic Surveillance (LAES) and compliance services to a diverse community of communications service providers. From national carriers to ultra-small rural providers, our clients serve millions of subscribers with a wide range of communications services. These services are often complex, multi-vendor environments encompassing differing phases of evolution and technological approaches.

SUBSENTIO,
The CALEA Compliance Company™

SAFE HARBOR INTERCEPT MEDIATOR - SHIM

Mediation system, including delivery and administration, initially supporting Sonus Networks based VoIP networks

The Safe Harbor Mediation System, or SHIM, serves as a complete CALEA solution for VoIP networks deploying equipment from Sonus Networks. It interfaces with the Sonus Insight Element Management System (EMS), GSX Open Services switches, and SBC 5x00 Session Border Controllers.
The SHIM is available as a physical appliance or as a virtual machine.

Key Features and Benefits

- Provides Safe Harbor CALEA compliance
- Supports ATIS 678 version 3 CALEA standard
- Much lower cost than competitive solutions
- Integrated provisioning requires no separate administrative system
- Integrated VPN reduces installation complexity
- Email alerts and notifications
- Buffering options selectable for each intercept

The Safe Harbor Intercept Mediator is an easy-to-install, self-contained system that provides interception, administration, and VPN security — all in one device. Intercepts are configured or provisioned in the Probe through a secure web browser interface.

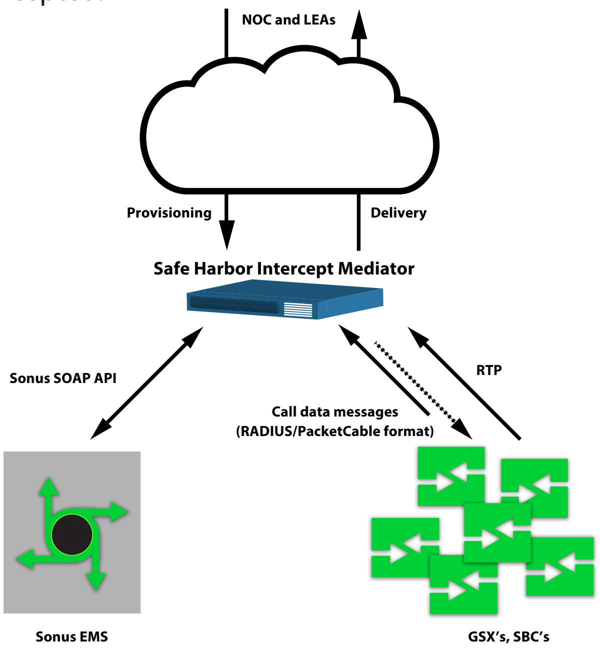
VoIP Intercepts: Pen register and full content voice intercepts are provided. The identifiers that can be provisioned are:

- Phone numbers, both US numbers and international numbers
- SIP URIs

DTMF (dialed digits) reporting is a selectable option. Also, the SHIM contains several optional functions to filter out duplicate intercepted calls, a problem often arising in large voice networks. If enabled, calls with identical call IDs are eliminated, as well as calls with different call-id's but with the same calling and called parties as another concurrent call. The SHIM can also ignore a leading '+' and leading U.S. country code in looking for duplicates.

Standards: The SHIM uses the ATIS 678 V3 standard, and also supports the optional features of the standards embraced by law enforcement, such as surveillance start, stop, and continuation messages. Optionally, the prior version of the 678 standard can be specified. The SHIM also supports, in conjunction with 678, the ATIS- 1000069 standard, which allows the SHIM to report conditions such as failed delivery interface, input interface down, lost output, dropped input, and others to the collection system(s).

Network interconnection: The connections to the voice network are shown in the diagram below. One connection is to the Sonus EMS, and over this interface the SHIM communicates the identifiers of the calls to be intercepted.



The EMS then distributes lawful intercept (LI) policies to the GSX and SBC, causing them to serve as Intercept Access Points (IAPs). Subsequently, as call events and call content are discovered for a call matching an LI policy, the GSXs and SBCs sent x2 and x3 information back to the SHIM.

Email Alerts and Notifications: The SHIM can be provisioned to send periodic reports to designated email addresses, including overall status reports (e.g., to operational personnel), and intercept case-specific reports to law enforcement. Additionally, certain events (e.g., delivery error, disk capability, VoIP call start) can be selected to trigger email messages.

Delivery: The SHIM contains a variety of mechanisms to maximize the robustness of the intercept delivery. One of these, buffering, prevents the loss of intercept information if anything fails on the upstream path. The buffering implemented in the SHIM is called "transparent buffering" in that the file system used is not visible outside the SHIM and thus this can be used with any law-enforcement collection system.

The SHIM integrates a site-to-site VPN capability, eliminating the need for a separate VPN appliance. The VPN is provisioned through the SHIM's web browser-based interface.

Security: The SHIM has two interfaces, both of which are highly protected – the provisioning interface and the delivery interface. The SHIM contains a firewall function that permits access to only a few services, and permits access from only a certain set of IP addresses. A specific client certificate is required to access the SSL- based provisioning interface. The delivery interface is typically protected using the built-in VPN capability. Certain information within the SHIM is encrypted, such as buffer files and the Probe's database.

Virtual SHIM (vSHIM): In addition to being available as a 1U physical appliance, the SHIM is available as a virtual machine (vSHIM). The vSHIM can run in the following virtual environments: (1) Amazon Web Services, (2) on a VMware ESXi hypervisor, and (3) on a KVM hypervisor. For instance, this allows multiple vSHIMs to run on the same physical machine or allows the vSHIM to run on the same physical machines as virtualized Sonus platforms.

Safe Harbor Intercept Mediator Physical and Electrical Characteristics

- 1U, 16.9" deep
- Approximately 16 lbs
- Operating temperature: 10-35 oC
- Two 1G system ports (typically one for provisioning and delivery, one for connection to the VoIP network)
- AC power, typical power 50w
- Remote management via BMC/IPMI