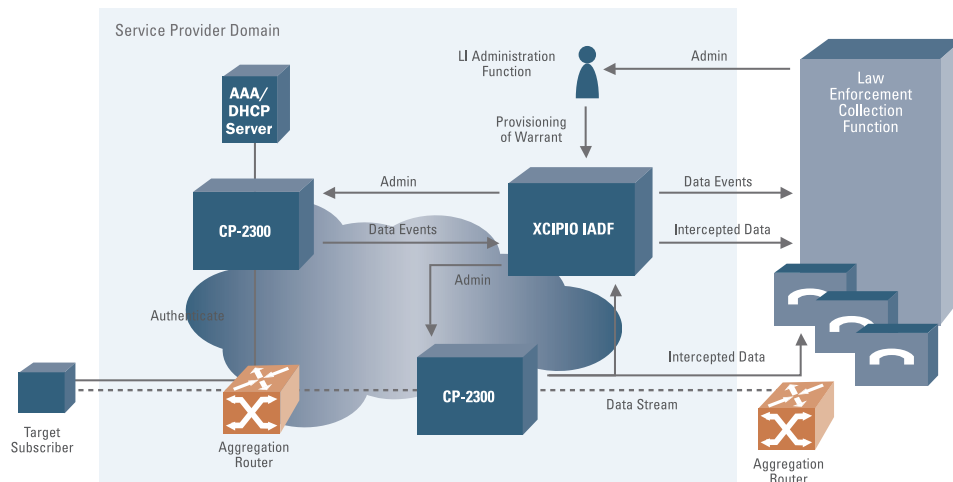


The Internet has brought about significant growth of IP-based communications. E-mail, chat, file transfer, and instant messaging applications constitute the bulk of these communications. Voice over IP (VoIP) calls will soon become as common as traditional circuit-switched voice calls. Criminal activities increasingly hide behind the Internet’s anonymity. New laws are also requiring telecommunications and Internet service providers (ISPs) to provide interception services to law enforcement agencies. It has become imperative to have lawful intercept solutions that are effective in the dynamic IP environment. The Xcipro™ lawful intercept platform from SS8 Networks™ offers an Internet Access Delivery Function (IADF) designed specifically to intercept and deliver IP traffic to law enforcement agencies.

### Real-time IP Intercept Capabilities

Xcipro IADF provides both access and delivery functions that enable ISPs to deliver session-identifying information and communications content to law enforcement agencies using standard protocols, transmission media, and delivery standards.

#### Xcipro Internet Access Delivery Function



The Xcipro IADF runs on standard Sun Microsystems servers and Xcipro CP-2300-ISP content processing module. Once lawful intercept is authorized by a court order, the CP-2300-ISP module is provisioned with target identifying information by the Xcipro provisioning engine. This information is then used to identify data packets belonging to the target subscriber and extract them from the IP network data stream—all in real-time.

In addition to passive monitoring capabilities, the Xcipro IADF supports dynamic IP addressing, enabling data packets to be extracted in real-time from network switches and aggregation routers. The CP-2300-ISP platform manages information processing, routing, replication, identification, encapsulation, and delivery to law enforcement in a standard format for secure access by authorized users.

Service providers can deploy Xcipio SSDF cost-effectively, easily meet the specific needs of law enforcement agencies, and do it without disrupting existing IP service offerings. The proven Xcipio OA&M platform has been deployed in more than 50 countries. Xcipio implements a generic managed object server (GMOS), which is responsible for maintaining and administering the delivery function, configuration, and databases. It also protects intercept controls, intercepted call content and call-identifying information, consistent with service providers' security policies and practices.

### **Flexible Architecture**

Designed for maximum flexibility, the Xcipio platform can be cost-effectively deployed by local or regional service providers, as well as scale to meet the needs of large domestic or global carriers.

### **Secure Platform and Access**

A comprehensive range of security features ensures a secure platform and secure access for law enforcement users. Physical access to Xcipio is restricted to either network connectivity via the Ethernet card or a direct RS232 port. Industry-leading authentication, and security features safeguard data and content. Rule-based user privileges can be tailored to restrict system access to only necessary and appropriate users.

### **A Strong Industry Partner**

As the leading provider of lawful intercept solutions, SS8 Networks works closely with service providers and network equipment manufacturers to deliver robust, high-availability intercept solutions. In addition, SS8 provides a vital liaison between equipment vendors, service providers and the law enforcement community, exchanging new ideas, supporting existing solutions, and ensuring that future solutions will continue to meet their needs.

Training and knowledge transfer are key elements of SS8 lawful intercept solutions. We provide extensive support to the system administrators, operators, and agents who maintain and use the Xcipio platform.

### **Key Features**

- Supports range of network elements, including softswitches, media gateway controllers, call agents, routers, trunking gateways, and CMTS
- Flexible architecture supports co-located, regional, or centralized deployment models and networks of any size
- Centralized provisioning capabilities and single point of administration simplifies deployment and management
- Distributed system architecture enables presence and reach across an entire IP network
- Enables centralized operational management of call data delivery to law enforcement agencies
- Simplified deployment and management features reduce lawful intercept administration costs
- Reinforces high network security measures through centralized management of call data delivery
- Multiple security features for data transport, delivery, and law enforcement access
- Supports simultaneous fan-out of specific CDC and CCC messages to multiple law enforcement agencies
- Filters data to specific agencies
- Proven, field-hardened platform and OA&M features, including: ITU standard MML support, surveillance provisioning GUI, built-in remote testing tools, alarm reporting and error logging, automatic software fault recovery, and automatic or manual disk backup
- Standards-compliant—J-STD-025, PacketCable, CALEA, and ISC



#### **SS8 Networks**

91 East Tasman Drive, San Jose, CA 95134

Tel: (408) 944-0250 Fax: (408) 428-3732

[www.ss8.com](http://www.ss8.com)

Some of the features listed may be under development. Please contact SS8 for feature availability schedule. This document does not create any express warranty by SS8 Networks or about its products or services. SS8 Network's sole warranty is contained in the written product warranty for each product. The end-user documentation shipped with SS8's products constitutes the sole specifications referred to in the product warranty. The customer is solely responsible for verifying the suitability of SS8's products for use in its network. Specifications are subject to change without notice.

Copyright © 2006 SS8 Networks, Inc. SS8 Networks, the SS8 Networks logo, Xcipio, and ServiceController are trademarks of SS8 Networks Inc. All other trademarks mentioned in this document are the property of their respective owners.