Contact GDC http://www.gdc.com

Secure Access Control System

for out-of-band control of network equipment

General DataComm

General DataComm, Inc., is a leader in the design, development, and manufacture of high-speed network access equipment for carriers , service providers, governments, and commercial end-users worldwide.

General DataComm, Inc.
6 Rubber Avenue
Naugatuck, Connecticut 06770 USA
Tel: 1 (203) 729-0271
Fax: 1 (203) 224-0588
www.gdc.com

Encrypt and Authenticate with Telco-Tough Reliability

Network operating companies will continue to deploy networking equipment in remote, unattended locations, with management conducted from centralized locations over the network itself (inband). Although this approach reduces the management devices required and eliminates travel time to/from the site, there are potential failure scenarios where in-band management itself may become crippled by an event.

For example, when equipment providing the network has failed, the only solution might be local diagnostics and recovery via a directly connected console, which is time consuming and costly. However, with out-of-band management, modems are deployed with corresponding circuits on the network equipment. This allows access via an alternative network (PSTN) during a failure, thus avoiding a site visit. The degree of protection afforded to the network equipment will depend on how capable the modem is in detecting and blocking unauthorized users.

> ***"... there are potential failure scenarios where in-band management itself may be crippled ..."***

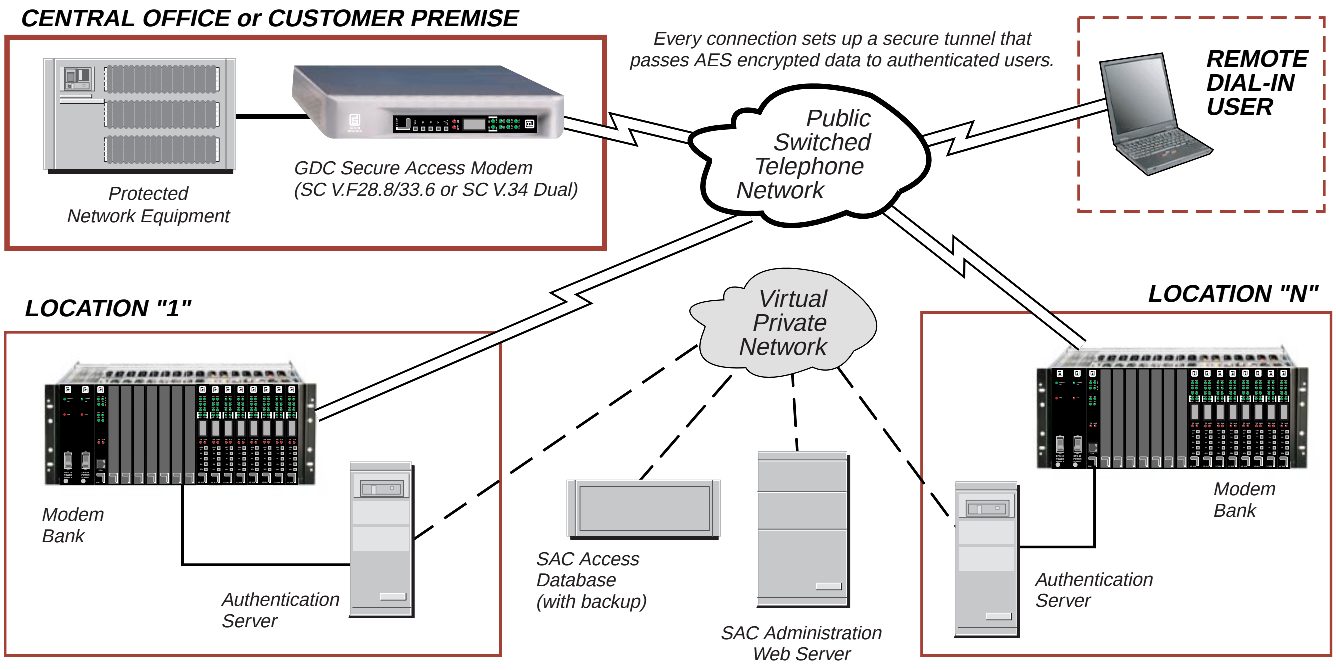
Scope of this Document

General DataComm has developed the Secure Access Control System (SAC) for out-of-band management of equipment. In a SAC system, GDC's family of NEBs-compliant SpectraComm modems integrate seamlessly with Secure Access Servers and the client desktop software.

The encryption and authentication capable modems enable secure access to equipment via a dial-up connection, thereby addressing the security exposure.

This document describes the theory of operation and the interoperability of key hardware and software components.

Figure 1: Principal SAC System Components


CENTRAL OFFICE or CUSTOMER PREMISE
Protected Network Equipment
GDC Secure Access Modem (SC V.F28.8/33.6 or SC V.34 Dual)
Every connection sets up a secure tunnel that passes AES encrypted data to authenticated users.
Public Switched Telephone Network
REMOTE DIAL-IN USER
LOCATION "1"
Modem Bank
Authentication Server
Virtual Private Network
SAC Access Database (with backup)
SAC Administration Web Server
LOCATION "N"
Modem Bank
Authentication Server

Principal SAC System Components

The Secure Access Controller (SAC) is a system that provides secure and authenticated access to network equipment such as switches, routers, multiplexers, data transport devices, etc.
A SAC protected network offers a substantial advantage over non-encrypted and non-authenticated connections in that the equipment is protected from illegal access with substantially no risk of compromise.

The SAC system consists of five principal components:

- SAC Administration Web Server
- SAC Access Database (with Backup)
- Authentication Server (AS)
- Secure Access Modem (SAM)
- Client desktop software

SAC Administration Web Server

Access privileges to network equipment is determined by an administrator who operates the SAC Administration Web Server, typically located at a service coordination center. The Administration Web Server function includes the SAC Access Database, wherein access data and remote user accounts are stored.

SAC Access Database

Remote users must make a request of the administrator for access rights to particular network equipment. User data is then entered in the SAC Access Database for retrieval by the Authentication Servers.

Authentication Server

The Authentication Server (AS) connects to the PSTN by a modem bank. Access data obtained from the SAC Access Database allows the server to permit only authorized personnel to access the network equipment.

The Secure Access Modem

The Secure Access Modem (SAM) protects managed network equipment connected via the PSTN from malicious or unauthorized tampering by remote users.

The Client Desktop Software

The client software initiates calls to SAM and AS, sets up secure tunnels between those devices, and functions as the user's interface to the protected network equipment.

SAC System Connections

The Secure Access Modem is connected to a PSTN by voice-band modems. The Authentication Server is connected to the PSTN via a modem bank, allowing access to the server by multiple users. To minimize delay and avoid downtime, a spare authentication server can be used.

Remote User Validation

In order for the remote user to establish a connection with the protected network equipment, the following actions must occur:

1. A valid Secure Access Modem and remote user accounts must be entered in the SAC Access Database.

2. A Secure Access Modem must obtain a valid cryptographic (private) key from the Authentication Server at reset, powerup or timeout, or at the end of a session. If information in the database does not agree with information sent by the modem, the Secure Access Modem will be denied a valid private key.

3. The remote user's client software must contact the Authentication Server for verification of the User ID and Password. The authenticated user can then make a connection with the requested Secure Access Modem and the protected network equipment.

Figure 1 shows SAC architecture with SAC components and protected network equipment communicating over secure tunnels via the PSTN.

Theory of Operation

Remote User Registration

Remote users must register with the administrator to verify access privileges to certain equipment. The administrator enters remote user information into the System Access Database. The Authentication Server obtains access data from the Access Database with every access attempt.

Remote User Access

Remote users make a connection to the Authentication Server through the PSTN via a modem. The remote user employs client software to request a connection to the Secure Access Modem. This involves contacting the Authentication Server to check the user's ID and password, and then initiating a client software connection with the requested Secure Access Modem. Once the remote user is authenticated as a trusted user, the Authentication Server transfers the necessary connection data to the client software and disconnects from the user. The client software then calls the Secure Access modem and sets up a secure tunnel via the PSTN, allowing encrypted and authenticated access to the appropriate protected network equipment.

Key Generation

The Authentication Server generates public and private keys used in the SAC system. When a Secure Access Modem is powering up from a power failure, or a reset, or a key timeout, it requests a connection to the Authentication Server in order to update its private key. The Secure Access Modem uses this private key to authenticate whether the remote user is a trusted user to access the equipment. If the remote user is authenticated by the Authentication Server, then the user is sent a public key associated with the private key of the Secure Access Modem. This public key is used to communicate securely with the Secure Access Modem via a proprietary authentication protocol.

After the authentication process, a session key is set up for symmetric encrypted data communication between the remote user and the Secure Access Modem. Standard AES technique is employed in the data encryption and decryption. After the remote user has terminated the equipment access, the Secure Access Modem requests a connection to the Authentication Server to obtain another new private key, thus preventing further access from the previous remote user.

General DataComm
The Best Connections in the Business
www.gdc.com

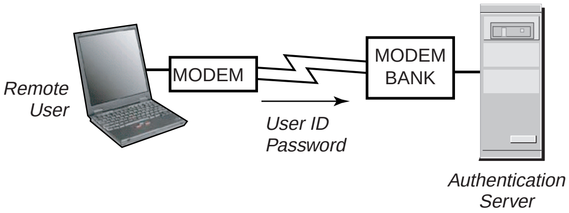
Message Flow

Background Communication

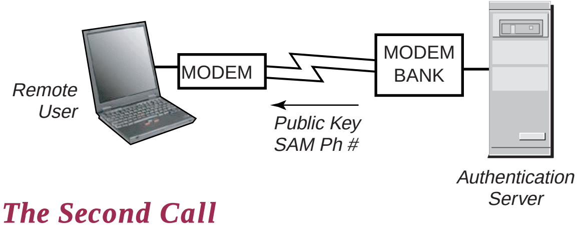
The Secure Access Modem (SAM) obtains a new private key from the Authentication Server (AS) via a secure tunnel at every power-up, reset, key time-out or session end.

The First Call

A. The remote user's client software calls the Authentication Server and is identified via encrypted communication over a secure tunnel. In the event of a hacker attempt, a secure tunnel is never established.



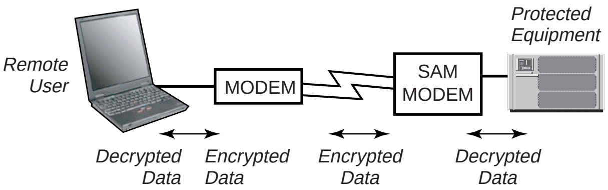
B. When the caller is authenticated, the Authentication Server sends the client the SAM phone number and its public key over the secure tunnel. The AS then disconnects the call.



The Second Call

C. Client calls the SAM and performs a public key exchange over a secure tunnel. The user may now manage the protected network equipment via the secure tunnel, employing AES data encryption:

- Client sends AES encrypted data to SAM;
- SAM decrypts data and sends it to the protected network equipment;
- The protected equipment sends data to SAM;
- SAM encrypts data and sends data to client;
- Client decrypts data and displays it to user.



Added Security

When the user terminates the management session, that public key is no longer valid.