CENTRALERT STANDARD ENCRYPTION METHOD

UNIQUE ENCRYPTION FOR EVERY DEVICE

ENCRYPTION TO KEEP YOUR TRANSMISSIONS SECURE

Each CentrAlert device has the ability to form a unique encryption key. All encryption and decryption reside in firmware stored on CentrAlert hardware, such as the CentrAlert Single Communications Link (SCL). No keys, ciphers, or certificates are stored on PCs or other non-CentrAlert hardware for the device-to-device encryption.

The current timestamp on devices (i.e. SCL) is utilized as the seed to calculate two separate indexes for each lookup key. These two indexes are processed for encrypting each byte of the payload. Since the seed utilized to get the indexes into the lookup table is based on the device's current timestamps, the encrypted data will not be duplicated for the same underlying transmission/command. This removes the ability for malicious record and playback transmissions.

Operational Features

- One Transmission for All Activations
- No Playback Threat

The CentrAlert® hardware line works seamlessly with our Crisis-Driven Alert & Control™ (C-DAC) software suite, providing both input activation controls and output notification devices. Our hardware products can also integrate third-party components for C-DAC control. Additionally, they can be installed as standalone devices for use where third-party controls are in place. We also manufacture custom devices - call CentrAlert for details.