CENTRALERT STANDARD ENCRYPTION METHOD

256-BIT ENCRYPTION TO KEEP YOUR TRANSMISSIONS SECURE

UNIQUE ENCRYPTION KEYS THAT CHANGE AT REGULAR INTERVALS

Each CentrAlert device has two 256-byte keys that combine to form unique encryption keys that change at regular intervals and each device maintains a synchronized clock that gets re-synched every week to ensure proper encrypt/decrypt functionality. All encryption and decryption reside in firmware stored on CentrAlert hardware, such as the CentrAlert Single Communications Link (SCL) and the CentrAlert Advisor Alert Radio (AAR). 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 command for all activations
- No playback threat

CentrAlert 3090 Harrodsburg Road, Lexington, KY 40503 | 859.224.1047 | info@centralert.com | centralert.com