ClearOne

APPLICATION TECH NOTE

PRODUCTS SUPPORTED:
DIALOG20® Wireless System

CLEARONE DOCUMENT NTS-0116-001 (v2)
March, 17, 2021

Encryption:

AES FIPS PUB 197 Encryption Standard: OVERVIEW

DIALOG20® Digital Wireless System

Encryption is one of the key advantages of digital wireless microphones. Anybody can remotely listen in on confidential analog wireless microphones, but the Clearone DIALOG20® Wireless system conforms to the Advanced Encryption Standard (AES) Federal Information Processing Standards (FIPS) PUB 197. This cryptographic algorithm is the U.S. federal government standard for the encryption of electronic data established by the U.S. National Institute of Standards and Technology (NIST) and it was approved by the US National Security Agency (NSA) for top secret information when used in an NSA approved cryptographic module. The Clearone DIALOG20 Wireless System uses 128 bit key, AES, always on, lab verified, FIPS 197 Standard http://csrc.nist.gov/publications/fips/fips197/fips-197.pdf .

How DIALOG20 Encryption works:

1. Each DIALOG20 transmitter and receiver pair is programmed with its own random 128-bit encryption key which scrambles the signal one of 3.4 x 10^38 (that's 340 followed by 36 zeros) different ways. The transmitter uses the key to scramble the signal before it sends it through the air and the matching receiver uses the key to de-scramble the signal back into audio. Anyone listening in will hear only white noise.

2. Transmitter and receiver pairs acquire a different random 128-bit encryption key every time they are sync'ed via the IR link. Any DIALOG20 transmitter can be sync'ed to any DIALOG20 receiver, but only one unique transmitter and one unique receiver can operate together at a time. Establishing a new random encryption key is as easy as pushing two buttons on the receiver (Then, for Podium or Boundary Mics, hold the mute button, power on, and, release mute. For Handheld or Beltpack, hold "S" button, power on, and, release "S"). If it was an agency's protocol to change the key often, there would be plenty of time during coffee breaks to re-key all the mics in a system.

3. In addition, the IR link that establishes the encryption key in the transmitter - receiver pair is itself encrypted so there is no way learn the encryption key.

4. For further security, several of the system's electronic components are protected from tampering with their own unique encryption keys. Even if the enemy was given an encryption key, it could not be programmed into a receiver.

5. All Clearone DIALOG20 systems conform to the security encryption standard AES, U.S. FIPS PUB 197.

SALES AND INQUIRIES

Headquarters
5225 Wiley Post Way
Suite 500
Salt Lake City, UT 84116

US & Canada
Tel: 801.975.7200
Toll Free: 800.945.7730
Fax: 801.303.5711

International
Tel: +1.801.975.7200
global@clearone.com

Sales
Tel: 801.975.7200
sales@clearone.com

Tech Support
Tel: 801.974.3760
tech.support@clearone.com