



Security Engineering Ltd.

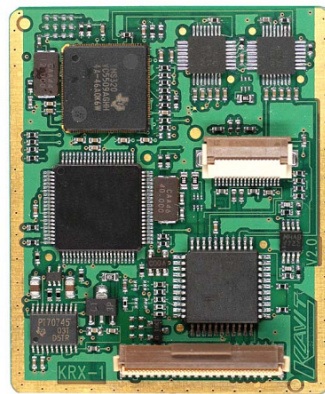
EKSE 1440 - Digital Encryption Module for Analog Radios

A professional voice digital-encryption module with very high capabilities, made especially for all Motorola Pro series (e.g. GP328/338, GP340/360, HT750/1250, PRO5150/7150 etc.).

It can also support virtually any other radio model (e.g. Icom, Kenwood, Vertex, Tait etc.). The EKSE 1440 has a top-security classification and provides excellent value for money, making it an ideal solution for military and government use.

The EKSE 1440 utilizes the latest technology to encrypt digitized voice, and has been designed specifically for two-way radio environments. The EKSE 1440 raises the security of analog radios to an unparalleled level, which up until now was available only in the most sophisticated digital radios.

The EKSE 1440 can work with existing analog repeaters and base stations (conventional, simplex, trunking, voting etc.), without having to make any changes. It is also upgradeable, which means that the EKSE 1440 will support future enhancements when they become available.





Security Engineering Ltd.

Main Features

- Unparalleled security level & cracking time, previously only available in the most sophisticated encrypted digital radios.
- Session algorithm: Stronger than Triple-DES & AES (Advanced Encryption Standard)
- Number of encryption bits (depends on the specific model): 128 bit – 512 bit 38
- Number of encryption codes (depends on the specific model): 3.4 x 10 or more
- Simple plug & play installation for all Motorola Pro series as well as any other radios that support this feature (e.g. GP328/338, GP340/360, HT750/1250, PRO5150/7150 etc.)
- Excellent voice recognition Standard digital features: Reduced static noise, negligible range loss, no lost audio, continuous late entry, improved voice quality in poor environments, etc.
- Clear/Secured: Automatically selected (in Rx mode) Supports Secure-OTAR (Over The Air Reprogramming) and Wireline programming Standard Secure-OTAR's features: Re-programming,
- KILL capability for disabling lost or stolen radio, ANI – Automatic Number Identification, etc.
- Planned support for OTeR – Over The-air encrypted Reprogramming
- Multiple encryption keys – Allows working only with the requested keys or groups, while muting incoming messages that cannot be decrypted
- Works with existing analog repeaters (conventional, simplex, trunking, voting)
- Upgradeable to support any future enhancements when available
- Can be quickly adapted to most radio models Friendly software for reprogramming the encryption keys