Paging Encryption Server

- **Secure your communications**
- **Encrypt your paging messages**
- **For health care, meet HIPAA requirements for over the air messaging**
- **128bit AES encryption**
- **Simple, web based user interface for key management**
- **Hosted service or deployed on site**

At last, the ability to encrypt paging messages to meet HIPAA requirements, and secure your transmissions.

The new Prism-IPX - Hark Tech Paging Encryption Server (PES) has arrived. Designed for carriers and larger users, the PES combines a simple web based management system with a powerful encryption server. Currently supported protocols are the Unication Flex and POCSAG formats. As other paging manufacturers provide their protocols, and as demand dictates, these will be incorporated into the system.

The PES provides standalone encrypting of paging messages. It is not tied to a particular paging switch or encoder. However, not all encoders have been tested to confirm they can encode the encrypted messages.

Messages are sent via TNPP (serial or IP) as a cap page to the PES. Based on the configuration for that cap code the PES will either pass the message unencrypted, or encrypted the message before forwarding it. Messages are returned via TNPP for encoding and dispatch.

Whilst TNPP is not an encrypted transport, when customers use the Prism-IPX IPT the TNPP packets between the IPT and the PES can be encrypted so that messages are never in the clear after leaving the customer premises.

The web interface allows varying levels of user access with differing rights. This allows for the control and security of encryption keys within the system.

The system can be deployed as a single server, or on multiple servers to provide resiliency and redundancy. Up to 4 servers can be deployed as a load balanced group offering high availability for critical services and applications.

Prism-IPX offers the PES as both a hosted solution for smaller customers and as deployed system for carriers and larger users (or end users that require their data held within the premises).