

Network Security and Encryption

Definition and Applications



NETWORK SECURITY

Security Risk: Scanning and Interception

Zeon Digital recognises that eavesdropping and interception may occur easily in some radio systems and are a threat to confidentiality. Zeon Digital network security is inherent by design. Due to the digital nature of the signal, Zeon Digital transmissions are more difficult to scan and decode than analogue counterparts.

Security Risk: Lost or Stolen Radios

Zeon Digital recognises the importance of protecting our customers against radios being used by unauthorised persons. It is likely that a considerable number of terminals will be lost every year.

Zeon Digital terminals may be disabled either temporarily or permanently over-the-air which prevents them operating until they are enabled. All radios are also capable of being protected by a PIN code. The PIN will be requested each time the radio is switched on. Three failed attempts at entering the PIN will lock the radio until the PUK code is entered.

Over-the-air disabling and PUK codes are only available by making an official request in writing on company letterhead, including customer and radio ID details, submitted to Motorola.

Lost or stolen radios can be replaced either by establishing a rental agreement or by purchasing a new radio outright which can be used to fulfil the remainder of any Zeon Digital contract (if relevant).

Security Risk: Radio Cloning

Zeon Digital recognises that masquerading as a legitimate user may occur if terminals can be cloned and the subscriber identity copied.

All Zeon Digital radios and talk groups must be authenticated on the system in order to operate. This is a continuous process, with authentication occurring every time the radio is turned on and off.

ENCRYPTION

End to end encryption is offered as a feature which allows users to be sure that their confidentiality is assured all the way through the system.

End to end encryption requires special Zeon Digital radios with an in-built Universal Crypto Module (UCM). The UCM encrypts all information at the transmitting end and then decrypts this at the receiving end. Both transmitting and receiving radios must have the UCM in order for encryption to take effect. There is no need to trust the network provider.

End to end encryption on the Zeon Digital network will provide:

- Confidentiality: the ability of the system to keep user data and traffic secret.
- Availability: The continuance of the service reliably and without interruption.
- Integrity: The system's strength in ensuring user traffic and data is not altered.

End to end encryption requires careful liaison between the customer and Motorola to ensure the customer's needs are properly met and they have the opportunity to speak directly with Motorola's engineers to completely understand the technical requirements. Fees are quoted only on a case-by-case basis once all technical specifications are agreed.



MOTOROLA