

A lot of telephone conversations and business meetings are confidential by nature. Recordings of calls however, may be accessible to different people in an organisation unless you use the CryptoCard technology to encrypt, safely store and decrypt your recordings.

All stand alone Vidicode recorders have a built in IC card reader. This can be a traditional card slot or a SIM card as used in mobile phones, or both.



There are two types of CryptoCard sets:

- The regular CryptoCard
- Crypto Card Privacy

CryptoCard

The regular CryptoCard set is usually used in desktop recorders. An employee has his own encryption and decryption card which can be inserted in the recorder and taken out when the employee leaves. This type of Crypto Card is especially suited for Call Recorders shared by different individuals who should not have access to each others recordings. Every employee has his or her own CryptoCard set which can be taken out of the recorder and stored in a safe or taken home by the employee .

The MasterCard available in this CryptoCard set allows managers to listen to all recordings of all employees by downloading them to his or her PC, entering the Master Card and PIN code and decrypt all downloaded recordings.

The MasterCard is inserted in a card reader slot on a PC, the CryptoCard regular is inserted in the Call Recorder.

CryptoCard Privacy

The Crypto Card Privacy has been developed for use in server rooms and computer rooms, especially for multi channel Recorders. Recordings are encrypted and stored on the Hard Disk of the multi line recorder. Because all recordings are encrypted, they can not be played back in the computer room or server room by unauthorised people. Recordings may also be sent via LAN to any PC without the risk of unauthorised people playing them back.

Sometimes two people share a job or a working space. They share their telephone and Call Recorder, but the recordings they make during working hours should not be accessible for their colleagues. The solution is to both keep a CryptoCard in their pocket and place it in the recorder when they come to work. Their recordings become personalised and colleagues cannot listen to them.

In some applications there might be a need to listen to all calls using a special card that can decode all other cards. This card can be kept in a very secure place and the password might even be kept in another secure place. In case of a serious emergency, all recordings are available.

Management may record meetings. The secretary has access to all recordings via the LAN. This might be considered a threat to the confidentiality of the meetings. A Crypto Card is placed in the recorder and another card is used in the PC of the secretary.

When recording is centralised using a multi channel Call Recorder, access to the recordings often is via the LAN. Normally the access is password protected. Using encryption with Crypto Cards raises the level of security far above that of password security. Both the access to confidential data and the network transportation have become secure.