PACE (MERCS)

Pocket-size Automatic Crypto Equipment

PACE is a small, pocket-sized, hand-held terminal for off-line encryption and decryption of messages, developed by Lehmkuhl in Norway (now: Kongsberg) in the early 1980s. It features a 16 character LCD screen, a 4000 character memory buffer and is fully approved by NATO. PACE is also known as the **MI-300** Cryptographic Field Terminal by **NFT Crypto** from Oslo (Norway).

The device allows secure messages to be sent over standard unprotected telephone lines and voice radio channels. It is suitable for both desktop and field use, is battery-powered and can be connected to a personal computer. It provides full error-detection and correction and is approved by NATO for all classification levels, including NATO COSMIC TOP SECRET.

PACE is interoperable with the ASCOM-mode of the RACE (KL-51) cipher machine by STK. The image on the right shows a typical PACE device as it was shown on the Kongsberg website.

The device is housed in a water-resistant aluminium case, has a full QWERTY keyboard and a 16-character LCD screen. The built-in memory can hold up to 3800 characters of either plain text or encrypted text. The unit has built-in acoustic and optical modems, allowing messages to be transferred via virtually any medium, such as phone, radio, mail or messenger service. Full error correction is built-in allowing error rates of up to 10% and burst errors up to 37 consecutive bits.

A key variable consists of 30 characters, including the key identifier and the check character at the end. More than 10^{36} keys can be used and each key produces a key stream with a period of 10^{23} bits. The encrypted output of the PACE consists of the 26 letters of the alphabet, arranged five-letter groups. Over the years, more than 20,000 PACE devices were sold to many NATO and non-NATO countries, making PACE one of the most widely used message devices in the world. The specifications below were taken from the Kongsberg website.

Features

PACE has multiple functions for:

- Encryption of free text
- MERCS application
- Authentication
- Recognition and Identification

Branding

The PACE message terminal was initially developed by Lehmkuhl in Oslo (Norway) and was known as the Lehmcoder Mini. The product may also have been sold by other suppliers as an OEM product. The latest supplier is Kongsberg. The following names are known for this product:

- Lehmcoder Mini (Lehmkuhl, Oslo, Norway)
- MI-300 (NFT Crypto A/S, Oslo, Norway)
- PACE (Kongsberg)

Accessories

The following accessories were available for PACE:

- Tempest Field Printer
- RS232 serial interface
- Radio Adapters

Technical specifications

- Modes: 7 different operational modes
- Modem: FSK, 2025/2225Hz (Bell 103)
- Memory: 2 stores, dynamically divided, 3500 characters total
- Crypto: Two NATO-approved algorithms
- Device: Unclassified, CCI
- Security: All classifications
- Key variables: Storage space for 9 keys
- Key setting: Physical (manually) or via electronic transfer
- TEMPEST: AMSG 720B-approved