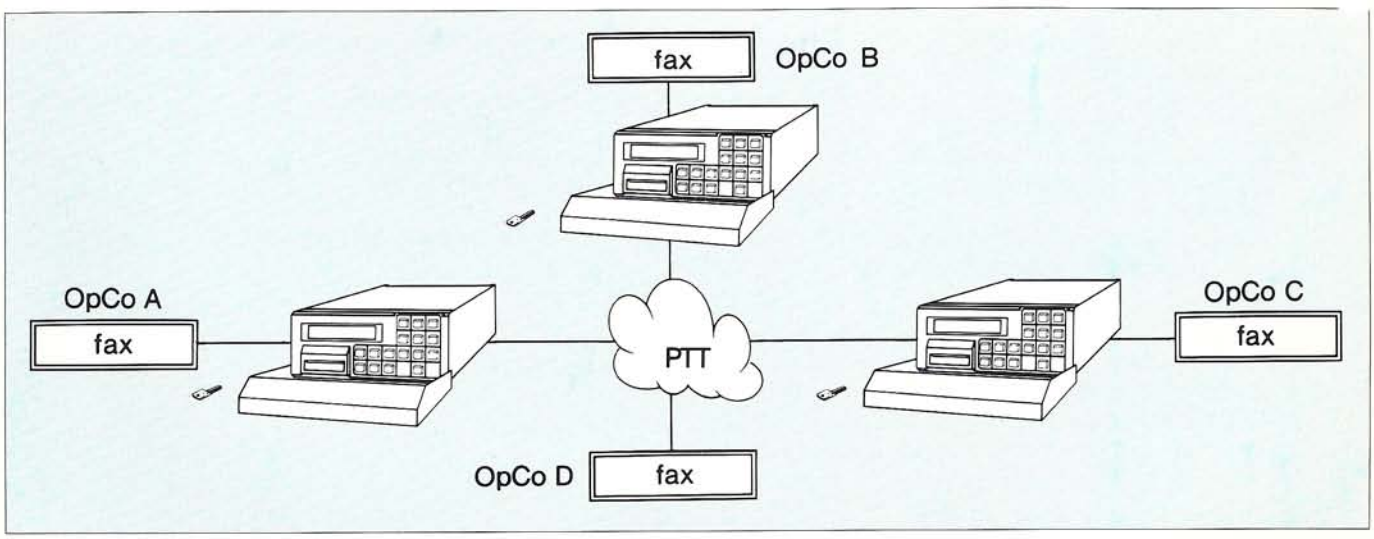
Facsimile Processing Equipment

The Facsimile Processing Equipment group 3 is a facsimile encryption device providing fax privacy. The FPE-3 is the Shell Group recommended solution where facsimile security is required. The operability and level of security provided have been tested and verified within the Shell Group environment.
The FPE-3 is connected between any group 3 facsimile terminal and the normal telephone line. Transparant transmission and reception of both plain and encrypted messages are possible, depending upon the configuration as set up. This device is simply to connect, therefore specialists are not required.

It is designed to operate internationally all over the world. Differences between the PTT networks do not influence the proper operation. It has been tested to the extent possible over international Group communications (including Inmarsat).

Below is shown that Operating Companies A, B and C have the opportunity to set up a secure communication link via their FPE-3 encryption devices. At OpCo D a FPE-3 is not installed so communication with this OpCo is only possible in plain.



Facsimile Processing Equipment

Application
- Preferred configuration programmed via softtouch keypad.
- User friendly menu structure.
- Clear indication of operational status via LCD display.
- Tamper protection by means of front cover and sealed rear panel.
- Surge protected power supply.

Security
- Access control via smart card.*
- Smart card pin-code protected.
- End to end security over public networks and satellites.
- Authentication of the other party.
- Specific key management system.
- Unique encryption key per session.
- Shell unique encryption process.
- The level of security assured by independent evaluation supervised by ICT/8.

Connectivity
- Stand-alone unit.
- Fax type independent.
- No adaptions on fax terminal.
- Simple connection to existing networks.

Operability
- Unattended operation.
- Encryption mode ON or OFF selection.
- Encryption OFF mode for compatibility with non-FPE-3 equipment.
- Automatic adaption to the processing mode of the sender.
- Standard facsimile functions retained.
- Configurations set by user friendly pull down security and installation menu.

Environment
- Desk top model.
- Normal office conditions.

For further details contact ICT/8

Key Management Structure
Key management are the procedures dealing with the generation, storage, secure distribution and application of encipherment keys in accordance with a security policy.
The key management structure is determined on the pin-code protected smart card. The smart card provides the access to the facsimile processing equipment and the key for secure communication. By entering the card into the machine an access-check is automatically executed to determine whether this smart card is authorized to use this machine.

To operate in the secure mode it is necessary that the smart cards of both the sender and receiver accept each other. Hereafter the encryption key is automatically calculated.

Two types of smart cards are available, OpCo - specific and International - OpCo.
Secure communication between OpCo and Central Offices make use of the last mentioned smart cards.

Technical data

Processing	– Automatic encryption/decryption. – Automatic key-selection system. – Pin-code protected key Information-storage on smart card.	
Interfacing	– CCITT/T40 for group 3 – 2-wire half-duplex – 300 to 9600 bps – Adjustable modem levels – V.21 modem for signalling – V.27ter/V.29 modem for message data	
Power supply	– Voltage (nominal) – Frequency – Power consumption – Surge protection	110/220/240 Vac 50/60 Hz 15 W max 80-320 V
Dimensions	– Width-Height-Depth (nominal)	215x123x355 mm

* "INNOVATRON S.A. LICENCE"

Printed in The Netherlands
Document No. 9922 154 17641

Philips Crypto B.V.
Building BAH
P.O. Box 218
5600 MD EINDHOVEN
The Netherlands
Tel: +31 (0)40 72 26 00
Telex: 35000 phte nl
Fax: +31 (0)40 72 36 58