

FAX ENCRYPTOR

PFDX 2035



Philips
Crypto



PHILIPS

PFDX 2035 Fax Encryptor for group 3 fax terminals

The 2035 is a stand-alone, fax-type independent, desktop unit which is simply connected between the fax terminal and the line, requiring no modifications to the fax equipment. It provides realtime user-to-user security for group 3 fax equipment conforming to CCITT Recommendation T.4, and also supports all normal fax functions. The unit has a 2 x 24-character LCD display and a keypad for entering functions such as the user's PIN-code, mode changes and programming.

The equipment adapts automatically to the standard fax facilities. Fax facilities and crypto settings are established by exchanging protocols, after which encryption/decryption commences automatically. For every secured transmission a unique session key will automatically be generated. These operations are carried out with the aid of Philips Crypto's advanced key management system PKMS 2000, in which each user's crypto key material is stored in a personal Smart Card* with PIN-code protection.

© Philips Crypto B.V. 1994
Data subject to change without notice
All rights reserved

**Innovatron s.a. Licence"

Philips Crypto B.V.
P.O. box 218
Building BAH
5600 MD Eindhoven
Tel.: +31 (0)40 - 722600
Fax : +31 (0)40 - 723658

Document Nr. 9922 154 19191

In the more detailed description of the communication procedure which follows, the phases and protocols towards the fax are as defined in CCITT Recommendation T.30.

- Phase A: Connection set-up.
During this phase the 2035 is transparent to the initial fax signals.
- Phase B: Pre-message procedure. The 2035 monitors and adapts the facility protocol from the fax terminal, extending it by adding crypto signalling in the 'non-standard facility' frame. This is done to check for the presence of a crypto unit at the other end of the link and to initiate the automatic key-selection procedure.
- Phase C: Message transmission. In this phase all message data are encrypted and decrypted by the 2035 units at the sending and receiving stations respectively.
- Phase D: Post-message procedure. For a multi-document message, Phase B is repeated. Encryption ceases when EQM is received from the facsimile equipment.
- Phase E: Call release. The 2035 reverts to the passive state to await the next Phase A.

Technical data

- Application**
- standard fax group 3, connected to automatic switched public/private networks and leased lines
 - proven operability on inmarsat A satellite communications
- Configuration**
- stand-alone, desktop, built-in smartcard reader
 - connected between fax equipment and line
 - no fax modifications required
 - no digital fax interface required
 - V21 modem for signalling
 - V27ter/V29 modem for message data
- User facilities**
- unattended crypto operation
 - automatic user identification
 - all standard fax facilities retained
 - user-programmable installation settings
- Crypto**
- "high end" Philips proprietary algorithm in hardware
 - customer-unique crypto algorithm (on request)
 - automatic encryption/decryption
 - key management: off line system based on smart cards
 - access control via PIN, 3 consecutive wrong PIN entries disable the card
 - key generator cycle length: >1.000.000 years
 - key diversity: >10³⁶
- Interfaces**
- fax : 2-wire half-duplex, 300 to 9600 bps. V21/V27ter/V29
 - line : see "fax "
- Power**
- voltage (nominal): 110 or 220 Vac
 - frequency: 47-63 Hz
 - power dissipation 15 VA max

