

# PPSX X.25 DATA ENCRYPTOR

# PPSX 2061 Communication Security System



Philips  
Crypto



# PHILIPS



## PPSX 2061 Data Encryptor

Philips Crypto offers standard and tailor-made solutions for securing your X.25 communications network. These solutions are based on the PPSX 2061 Data Encryptor and the matching PKMX 2008 Security Management System.

The PPSX 2061 is a compact unit which is simply plugged between de user's Data Terminal Equipment (DTE) and the network Data Communication Equipment (DCE). This unit analyses each incoming and outgoing packet and if required, isolates and encrypts or decrypts the user data, reconfigures the packet and passes it to the DTE or DCE as appropriate.

With the aid of the PKMX 2008 Security Management System, which consists of a PC with the Security Management Program, the Security Manager can control the security aspects of the secured network.

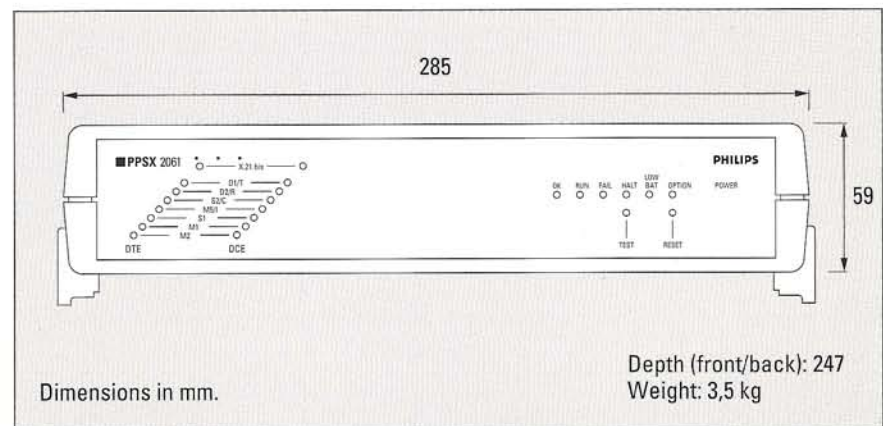
## Technical data

- |                                 |   |
|---------------------------------|---|
| Application                     | <ul style="list-style-type: none"><li>• public and private X.25 networks</li></ul>  |
| Configuration                   | <ul style="list-style-type: none"><li>• stand-alone encryption device</li><li>• security management software</li><li>• local and remote security management.</li></ul>  |
| Communication characteristics   | <ul style="list-style-type: none"><li>• encryption of upto 128 logical channels (both Permanent Virtual Circuits and Switched Virtual Circuits)</li><li>• communication speed upto 64 kbps</li><li>• local and remote management</li><li>• physical interface connections according to CCITT X.21 and X.21bis (V.24/V.28)</li><li>• full X.25 intelligence</li><li>• X.25 specifications according to CCITT 1984 and ISO 8208</li><li>• ISO 8882/2/3 conformity</li></ul>                           |
| Cryptographic characteristics   | <ul style="list-style-type: none"><li>• tamper proof hardware security module</li><li>• key management system : RSA public key</li><li>• DES encryption algorithm, other algorithms on request</li><li>• access control on in- and outgoing connections</li><li>• authentication according to CCITT X.509</li><li>• no communication data expansion during data transfer</li><li>• simultaneously secured and unsecured connections possible</li><li>• automatic recording of access logs</li></ul> |
| Security Management (PKMX 2008) | <ul style="list-style-type: none"><li>• creation of unique security domains</li><li>• automatic generation of security keys</li><li>• local and remote control of the encryption devices</li><li>• remote and local examination of access logs</li><li>• inter domain communication</li><li>• configuration management</li></ul>  |

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

**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 19321



**Philips  
Crypto**



**PHILIPS**