



DATACRYPTOR™ 2000

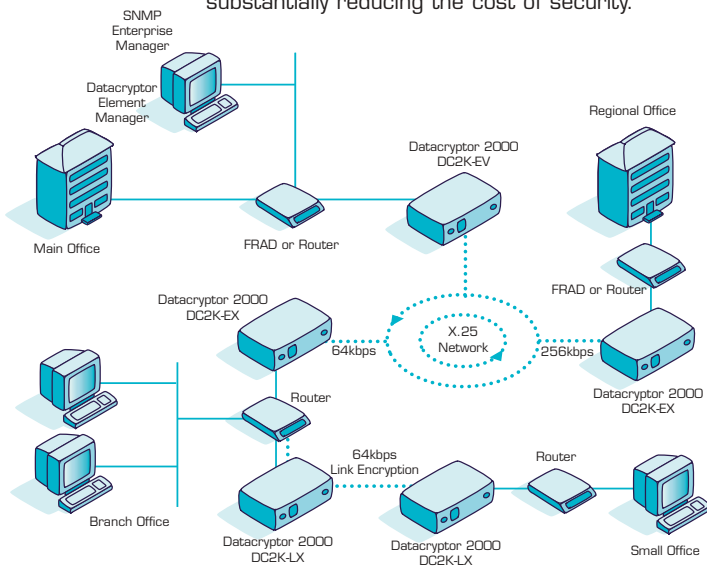
X.25 Encryptors



Are you concerned about the security of your X.25 network?

X.25 networking remains a key technology for many wide area communications infrastructures. However, as a significant percentage of these X.25 networks utilise public components, transmitted information is vulnerable to disclosure and attack.

Datacryptor™ 2000 X.25 encryptors offer secure communications on an end-to-end basis, establishing a secure virtual private network within the public X.25 network. Data is encrypted prior to transmission, remains encrypted through the network, and is decrypted at its final destination. All header and routing information is maintained 'in the clear' for proper routing of packets. This end-to-end encryption capability allows units to be installed only at endpoints of the network and not on every individual link, substantially reducing the cost of security.



Network security is enhanced since data remains encrypted throughout the network and is not exposed at switching centres.

Secure X.25

The Datacryptor™ 2000 X.25 automatically authenticates remote devices and encrypts or decrypts data.

The Datacryptor™ 2000 comes in two different models supporting the transmission of encrypted data at speeds up to 64 Kbps, and 1 Mbps. The Datacryptor™ 2000 X.25 ships with the Triple DES algorithm, the new Rijndael Advanced Encryption Standard (AES), government algorithms such as EMBATTLE, or customised cryptography.

Each Virtual Circuit (VC) handled by a Datacryptor™ 2000 is in one of three security states: secure, bypass, or standby. In standby, the Datacryptor™ 2000 does not transmit user data. In bypass it transmits user data in the clear. In secure mode, it encrypts and decrypts. The Datacryptor™ 2000 X.25 model encrypts all communications transmitted to the network for each virtual circuit, which has been configured to secure mode. Unit can support up to 1000 encrypted virtual circuits. To improve security, each encrypted virtual circuit is protected by a unique set of keys. In fact different keys are used in each direction of transmission on the same logical connection!



Technical Specifications

Maximum Data Transfer Rate	DC2K-EX: up to 64 Kbps, full duplex, synchronous RS232, RS530, V.35 or V.11 (X.21). DC2K-EV: up to 1 Mbps RS232, RS530, V.35 or V.11 (X.21).			
Maximum Packet Size	4096 bytes.			
Maximum Secure Circuits	1000 encrypted virtual circuits.			
X.25 Specifications	CCITT X.25 1980.			
Encryption Algorithm	Triple DES as standard algorithm (ANSI X9.52, 168-bit key). Rijndael (AES 128, 192, 256-bit). Other commercial or government approved algorithms available. Custom algorithms.			
Key Management	Signed Diffie-Hellman Key Agreement Protocol with 1,024-bit modulus 1,536-bit available). DSA Signature Algorithm with 1,024-bit key and 160-bit signature (FIPS 186). SHA-1 Hash Algorithm (FIPS 180). X.509 Certificates.			
Device Management	Management using PPP protocol (9-pin D serial port) or IP protocol (10 baseT RJ45 Ethernet port).			
Physical Interfaces	RS.232, RS.530, V.35, X.21 (V.11) to 1Mbps.			
Cables	Smart cables supplied (length 1m): 26-way, high-density D connectors terminating in appropriate physical connector. - RS232 (25-pin male and female D-Type connectors) - V.11, X.21 (15-pin male and female D-type) - V.35 (34 way male and female MRAC connectors) - RS530 (25 pin male and female D-Type connectors)			
Physical Security	Tamper evident case. Tamper detection envelope surrounds cryptographic module. Protection against voltage, chemical and penetration attacks. User selectable protection against compromise by theft.			
Security Certification	FIPS 140-1 Level 3. Security sub-system certified FIPS-1 level 4. FIPS 140-2 Level 3/4 and Common Criteria EAL 4 and 5 in progress.			
Power	+/-12V and +5V, less than 7W auto-sensing 110-240V AC/50-60 Hz external power supply included,			
Temperature	Operating	5°C to 40°C (40°F to 100°F)		
	Storage	-10°C to 60°C (15°F to 140°F)		
Relative Humidity	10% to 90% at 25°C (77°F) non-condensing, falling to 50% maximum at 40°C (100°F).			
Barometric Pressure	780 to 1100 mBar.			
Physical Specifications	Height	3.5 cm (1.4")	Depth	23.0 cm (9.0")
	Width	22.0 cm (8.7")	Weight	1.8 Kg (4.0 lbs.)

THALES

EUROPE, MIDDLE EAST, AFRICA

THALES e-SECURITY LTD.

Meadow View House
Long Crendon, Aylesbury
Buckinghamshire, HP18 9EQ, UK
Tel: +44 (0)1844 201800
Fax: +44 (0)1844 208550
e-mail: [emea.sales@thales-
esecurity.com](mailto:emea.sales@thales-
esecurity.com)

AMERICAS

THALES e-SECURITY, INC.

2200 N. Commerce Parkway
Suite 200
Weston, Florida 33326, USA
Tel: +1 888 744 4976
or: +1 954 888 6200
Fax: +1 954 888 6211
e-mail: [americas.sales@thales-
esecurity.com](mailto:americas.sales@thales-
esecurity.com)

ASIA PACIFIC

THALES e-SECURITY (ASIA) LTD.

Asia Pacific
Units 2205-06, 22/F Vicwood Plaza,
199 Des Voeux Road
Central, Hong Kong, PRC
Tel: +852 2815 8633
Fax: +852 2815 8141
e-mail: [asia.sales@thales-
esecurity.com](mailto:asia.sales@thales-
esecurity.com)