



DATACRYPTOR™ 2000

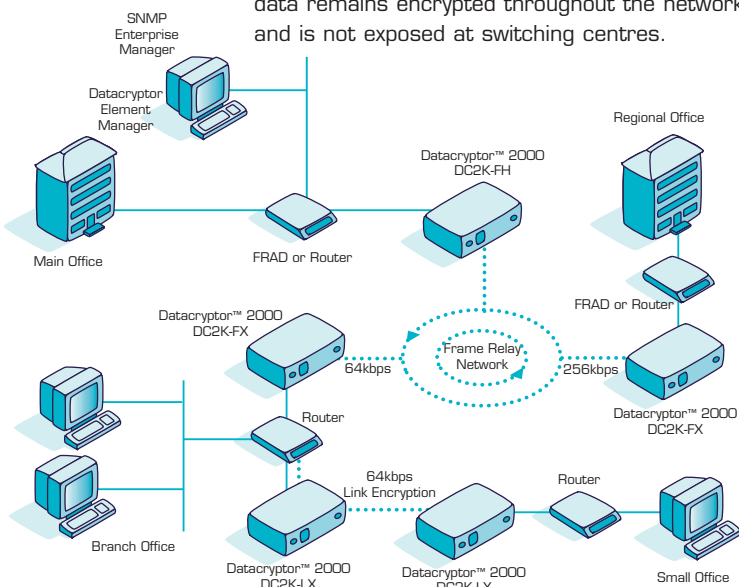
Frame Relay Encryptors



Are you concerned about the security of your frame relay network?

Frame relay technology offers distinct advantages for the wide area network. However, frame relay is a public service and transmitted information is vulnerable to disclosure and attack.

Frame relay encryptors offer secure communications on an end-to-end basis, establishing a secure virtual private network within the public frame relay 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 frames. 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.



Encryption may be selected for virtual connections that require protection while other connections remain in the clear. As a result, nodes in the network that have no privacy requirement will not require encryptors.

Secure Frame Relay

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

Depending on the model, you can transmit encrypted data at speeds up to 256 Kbps, 2.048 Mbps, or 8 Mbps. Data is encrypted using triple DES, the new Rijndael Advanced Encryption Standard (AES), government algorithms such as EMBATTLE, or customised cryptography. Each Data Link Connection Identifier (DLCI) 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 Frame Relay model encrypts all communications transmitted to the network for each DLCI which has been configured to secure mode. Each unit can support up to 992 encrypted DLCIs. To improve security, each encrypted DLCI is protected by a unique set of keys. In fact different keys are used in each direction of transmission on the same logical connection!

The Datacryptor™ 2000 Frame Relay automatically discovers the identity of peer units, address and the associated DLCI allocation of all Datacryptor™ 2000 units connected to it over the frame relay network. This feature significantly reduces configuration and management overhead.



Technical Specifications

Maximum Data Transfer Rate	DC2K-FX: up to 256 Kbps, full duplex, synchronous V.35 or V.11 (X.21) DC2K-FH: up to 2 Mbps V.35 or V.11 (X.21) DC2K-FE: up to 2.048 Mbps (E1) DC2K-FV: up to 8 Mbps V.35 or V.11 (X.21).			
Maximum Packet Size	4096 bytes.			
DLCI Allocation	DLCI	Function		
	0	LMI channel		
	1 - 15	Reserved		
	16 - 1007	User virtual circuits (up to 992 encrypted DLCIs)		
	1008 - 1022	Reserved		
	1023	In-channel layer management		
Frame Relay Specifications	FRF 1.1 User to Network (UNI) Implementation Agreement. FRF 3.1 Multiprotocol Encapsulation Implementation Agreement (MEI). I.122, [1993] [Publ.: Apr 92] - Framework for frame mode bearer services. I.233, [10/91] New [Publ: Apr 92] - Frame mode bearer services.			
Encryption Algorithm	Triple DES as standard algorithm (ANSI X9.52, 168-bit key). Rijndael AES Ready (128, 192, 256-bit) Other commercial or government approved algorithms (EMBATTLE) available. Custom algorithms.			
Encryption Mode	Self-synchronising, 8-bit cipher feedback.			
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	V.35, X.21 (V.11) to 8 Mbps. V.35, X.21 (V.11) to 8 Mbp. Unframed operation to 8 Mbps: G703 (E1 120ohm or 75ohm*). HDB3 encoding.			
Cables	Smart cables supplied (length 1m): 26-way, high-density D connectors terminating in appropriate physical connector - V.35 (34-pin male and female MRAC connector). - X.21, V.11 (15-pin male and female D-type) - E1 cable (length 3m): RJ45 connectors - E1 cable (length 2m): BNC 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 140-1 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.)

*requires optional external adapter. Specifications subject to change without notice

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

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

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