BLACK BOX®

NETWORK SERVICES

Datacryptor 2000

Key Features

- Secure Point-to-point Communications for Leased Line Links, Frame Relay, X.25 and IP Networks.
- Transparent to Data Protocols over Private or public Networks.
- Standard, high and very high speed Models are available.
- Tripple DES (168Bit) Encryption.
- Advanced Encryption Standard (AES) ready.
- Datacryptor 2000 has the flexibility to support any IP security policy, including multiple virtual private networks.

The Datacryptor 2000 range of hardware encryptors provides strong and certified perimeter security for a wide range of network architectures including dial and leased line links, Frame Relay, X.25 and IP networks (encryptors for Dial-up Lines available on request).

With triple DES (168bit) built in, or using other standards, customised, or national algorithms, it is the first family of encryption products to offer algorithm flexibility and protocol agility. This means that not only can the unit be programmed with different cryptographic algorithms as specified by the customer, but depending on the infrastructure and certain physical limitations, the same unit can be loaded to support various communications protocols. These unique features enable territory-specific algorithms to be implemented and protects the customer's investment by allowing migration to changing protocols and new algorithms including the future Advanced Encryption Standard (AES).

The IP Encryptor, the Link Encryptor, the Frame Relay Encryptor and the X.25 Encryptor models are the first and only encryptors to be AES-Ready, and have been tested to support all five candidate algorithms. These models allow customers to conveniently migrate to AES by simply performing a software upgrade on the spot or remotely, without having to return the unit to a depot. Approved to international standards including FIPS 140-1, the Datacryptor 2000 Family provides robust tamper resistance, operates at native network speeds without undue latency, and integrates easily with legacy and new networks. An integrated element management feature and Simple network Management Protocol (SNMP) compatibility also provide secure enterprise management options. Forward-looking and committed to product innovation, responsiveness, technical expertise, and value, the Datacryptor 2000 Family secures not only your business' sensitive data, but also the investment your company makes in security products for years to come.

IP Encryptor

IP Encryptor Delivers Standards-Based Security

IP Encryptor acts as a security gateway, encrypting IP packets and securely connecting as many as 1,000 destinations to provide privacy for all of the LAN resources at those 1,000 locations. Available today with 10Base-T Ethernet interfaces, a 10/100 Mbps version is planned for release in 2003. Ist standard encryption algorithm is Triple DES; optional algorithms including Rijndael (the Advanced Encryption Standard) are available as digitally-signed software upgrades. The Datacryptor 2000 Family can use custom and national algorithms, including the Embattle algorithm at UK Enhanced Grade. Packet-level encryption is performed as specified in IPsec for both Transport and Tunnel modes.

Flexibility To Match Your Security Needs

When used to protect a site, the IP Encryptor is typically installed between the protected LAN resources and the router that provides wide area access for the site. To protect an individual workstation or network segment, the IP Encryptor can be installed between that workstation or network segment and the rest of the network. The ability to install the Datacryptor between any LAN segment and the remainder of the network allows protection to be brought as close to the source of information as your security policy requires. It also allows multiple virtual private networks to be established over a shared internetwork.

Soft-Loadable Algorithms and Protocols Make the Datacryptor Future-Proof!

The IP Encryptor is the world's first IP encryptor that can be software upgraded with Rijndael, the Advanced Encryption Standard (AES). To assure that the IP Encryptor grows with your evolving network, the unit is designed and built to be field upgradeable if and when your requirements change.

Specifications

Network Protocols — IP (RFC 791), ICMP (RFC 792)
Supported IP Encryption Modes — IPsec Encapsulating Security Payload (ESP [RFC 2406]); IPsec Tunnel and Transport Modes; Trunk IP Mode (proprietary)
Key Management — Commercial – Automatic KEK and DEK exchange using signed Diffie-Hellman; UK Enhanced Grade; Unit Authentication using X.509 Certificates
Encryption Algorithms — Standard – Triple DES 168-bit (ANSI 9.52, 168-bit key).; Optional – Rijndael Advanced Encryption Standard (AES 128, 192, 256-bit); UK Enhanced Grade – Embattle Custom and National algorithms available
Device Management — 10BASE-T (RJ45) or 9-pin serial port; Element Manager, Front Panel Viewer and Certificate Manager; Crypto Manager for UKG applications; SNMP Network Management
Security Features — Tamper evident chassis; Certified Hardware Random Number Generator; Management Channel encrypted using same algorithm as Data Traffic
Security Certification — FIPS 140-1 Level 3; Security Sub-System FIPS 140-1 Level 4; CESG CAPS Approved (UK Baseline and Enhanced Grade); FIPS 140-2 Level 3/4 and Common Criteria EAL 4 and 5 in progress
Physical Interfaces — 2 x 10BASE-T (RJ45 connectors); a 10/100 Mbps version is planned for release in 2003
Regulatory — EN60950, FCC, UL and C-UL, CE, EN 50082-1, EN 55022
Power — +/- 12V and +5V, less than 10.6W auto-sensing 110-240V AC/50-60 Hz; external power supply
Temperature —
Operating: 5°C to 40°C
Storage: -10°C to 60°C
Relative Humidity — 10% to 90% at 25°C non-condensing, falling to 50% maximum at 40°C
Barometric Pressure —
780 to 1100 mBar
Physical Specifications —
H x D x W 3.5 x 23.0 x 22.0 cm
Weight 1.8 kg

Ordering information

ITEM	CODE
Link Encryptor Ethernet 10BASE-T	LES950AE

Link Encryptoors

Secure Communications
The Link Encryptor models are designed to protect data transmitted over leased lines. The Datacryptor 2000 Family will authenticate remote devices and encrypt and decrypt transmitted data. Depending on the model, you can transmit encrypted data at speeds up to 512 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 customized cryptography.

Each logical link handled by a Link Encryptor is in one of three security states: secure, bypass, or standby. In standby, the Link Encryptor does not transmit user data. In bypass it transmits user data in the clear. In secure mode, it encrypts and decrypts. The Link Encryptor models encrypt all communications sent to the network and decrypt all communications arriving from the network; they are transparent to data protocols. In framed T1/E1 applications, each sub-channel is a separate logical connection with its own security state. Highly scalable the Datacryptor 2000 has been designed to support a wide variety of network applications.

Specifications

Maximum Data — DC2K-LX: up to 512 Kbps, full duplex, synchronous.
Transfer Rate —
DC2K-LH: up to 2 Mbps.
DC2K-LT: up to 1.544 Mbps (T1).
DC2K-LE: up to 2.048 Mbps (E1).
DC2K-LV: up to 8 Mbps.
Encryption Algorithms — Triple DES as standard algorithm (ANSI X9.52, 168-bit key); Rijndael (AES 128, 192, 256-bit); Other commercial or government approved algorithms available. (EMBATTLE): or 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. Hardware random number generation.
Device Management — Management using PPP protocol (9-pin D serial port) or IP protocol (10 Base-T RJ45 Ethernet port).
Physical Interfaces — RS-232 (V.24), RS530 V.35, X.21 (V.11) to 512 Kbps; Unframed or framed operation to 2.048 Mbps: G703/4 (E1 and T1 balanced); Unframed operation to 8 Mbps: V.35 or V.11 (X.21); Externally clocked T1-ESF or T1-D4 Framing; B8ZS line coding; FDL performance messages. (ESF); E1-HDB3 encoding.
Cables — T1/E1 cable (length 3m): RJ45/RJ48C connectors on both ends. Smart cables (length 1m): 26-way, high-density D connectors terminating in
- RS-232 (25-pin male and female D-type)
- V.35 (34-pin male and female MRAC connector); - X.21, V.11 etc. (15-pin male and female D-type)

Synchronisation — Automatic, continuous.
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
Storage -10°C to 60°C
Relative Humidity — 10% to 90% at 25°C non-condensing, falling to 50% maximum at 40°C.
Barometric Pressure —
780 to 1100 mBar.
Physical Specifications —
H x D x W 3.5 x 23.0 x 22.0 cm
Weight 1.8 Kg

Ordering information

ITEM	CODE
Link Encryptor High Speed E1	LES955AE
Link Encryptor Channelized E1	LES961AE

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 Encryptor offers 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 Frame Relay Encryptor 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 Frame Relay Encryptor is in one of three security states: secure, bypass, or standby. In standby, the Frame Relay Encryptor does not transmit user data. In bypass it transmits user data in the clear. In secure mode, it encrypts and decrypts. The Datacryptor 2000 Family models encrypt 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 Frame Relay Encryptor automatically discovers the identity of peer units, address and the associated DLCI allocation of all Frame Relay Encryptor units connected to it over the frame relay network. This feature significantly reduces configuration and management overhead.

Specifications

Maximum Data — DC2K-FX: up to 256 Kbps, full duplex, synchronous V.35 or V.11 (X.21)
Transfer Rate —
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 — FRF 1.1 User to Network (UNI) Implementation Agreement.
Specifications — 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 — Triple DES as standard algorithm (ANSI X9.52, 168-bit key).
Algorithm — 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 — V.35, X.21 (V.11) to 8 Mbps. V.35, X.21 (V.11) to 8 Mbp.
Interfaces — Unframed operation to 8 Mbps: G703 (E1 120Ω or 75Ω*). 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 — FIPS-140-1 Level 3.
Certification — 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
Storage -10°C to 60°C
Relative Humidity — 10% to 90% at 25°C non-condensing, falling to 50% maximum at 40°C
Barometric Pressure —
780 to 1100 mBar
Physical Specifications —
H x D x W 3.5 x 23.0 x 22.0 cm
Weight 1.8 Kg

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

Ordering information

ITEM	CODE
Link Encryptor Frame Relay, E1/X.21/V.35	LES972AE
Further models on request.	

X:21 Encryptor

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. 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 X.25 Encryptor automatically authenticates remote devices and encrypts or decrypts data. The Frame Relay Encryptor comes in two different models supporting the transmission of encrypted data at speeds up to 64 Kbps, and 1 Mbps. The X.25 Encryptor 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 X.25 Encryptor is in one of three security states: secure, bypass, or standby. In standby, the X.25 Encryptor does not transmit user data. In bypass it transmits user data in the clear. In secure mode, it encrypts and decrypts. The X.25 Encryptor 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!

Specifications

Maximum Data — DC2K-EX: up to 64 Kbps, full duplex, synchronous RS232, RS530, V.35
Transfer Rate — 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 — 1000 encrypted virtual circuits.
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 (10BASE-T 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
Storage -10°C to 60°C
Relative Humidity — 10% to 90% at 25°C non-condensing, falling to 50% maximum at 40°C.
Barometric Pressure —
780 to 1100 mBar.
Physical Specifications —
H x D x W 3.5 x 23.0 x 22.0 cm
Weight 1.8 Kg

Ordering information

ITEM	CODE
Link Encryptor X.25	on request

These Products are produced by Thales E-Security.

Black Box Network Services - The world's largest network services company

We are, with 25 years of experience, the world leader in network infrastructure services.

On the Phone — no charge, answer calls in less than 20 secounds, find the right product with our technical experts.

On-site — superior design and engineering, Certified installations, end-to-end service.

On-line — receive techincal knowledge on-line, including technology overviews, BLACK BOX Explains and the Knowledge Box.

Most comprehensive TECHNICAL SUPPORT — our best Product! Free hotline TECH SUPPORT!

The world's best customer service — Custom design services and products, the best warranties, money-saving discount programs.

BLACK BOX exclusives — Certification Plus. Guaranteed-for-life products and services.