

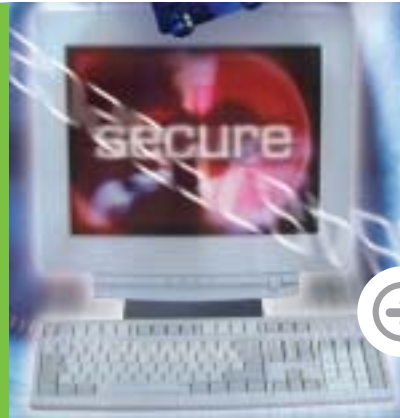
## THE DATACRYPTOR™ 2000 FAMILY



### Next Generation Encryption

- Soft loadable capability protects initial hardware investment
- AES ready
- Support for a full range of network protocols for Public and Private networks
- Support for diverse encryption standards
- Designed to the highest security standards, FIPS, CAPS and Common Criteria
- Physical integrity ensured
- Developed from 20 years of WAN encryption experience

# → THE DATACRYPTOR™ 2000 FAMILY



## Thales Understands Network Security

In a world where information is becoming increasingly important to businesses and governments, it is vital that foolproof security mechanisms be used to ensure

data privacy. Consider a large brokerage firm or a major bank; each deals with sensitive client transactions – information that travels across networks. If this information is compromised, individuals or companies could be ruined. Government institutions are another sector that deals with highly confidential and economically sensitive information. A breach in security due to disclosure over a network would be devastating. Networks are a vulnerable but necessary component of today's sophisticated information age. The key to eliminating this vulnerability is to protect information as it travels across the network using encryption techniques. Unlike solutions that protect only one application or protocol, network security products protect everything that is sent or received over a virtual or physical connection. For businesses and institutions that deal with sensitive information, using encryption to secure information isn't just a requirement; it's an absolute necessity.

Thales has spent 20 years protecting wide-area network communications for governments, financial institutions, and information-critical industries worldwide. It was one of the first companies to introduce a link encryption product to the market in the early '80s, and with over 60,000 network security devices in operation, Thales is a global leader in the network security market. It's this kind of experience and expertise that is built into Thales' next generation network security devices, the Datacryptor™ 2000 family.

## Flexible Solutions to Global Security Requirements

The Datacryptor™ 2000 family offers products that support private and public networks including Leased Line, Frame Relay, X.25 and IP. It also solves the issue of diverse algorithm standards by offering the only network security product with soft loadable encryption algorithms. Datacryptor™ 2000 customers can easily migrate from Triple DES to the new Rijndael Advanced Encryption Standard (AES) and retain their initial investment in hardware. In addition to planning for the future, the Datacryptor™ 2000 family supports Triple DES, its predecessor DES, and other algorithms employed by governments such as, Embattle, baton, Redpike, SAFER SK, and SKIPJACK.

Every Datacryptor™ 2000 we manufacture contains the Digital Signature Algorithm (DSA) and the Secure Hash Algorithm (SHA-1) to allow digitally signed firmware to be loaded electronically. Digital Signatures provide state-of-the-art protection for the logical integrity of the product while still providing the benefits of flexibility.

Flexible cryptography lengthens the life of the Datacryptor™ 2000. It also shortens the time to implement new encryption algorithms, while preserving top hardware-based encryption performance.

In order to meet the demanding requirements of global customers, the Datacryptor™ 2000's crypto engine, the SafeGuard Security Subsystem, is certified FIPS 140-1 Level 4. The unit overall is rated at Level 3. Approval under the new FIPS 140-2 process is ongoing. The Physical and Logical Security of the Datacryptor™ 2000 is so strong, Governments bank on it. A UK Government version of the Datacryptor™ 2000 using the Embattle algorithm is CAPS approved.

## Designed for Performance

Because the Datacryptor™ 2000 is based on a special processor to accelerate encryption, there is minimal delay or extra bandwidth consumed for encryption. Datacryptor™ 2000 excels at the most demanding applications such as voice over Frame Relay. Users can tailor device selection to performance requirements paying only for the throughput required. Standard, high-speed, and very-high speed models are offered across the product line. Datacryptor™ 2000 Link encryptors secure information being transmitted over point-to-point communication networks with transfer rates of 512 kbps, 2.048 Mbps, and 8 Mbps respectively. Similarly, Frame Relay network support is provided by Datacryptor™ 2000 Frame Relay products with 256 kbps, 2.048 Mbps, and 8 Mbps transfer rates. Datacryptor™ 2000 X.25 encryptors establish a virtual private network within the public X.25 network and offer transfer speeds of 64 kbps, and 1 Mbps. The

Datacryptor™ 2000 IP performs IP packet level encryption over 10BaseT Ethernet connections at speeds up to 5 Mbps, a 10/100 baseT unit will be available in Q4 2002



## Guaranteed Ready for AES

The Datacryptor™ 2000 family is designed to preserve your investment by permitting soft upgrade to new encryption schemes or protocols. Based on Field Programmable Gate Array (FPGA) technology that allows digitally signed firmware to be loaded electronically from local or remote sites, Datacryptor™ 2000 products are the only network security devices available today that allow customers to migrate to the Rijndael (AES) algorithm without the costly process of removing, upgrading, and reinstalling hardware. This soft migration path provides significant cost savings and convenience.

## Protocol Agility

The Datacryptor™ 2000 can support our complete range of communication protocols. For example, customers currently using Frame Relay with plans to migrate to IP can purchase a properly configured Datacryptor™ 2000 and install our Frame Relay protocol today. When it's time for IP, install the IP protocol software, plug in your cables and connect to the Ethernet! This unique capability ensures that your investment is protected against the certainty of network migration.



## Flexible Management and Support

Thales gives you the flexibility to use industry leading SNMP enterprise management tools such as HP OpenView NNM, or SNMP-c to locally or remotely monitor Datacryptor™ 2000 products. You are free to select the management tool that best meets your needs. For instance, if you already have an existing SNMP enterprise management system, there is no need to purchase management from Thales. At no additional cost, Thales' Datacryptor™ 2000 Element Manager will smoothly integrate into existing SNMP systems. The Element Manager is a user friendly, pull down GUI interface, compatible with Windows 95/98 and NT that provides secure configuration and setup functions for Datacryptor™ 2000 products. On the other hand, if your network is segmented or does not already have an SNMP manager, then Thales integrates the SNMP-c management system including the Datacryptor™ 2000 Element Manager, providing a cost-effective solution. If you are implementing a small number of encryptors, an SNMP management system may not be necessary. In this case, you can simply rely on the Datacryptor™ 2000 Element Manager for the management of the encryptors. The choice is up to you; there's no need to unnecessarily duplicate expensive enterprise management with the Datacryptor™ 2000 family.

The ability to monitor and diagnose issues quickly is of utmost importance particularly when dealing with information security. The Datacryptor™ family offers a variety of diagnostics to ensure troublefree operation. Testing can be performed on-site or remotely. Log files track unit operation and events and can be printed using the

Datacryptor™ 2000 Element Manager or an SNMP manager. Sorting mechanisms allow recorded data to be categorized by date/time, log entry or a combination of these and other available fields.



In addition to a complete set of diagnostics, Thales offers service and support plans tailored to customer requirements. Thales offers many service options including 24 by 7 or normal business hour on-site support, and technical telephone support. Thales service personnel are experts in network security products and are committed to helping information critical businesses protect its most valuable asset – information.

## Streamlined Tamper-Resistant Design

Every Datacryptor™ 2000 product is designed to be tamper resistant. From inside to outside, the unit is constructed to sense and prevent harmful intrusions. Each unit is sealed in a tamper evident case. To detect penetration inside the case, the crypto module and tamper sensors for motion, temperature, voltage, and chemical attacks are housed in a tamper resistant envelope. The entire envelope is surrounded by a thin film, which is coated in opaque epoxy. Any compromise to this module triggers a critical alarm. To prevent compromise all keys are erased, which renders the unit unusable until re-commissioned. Transport sensors detect unauthorized movement of the units and also trigger critical alarms. These sensors can be turned off if motion detection is not needed. Thales has taken every precaution to ensure that the physical integrity of its products are not breached.

# THE DATACRYPTOR™ 2000 FAMILY

## Secure Key Management

The Datacryptor™ 2000 family utilizes sophisticated key management techniques to prevent infiltration and attack. All key management functions comply with industry standards specified for governments, financial institutions, and organizations with stringent information security requirements. For the Datacryptor™ 2000 Link, Frame Relay, X.25, and IP products, key management is based on the Diffie-Hellman key agreement protocol and the DSA Signature Algorithm with signed X.509 certificates to manage key exchanges. Keys are generated using a hardware random number generator. To provide maximum security and flexibility, keys can be automatically changed at user defined intervals.



The Datacryptor™ 2000 Certificate Authority (CA) is used to generate X.509 certificates for the units in the network. This application allows the user to transfer the root authority, add or delete certificate authorities, certify a unit key set, load Diffie-Hellman parameters, and delete key sets. Thales e-Security recommends that every user takes control of their own security. However, for those networks that do not require establishment of a closed community of units, the Datacryptor™ 2000 can

be used as supplied. The Datacryptor™ 2000 may be remotely managed. Both serial and Ethernet control ports are available that support PPP and IP, respectively, providing the ability to monitor unit status using an SNMP-based enterprise manager, or to launch the Datacryptor™ 2000 Element Manager.

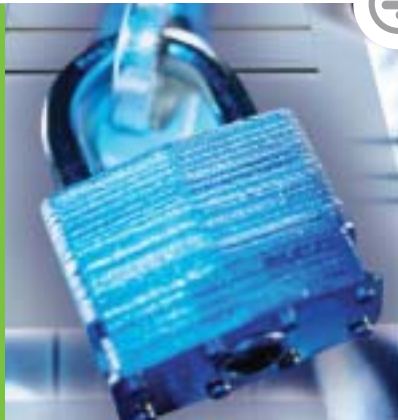
## Advanced Diagnostics

A variety of diagnostics are available to maintain trouble-free operations. Log files are maintained in the Datacryptor™ 2000 and can be viewed or printed with the Element Manager or an SNMP manager. Data can be sorted by date/time or by log entry type or by a combination of these and other available fields.

## Guaranteeing the Future

Thales and the Datacryptor™ 2000 family offer versatile encryption solutions designed for the future. Thales offers the only cryptography solution that will allow users to seamlessly migrate to the new Rijndael (AES) algorithm while preserving the initial hardware investment. Any business that transmits sensitive information across networks can't afford to ignore the future. The future is now with the Datacryptor™ 2000 family.

It matters from which company you select your network encryption solutions. Thales has been providing data security solutions since 1980. Longer than anyone else in the business. To Governments, to over 70% of the world's banks, to industry... to customers that are the 'who's who' in communicating valuable information. With over 60,000 network encryption devices in continuous operation every day, Thales protects transactions, large and small, on every continent and in virtually every country of the world. Moving money, transmitting State secrets, protecting personal data. In fact, Thales' Datacryptor™ 64 family of encryption devices has protected some of the world's largest secure networks for more than a decade. We have taken that experience and the lessons learned in all of these critical applications to produce a new generation of encryption devices, the Datacryptor™ 2000. Security to match the most stringent needs, easy to install, easy to manage, compact and cost effective. And electronically upgradeable to keep pace with changes in algorithms, standards and protocols.



## Datcryptor 2000 Link, Frame Relay, and IP

- Secure data communication using Triple DES (168-bit)
- Rijndael-AES ready on same hardware platform (128, 192, 256-bit)
- Government and customized algorithms
- Signed Diffie-Hellman key exchange
- Digital Signatures (DSA, SHA-1)
- Digital Certificates (X.509)
- Compatible with SNMP managers
- Secure remote management
- FIPS 140-1 Level 3 / Security Sub-System certified FIPS-1 Level 4
- FIPS 140-2 (under evaluation)
- Common Criteria EAL 4 and 5 (under evaluation)



# 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)