THALES

Datacryptor®
AP Layer 3
IP Encryptor

www.thalesesec.com

Technical Specifications

	Datacryptor® AP 10/100 Mbps IP
Cryptography	Standard – AES (128, 192, and 256-bit) Standard – 3DES (168-bit) Custom and national algorithms available CBC and CFB8 mode
Protocols	Diffie-Hellman key exchange Tunnel mode Transport mode
Key Management	Automatic KEK and DEK exchange using signed Diffie-Hellman Unit authentication using X.509 certificates
Physical Interfaces	Host and network ports: Back panel 2 x full-duplex 10/100BaseT RJ-45 Maximum encrypted throughput: 186 Mbps. Management: Back and front panel serial RS-232 Back panel 10BaseT Ethernet RJ-45
Device Management	THALES' Element Manager: Secured with AES or 3DES In-band and out-of-band management Front Panel Viewer GUI Secure download of software updates SNMP network monitoring THALES' Certificate Manager
Security Features	Tamper proof cryptographic Tamper evident chassis Hardware Random Number Generator Management channel encrypted using same algorithm as data traffic (AES/3DES)
Certifications	FIPS 140-2 Level 3 International Common Criteria EAL 4 UK CAPS Enhanced Grade (Secret)
Regulatory	Safety: EN60950, UL and CE Emissions: FCC part 15 class B EN 55024 / EN 55022
Power	Standard internal power supply Auto-sensing 110-240V AC/50-60 Hz Optional internal power supply 48V DC
Environmental	Operating temperature: 5° C to 40° C (23° F to 100° F) Storage temperature: -10° C to 60° C (14° 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 1,100 mBar
Physical Specifications	Height: 4.20 cm. (1.65 in.) - 1U Width: 42.95 cm. (16.90 in.) - 19 in. rack mount Depth: 22.25 cm. (8.76 in.) Weight: 8 lbs. (3.63 kg)

Why Choose Thales and the Datacryptor® Product Line

Why Thales?

Because Thales Group employs 60,000 people in nearly 50 countries worldwide, with revenues of over $12 billion.

What does that mean to you, the customer?

It means we invest significant revenue into product research and development, thereby providing our customers with the latest in technology. It means that we are here for the long haul providing our customers with the knowledge that their investment in our products is safe. It means our clients and customers have bought Thales products because they trust Thales to deliver.

Why the Thales Datacryptor product line?

Because the Datacryptor employs state of the art encryption technology with the strongest commercially available algorithms, the Federal Information Protection Standard (FIPS)-approved Advance Encryption Standard (AES 256-bit strength) algorithm and industry standard automatic key exchange mechanisms.

Why the Datacryptor?

Because the Datacryptor is a proven family of certified cryptographic appliances that provide encryption protection to a range of communications infrastructures, all models use the same standard Element Manager application for secure commissioning, monitoring, and control of the fielded encryptors, no matter which model is deployed. Because the management application is included with the Datacryptor at no additional cost to the customer, the products are competitively priced, and the single management application greatly simplifies the job of the network manager and makes for simplified training and maintenance.

>> LAYER 3 IP DATACRYPTOR SOLUTIONS

Thales Understands Network Security

In today's world, government, military and civilian organizations require a secure, manageable, and highly scalable network. Thales understands network security as it has spent more than 25 years protecting wide-area networks for federal agencies, state and local governments, financial institutions, and businesses that require the protection of critical data in transit.

Innovative Technology for Mission Critical Networks

Networks are vulnerable, but a 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. The Thales Datacryptor® product line provides the assurance required to protect your mission critical networks. Thales is the recipient of the Technology Leadership Award in the field of encryption in recognition of the company's development of the innovative, industry-leading Datacryptor product line.[1]

Regulatory Compliance

In the United States, the federal government has issued a series of directives and mandates to ensure that data in transit is protected. Network security, however, is just not a federal government issue, state and local governments and financial institutions are also making significant changes to protect their critical data.

Regulations protecting the security of this data, as it moves across networks, have been passed in all of the major Homeland Security infrastructure areas. The following key directives are driving the mandates for the use of robust encryption in the government and financial markets.

Federal Government

- Department of Defense Directives DoD 8500.2 and DoD 8100.2 - Mandate encryption on communication devices and wireless links.
- Presidential Decision Directive 63 (PDD-63) - Require technology solutions to ensure protection of national critical infrastructure.
- Federal Bureau of Investigation – Criminal Justice Information System (CJIS) – All criminal data must be encrypted using FIPS 140-2 equipment employing the AES encryption algorithm.

State and Local Government

- California SB 1386 - Security Breach Information Act - Requires an agency, person or company that conducts business in California and owns or licenses computerized "personal information" to disclose a breach of unencrypted personal information.

Financial

- Gramm-Leach-Bliley Act and the Securities and Exchange Commission (SEC) regulations mandate encryption of consumer data on leased lines and dedicated circuits.
- Sarbanes-Oxley (SOX) - Requires all publicly traded company executives, auditors, and IT divisions to incorporate policies/processes to protect company financial data.
- International Regulation

  1. European Union (EU) Data Protection Directive (02/58/EC) – Requires information protection within EU countries and organizations conducting business with EU members.

1. Frost & Sullivan 2005 Technology Leadership Award

2. Basel II – Requires global financial services companies within the EU to implement information security mechanisms within its branches in and outside the EU.

3. Canadian Personal Information Protection and Electronic Document Act (PIPEDA) – Mandates the protection of personal sensitive data in commercial organizations.

4. Asia Pacific Forum on Privacy and Data Protection – Affects all businesses that collect personal data from their customers.

Why Layer 3 IP?

Layer 3 applications are appropriate for meshed network architectures, which allow the customer the ability to leverage the public infrastructure to connect to multiple sites. Thales provides a full range of IP-based encryption solutions, which can be deployed in large scale network architectures.

Key Advantages:

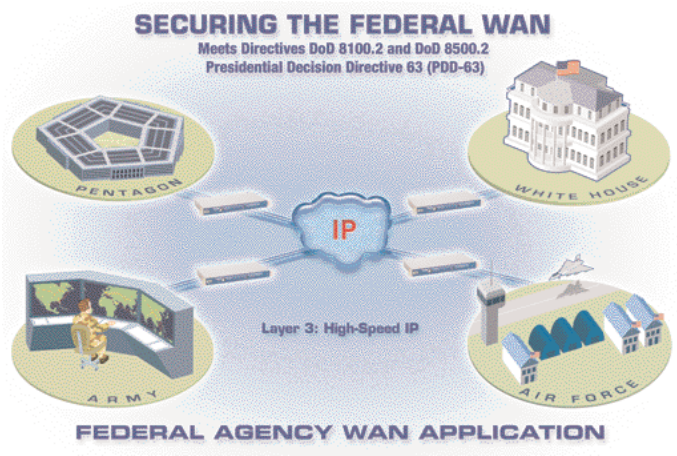
- Connect multiple sites over public infrastructure
- Ideal for wireless and wireline communications
- Ability to aggregate satellite offices

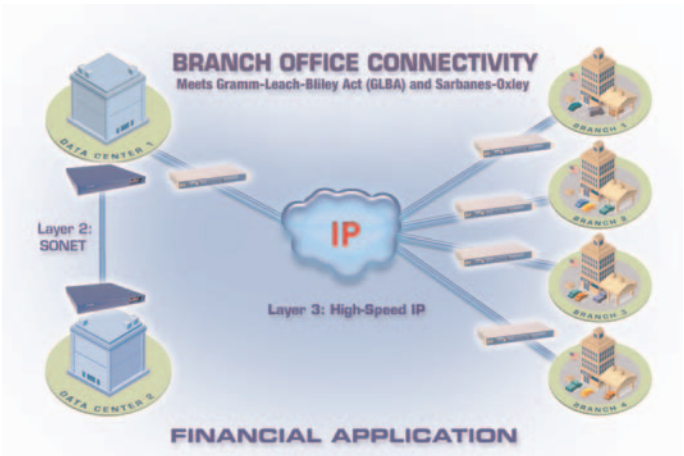
Target Applications

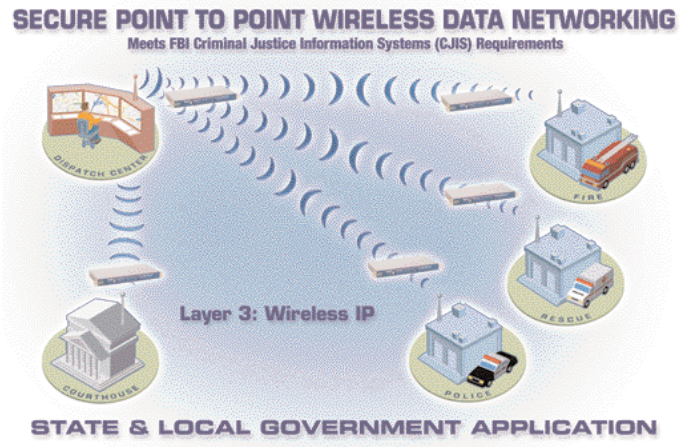
The Datacryptor product family can be deployed in any application that needs to protect data in transit. The ideal deployments are site-to-site, linking multiple buildings in a campus or linking campuses to each other in a Metropolitan Area Network (MAN), wireless point-to-point and voice over IP (VoIP) applications.

Datacryptor AP 10/100Mbps Encryptor

Datacryptor AP (Advanced Performance) 10/100 Mbps enables the benefits of IP networking to securely extend the reach of the customer's network to branch offices and businesses. Datacryptor AP is available in 10 and 100 Mbps models. The 10 Mbps model is also upgradeable to 100 Mbps for highly meshed architectures.







The Datacryptor AP 100 Mbps can aggregate lower-speed Datacryptor AP 10 Mbps devices. The 100 Mbps model provides up to 186 Mbps full-duplex performance with less than 7 microseconds of latency.

The solution is ideal for video, voice, data, as well as Command, Control, Communications, Computers, Intelligence Surveillance, Target Acquisition, and Reconnaissance Systems (C4ISTAR) applications.

Datacryptor Wireless Encryptor

As Wireless WAN (WWAN) solutions in a fixed and tactical deployment continue to proliferate, Thales once again is first to market. Thales offers an encryption solution exclusively targeted at WWAN applications. The solution has been tested by the leading wireless vendors and has already been deployed by many agencies. The architecture of this model has been optimized for wireless applications which utilize a single tunnel to connect two endpoints. The Datacryptor is ideal for base surveillance, voice, and video applications.

Secure Key Management

The Datacryptor family utilizes sophisticated key management techniques to prevent infiltration and cyber attacks. All key management functions comply with industry standards specified for governments, financial institutions, and organizations with stringent information security requirements. The Datacryptor uses key management techniques based on the Diffie-Hellman key agreement protocol and the Digital Signature Algorithm (DSA) with signed X.509 certificates to manage key exchanges. The Datacryptor Certificate Authority (CA) is used by the Datacryptor AP 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 keys.

Flexible Management and Support

Thales gives you the flexibility to use industry leading Simple Network Management Protocol (SNMP) enterprise management tools such as HP OpenView, or SNMP-c to locally or remotely monitor all Datacryptor products. Customers are free to select the management tool that best meets their needs. For instance, if one already has an existing SNMP enterprise management system, there is no need to purchase management from Thales. At no additional cost, Thales' Datacryptor Element Manager will smoothly integrate into existing SNMP systems. The Element Manager is a Windows-compatible user friendly, Graphical User Interface (GUI), that provides secure configuration and set-up functions for all Datacryptor products. If one is implementing a small number of encryptors, an SNMP management system may not be necessary. In this case, one can simply rely on the Datacryptor Element Manager for the management of the encryptos.

Service and Support

Thales is committed to delivering the highest level of service to its customers, providing unparalleled support for the entire range of Datacryptor products. The services provided include network design assistance, installation, training and post sales support. The Thales team of experienced engineers are network security experts. Our support team continually receives excellent reviews from our customers, as customer satisfaction is a key priority in our business. Thales is ready to support you with reliable and efficient service when you need it.

AMERICAS
2200 N. Commerce Parkway
Suite 200
Weston
Florida 33326
USA
Tel: +1 888 744 4976
+1 954 888 6200
Fax: +1 954 888 6211
e-mail: sales@thalesesec.com

Publication No: 1635-PSOA/0107/11214

THALES