



## La familia **Datacryptor™ 2000**

### Nueva Generación de Codificadores



- Capacidad programable garantiza la inversión del cliente
- Listo para algoritmo AES
- Apoya toda una gama de protocolos de comunicación
- Apoya diversos algoritmos de codificación
- Diseñado al más alto estándar de protección, FIPS 140-1, Nivel 4
- Seguridad física asegurada
- 20 años de experiencia en el desarrollo de codificadores

# La familia Datacryptor™ 2000

## Thales entiende seguridad de redes

En un mundo en que la información es cada vez más importante para los negocios y los gobiernos, es fundamental que se utilicen mecanismos infalibles de seguridad para garantizar la protección de los datos. Por ejemplo, tanto las firmas de corretaje financiero como los grandes bancos realizan transacciones sensibles con sus clientes, y esta información viaja a través de redes. Si estos datos se ponen en peligro, las personas o las compañías podrían quedar arruinadas. Las instituciones gubernamentales constituyen otro sector en el que se maneja información altamente confidencial y delicada desde el punto de vista económico. Para estas instituciones sería devastador que su seguridad se viera resquebrajada al quedar expuesta en una red. Las redes son un componente vulnerable, pero necesario, de la sofisticada era de la información en que vivimos. La clave para eliminar esta vulnerabilidad consiste en proteger la información que viaja por las redes, mediante el uso de técnicas de codificación. A diferencia de las soluciones que sólo protegen una aplicación o protocolo, los productos de seguridad de redes protegen todo lo que se envía o se recibe a través de una conexión, sea ésta virtual o física. Para los negocios e instituciones que manejan información sensible, el uso de la codificación para asegurar la información no es un simple requisito, sino una necesidad absoluta.

THALES lleva veinte años protegiendo las comunicaciones a través de redes de área extendida de gobiernos, instituciones financieras e industrias que manejan grandes cantidades de información en todo el mundo. Fue una de las primeras compañías que introdujo en el mercado un producto de codificación de enlaces, a principios de los años

80. Por otra parte, con más de 60,000 dispositivos de seguridad de redes en operación, THALES es una empresa líder en el mercado de seguridad de redes. Su nivel de experiencia y de conocimientos técnicos está incorporado en la próxima generación de dispositivos de seguridad de redes de THALES, la familia Datacryptor 2000.

## Soluciones flexibles para los requisitos globales de la seguridad

La familia Datacryptor 2000 incluye productos que se pueden aplicar a redes privadas y públicas, como Lease Line, X.25, Frame Relay e IP. También soluciona el problema de la diversidad de normas de algoritmos, pues ofrece el único producto de seguridad de redes que cuenta con algoritmos cargables de codificación. Los clientes de Datacryptor 2000 pueden migrar fácilmente de Triple DES a la nueva Norma Rijndael de Codificación Avanzada (AES) y conservar así su inversión inicial en equipos. Además de planificar para el futuro, la familia Datacryptor 2000 acepta la norma Triple DES, su predecesora DES, y otros algoritmos utilizados por los gobiernos, como Embattle, Redpike, SAFER SK y SKIPJACK.

Cada Datacryptor 2000 que producimos contiene el Algoritmo de Firma Digital (DSA) y el Algoritmo Seguro de Hash (SHA-1) para permitir que los soportes lógicos firmados de forma digital se carguen electrónicamente. Las Firmas Digitales ofrecen protección de primera línea a la integridad lógica del producto al mismo tiempo que brindan la ventaja de la flexibilidad. La criptografía flexible hace que se alargue la vida del Datacryptor 2000. También acorta el tiempo necesario para poner en práctica nuevos algoritmos de codificación, al tiempo que permite mantener el buen desempeño basado en los equipos.



A fin de satisfacer los exigentes requisitos de los clientes mundiales, el dispositivo codificador de Datacryptor 2000 (el Subsistema SafeGuard de Seguridad) cuenta con la certificación FIPS 140-1, Nivel 4. La unidad en general tiene clasificación de Nivel 3. El nivel de seguridad física y lógica del Datacryptor 2000 es tan alto, que los gobiernos confían plenamente en él. Una versión del Datacryptor 2000 utilizada por el gobierno inglés y basada en el algoritmo Embattle está aprobada por CAPS.

#### Diseñado para el máximo desempeño

Como el Datacryptor 2000 se basa en un procesador especial para acelerar la codificación, son mínimas la demora y la amplitud de banda extra necesarias para la codificación. El Datacryptor 2000 tiene un excelente desempeño con las aplicaciones más exigentes como las de voz a través de Frame Relay. Los usuarios pueden adaptar la selección de dispositivos a sus requisitos de desempeño, y sólo pagan por el volumen de transmisión que requieran. En toda la línea del producto se ofrecen modelos estándar, de alta velocidad y de muy alta velocidad. Los codificadores de enlaces de Datacryptor 2000 protegen la información que se transmite a través de redes de comunicación de un punto a otro, con índices de transferencia de 512 kbps, 2.048 Mbps y 8 Mbps respectivamente. Asimismo, los productos de Frame Relay de Datacryptor 2000 permiten su utilización en las redes de Frame Relay, con índices de transferencia de 256 kbps, 2.048 Mbps y 8 Mbps. Los codificadores de Datacryptor 2000 X.25 establecen una red privada virtual dentro de la red pública X.25 y brindan velocidades de transferencia de 64 kbps, 128 kbps y 1 Mbps. El

producto Datacryptor 2000 IP realiza la codificación a nivel de paquetes de IP a través de conexiones de Ethernet 10BaseT a velocidades de hasta 5 Mbps.

#### Garantizamos que está listo para AES

La familia Datacryptor 2000 se ha diseñado para proteger la inversión del cliente al permitir las actualizaciones de software a nuevos esquemas o protocolos de codificación. Al estar basados en la tecnología de Conjunto de Puertas Programable por Campos (FPGA), la cual permite que los soportes lógicos firmados de forma digital se carguen electrónicamente desde sitios locales o remotos, los productos Datacryptor 2000 constituyen los únicos dispositivos de seguridad de redes disponibles en la actualidad que permiten que los clientes migren al algoritmo Rijndael (AES) sin el costoso proceso de eliminar, actualizar y reinstalar equipos. Esta modalidad de migración basada en el software brinda ahorros significativos y una gran conveniencia.

#### Agilidad de protocolos

El Datacryptor 2000 están disponibles en modelos de Protocolo Único y también de Protocolo Variable (VP). Los modelos de VP aceptan toda nuestra gama de protocolos de comunicaciones. Por ejemplo, los clientes que estén utilizando Frame Relay y tengan planes de migrar a IP, pueden comprar hoy mismo un modelo de Datacryptor 2000 VP e instalar nuestro protocolo de Frame Relay. Cuando llegue el momento de pasar a IP, instale el software de protocolo de IP, conecte sus cables de 10BaseT, y conéctese a la Ethernet! Esta posibilidad especial garantiza que su inversión esté protegida frente a la ineludible realidad de la migración de redes.

### Flexibilidad administrativa y de apoyo

THALES les da a los clientes la flexibilidad de utilizar herramientas SNMP de administración empresarial de primer orden en la industria, como HP OpenView NNM o SNMP-c, para monitorear de forma local o remota los productos Datacryptor 2000. Cada cliente tiene la libertad de seleccionar la herramienta administrativa que mejor se avenga a sus necesidades. Por ejemplo, si un cliente ya tiene un sistema SNMP, no es necesario que le compre a THALES los medios administrativos. Sin costo adicional, el Administrador de Elementos Datacryptor 2000 de THALES se integrará perfectamente con los sistemas SNMP existentes. El Administrador de Elementos es una interfaz GUI fácil de usar y con menús desplegables, compatible con Windows 95/98 y NT, y brinda funciones seguras de configuración y definición para los productos Datacryptor 2000. Por otra parte, si la red del cliente está segmentada o aún no tiene un administrador de SNMP, entonces THALES ofrece e integra el sistema administrativo SNMP-c con el Administrador de Elementos de Datacryptor 2000, de modo que la solución sea eficaz en función de los costos. Si un cliente está instalando una cantidad pequeña de codificadores, tal vez no sea necesario un sistema administrativo SNMP. En este caso, el cliente puede simplemente utilizar el Administrador de Elementos de Datacryptor 2000 para la gestión de los codificadores. La elección depende del cliente pero, con la familia Datacryptor 2000, no hay necesidad de duplicar los costosos sistemas de administración empresarial.

La capacidad de monitorear y diagnosticar los problemas rápidamente es de la mayor importancia, especialmente cuando se trata de

seguridad de la información. La familia de productos Datacryptor brinda diversas modalidades de diagnóstico para que la operación esté libre de errores. Se pueden hacer pruebas en el lugar o a distancia. Los archivos de registro efectúan el seguimiento de las operaciones y los eventos y pueden imprimirse mediante el Administrador de Elementos de Datacryptor 2000 o mediante un administrador SNMP. Los mecanismos de clasificación permiten que los datos queden organizados en categorías de fecha y hora, entrada del registro o una combinación de campos como éstos u otros disponibles.

Además de un conjunto completo de diagnósticos, THALES ofrece planes de servicio y apoyo a la medida de los requisitos de los clientes. THALES brinda muchas opciones de servicio, incluida la asistencia técnica en el lugar, 24 horas al día, los siete días de la semana o en horario normal de oficina, y asistencia técnica por teléfono. El personal de servicio de THALES está integrado por expertos en productos de seguridad de redes que se han comprometido a ayudar a los negocios que dependen de los datos a proteger su propiedad más valiosa: la información.

### Diseño simplificado y a prueba de manipulación

Cada uno de los productos Datacryptor 2000 se ha diseñado para que esté a prueba de manipulación. Desde adentro hasta afuera, la unidad se construye de modo que detecte y evite las intrusiones dañinas. Cada unidad viene sellada en un gabinete resistente a la manipulación. Para detectar cualquier penetración en el gabinete, el módulo criptográfico y los sensores de manipulación que perciben movimientos, cambios de



# La familia Datacryptor™ 2000

temperatura o voltaje y ataques químicos, vienen protegidos en un módulo a prueba de manipulación. El módulo está rodeado por una delicada red conductora cubierta de resina epóxida de color opaco. Cualquier ataque al módulo causa una ruptura a la delicada red, activando una alarma de peligro. A fin de no correr riesgos, se borran todas las claves, con lo cual la unidad queda inutilizable hasta que se vuelva a comisionar. Los sensores de movimiento detectan cualquier intento no autorizado de cambiar las unidades de lugar y también hacen que se activen las alarmas de peligro. Estos sensores se pueden desactivar si no es necesaria la detección del movimiento. THALES ha tomado todo tipo de precauciones para garantizar que no corra peligro la integridad física de sus productos.

## Administración segura de las claves

La familia Datacryptor 2000 utiliza sofisticadas técnicas de administración segura de las claves a fin de prevenir la infiltración y los ataques. Todas las funciones de administración de claves son acordes con las normas industriales especificadas para los gobiernos, las instituciones financieras y las organizaciones que tienen estrictos requisitos de seguridad de la información. En los casos de productos como Datacryptor 2000 Link, Frame Relay, X.25 e IP, la administración de las claves se basa en el protocolo Diffie-Hellman de administración de claves y el Algoritmo de Firmas DSA, con certificados X.509 firmados para administrar los intercambios de claves. Éstas se generan mediante el uso de un equipo generador de números aleatorios. Para brindar el máximo de seguridad y flexibilidad, las claves se pueden cambiar automáticamente a intervalos definidos por el usuario.

La autoridad certificadora (Datacryptor 2000 CA) se utiliza para generar certificados X.509 para las unidades que integran la red. Esta aplicación permite que el usuario transfiera la autoridad de raíz, añada o borre autoridades de certificación, certifique un conjunto de claves de unidad, cargue parámetros Diffie-Hellman y borre conjuntos de claves. THALES recomienda que cada usuario tome el control de su propia seguridad. Sin embargo, en el caso de redes que no requieran el establecimiento de una comunidad cerrada de unidades, el Datacryptor 2000 se puede utilizar tal como se recibe. El Datacryptor 2000 se puede administrar a distancia. Tiene puertos de control en serie y de Ethernet que aceptan protocolos PPP e IP, respectivamente, lo cual brinda la posibilidad de monitorear el estado de la unidad mediante un administrador empresarial basado en SNMP, como el OpenView NNM de Hewlett-Packard, o de activar el Administrador de Elementos de Datacryptor 2000.

## Diagnóstico avanzado

Existen diversas formas de diagnóstico para mantener las operaciones sin problemas. En el Datacryptor 2000 se mantienen los archivos de registro, los cuales se pueden visualizar o imprimir con el Administrador de Elementos o un administrador de SNMP. Los datos pueden clasificarse por fecha y hora o por tipo de entrada en el registro, o por una combinación de estos campos u otros disponibles.

## Garantizamos el futuro

THALES y la familia Datacryptor 2000 brindan soluciones versátiles de codificación diseñadas para el futuro. THALES ofrece la única solución de criptografía que permite que los usuarios migren sin problemas al nuevo algoritmo





Rijndael (AES), sin perder su inversión inicial en equipos. Ningún negocio que transmita información sensible a través de redes puede darse el lujo de no pensar en el futuro. Con la familia Datacryptor 2000, el futuro ya está aquí. No cualquier compañía le puede brindar las soluciones de codificación de redes que usted necesita. THALES ofrece soluciones de seguridad de datos desde 1980. O sea, desde hace más tiempo que cualquier otro competidor. A los gobiernos, a más del 70 por ciento de los bancos del mundo, a la industria... a los clientes más importantes en la esfera de comunicación de datos valiosos. Tenemos más de 60,000 dispositivos de codificación de redes en operación continua cada día, y ni un solo cliente ha sufrido jamás una pérdida en una transacción protegida por THALES, en redes grandes y pequeñas, en todos los continentes y prácticamente en todos los países del mundo, en transferencias de dinero, transmisión de secretos estatales o protección de datos personales. La familia Datacryptor 64 de dispositivos de codificación de THALES ha protegido algunas de las más grandes redes seguras del mundo durante más de una década. Esa experiencia y las lecciones que hemos

aprendido en todas estas importantes aplicaciones nos han servido para producir una nueva generación de dispositivos de codificación, el Datacryptor 2000. Se trata de medios de seguridad que satisfacen las necesidades más exigentes, y son fáciles de instalar, fáciles de administrar, compactos y eficaces en función de los costos. Además, se pueden actualizar de forma electrónica para mantenerlos al día con los cambios en algoritmos, normas y protocolos.

#### Datacryptor 2000 Link, X.25, Frame Relay e IP

- Comunicación segura de los datos mediante Triple DES
- Listo para el algoritmo Rijndael-AES en la misma plataforma de hardware
- Algoritmos gubernamentales o adaptados al cliente
- Intercambio de claves firmadas Diffie-Hellman
- Firmas digitales (DSA, SHA-1)
- Certificados digitales (X.509)
- Compatible con administradores SNMP
- Administración segura a distancia
- Certificación FIPS 140-1 de Nivel 4

## THALES

### Europa, Oriente Medio, África

THALES e-SECURITY LTD.  
Meadow View House  
Long Crendon, Aylesbury  
Buckinghamshire, HP18 9EQ,  
Reino Unido  
Tel: +44 (0)1844 201800  
Fax: +44 (0)1844 208550  
Correo electrónico:  
emea.sales@thales-eseurity.com

### Américas

THALES e-SECURITY, INC.  
Sawgrass Technology Park  
1601 North Harrison Parkway  
Building A, Suite 100  
Sunrise, FL 33323, USA  
Tel: +1 888 744 4976  
ó: +1 954 846 4700  
Fax: +1 954 846 3935  
Correo electrónico:  
americas.sales@thales-eseurity.com

### Asia y Pacífico

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  
Correo electrónico:  
asia.sales@thales-eseurity.com

[www.thales-eseurity.com](http://www.thales-eseurity.com)

