

Racal Security and Payments



Datacryptor™ 2000

Standard and High-Speed Link models

Secure data communications using triple DES

Signed Diffie-Hellman key exchange

Digital signatures and certificates

SNMP and secure remote management

Flexible cryptography

Strong physical security

RACAL



Datacryptor™ 2000

Has there ever been a time when information privacy was of greater concern?

We are becoming a plugged-in, wired society. Our livelihood depends on the information we obtain and the information we provide. The global connectivity that is part of our lives has made our mission-critical, private information more vulnerable than ever before! Vulnerable to hackers and disgruntled employees, vulnerable to criminals, vulnerable to industrial espionage.

And now to improve access and reduce costs, the migration to public networks is accelerating, increasing the potential for compromise as your data travels over shared facilities. But these risks can be controlled. Technology has produced solutions to restore and improve the security that valuable or sensitive information requires.

It matters from which company you select your network encryption solutions...

Racal 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, not a single customer has ever suffered a loss on a Racal protected transaction. Large and small networks, on every continent and in virtually every country of the world. Moving money, transmitting State secrets, protecting personal data. In fact, Racal's Datacryptor 64 family of encryption devices has protected some of the world's largest secure networks for more than a decade.

We've 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.

The Benefits of Flexible Cryptography

The Datacryptor 2000 has been designed to support a wide variety of algorithms using the same hardware. The unit can be loaded with the standard Triple-DES algorithm, or a variety of national or custom encryption algorithms.

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.

Key Management

Every Datacryptor 2000 is loaded with the public key of its root Certificate Authority before shipment. During commissioning, the Datacryptor 2000 generates its own set of private and public keys. The Datacryptor 2000 submits its public key to the root Certificate Authority (CA). The signed public key is then placed in an X.509 certificate. Each Datacryptor 2000 stores its own X.509 certificate and presents it to other units when initiating a key exchange. The Datacryptor 2000 may store public keys of other CA's as well, so

that it can accept and validate certificates presented to it by Datacryptor 2000's from other user communities.

The signed certificates are exchanged during the initial connection to authenticate the units. This procedure prevents unauthorised devices from spoofing a Datacryptor 2000 and gaining access to a private network.

The Datacryptor 2000 uses the signed Diffie-Hellman key agreement algorithm to manage key exchanges. The Datacryptor 2000 employs a hardware random number generator in all cryptographic operations requiring random values, such as key generation. Each Datacryptor 2000 derives the Key Encrypting Key (KEK), Data Encryption Key (DEK) and Initialisation Vector (IV) from the exchange process. Within the confines of the tamper-protected storage, the Datacryptor 2000 stores DEKs, KEKs, Diffie-Hellman parameters, the public keys and identities of approved CA's, and its own X.509 certificate to speed-up future key exchanges with the same remote party.

To improve security and maximise the protection the Datacryptor 2000 provides, each logical connection is protected by a unique set of keys. In fact different keys are used in each direction of transmission on the same connection! Totally automated key changes at user definable times and intervals take the work out of running a secure network.

Strong Physical Security

The Datacryptor 2000 is contained in a sealed tamper-evident case. Inside the case, surrounding the entire cryptographic module is a thin tamper-resistant film immersed in opaque epoxy to detect penetration. Tamper-sensors for motion, temperature, voltage and chemical attacks are also contained within the tamper envelope. Batteries



which support the electronics inside the tamper envelope are external to the envelope (but inside the unit) to allow life cycle maintenance by our repair centres.

If the unit's envelope is compromised a "critical alarm state" is triggered which results in all algorithms (except DSA and SHA-1) and all keys being erased. Recovery from tampering requires repair at our product support centres to ensure all security features are working correctly.

Transport sensors can be turned off. When turned on, the sensors will automatically trigger an alarm if the unit is moved.

The Datacryptor 2000 is compliant with FIPS 140-1 level 3 and ITSEC level E3. The Datacryptor 2000 is year 2000 compliant.

Management Suite

The Datacryptor 2000 can be configured and managed using a combination of enterprise SNMP managers, the Datacryptor 2000 Element Manager and the Datacryptor 2000 Certificate Authority. The Datacryptor 2000 management applications are compatible with Windows 95, 98 and NT.

The Datacryptor 2000 Element Manager is used for local or remote device configuration. The Element Manager provides typical network and security management functions.

The Datacryptor 2000 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. Racal 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, such as Hewlett-Packard OpenView NNM, or to launch the Datacryptor 2000 Element Manager. In addition to out-of-band management through the rear panel management ports, the Datacryptor 2000 supports in-band management between communicating Datacryptor 2000's that share a logical and physical connection. This adds flexibility to the options for configuring the network. In-band management sends all management messages on the primary data path between units briefly interrupting the user's communications. For in-band management, the Datacryptor 2000 can operate as either a local or remote site unit. And, it offers a choice of management communications interfaces for operation over dial-up or high-speed digital networks.

Streamlined Design

The small footprint of the Datacryptor 2000 allows many units to be stacked into a cabinet or rack. The units can be stacked horizontally or vertically. In a vertical orientation 16 units can fit in a 19" rack saving valuable space. LEDs on the front panel easily communicate the status of the unit to the user. All cable and power connections are on the back.

Data ports for low-speed interfaces employ high-density connectors and smart-cables. The Datacryptor 2000 will automatically detect the attached cable type and configure for it.

Both low-speed and high-speed ports are included on high-speed units.

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.

Secure Communications

The Datacryptor 2000 link model is designed to protect data transmitted over leased lines. The Datacryptor 2000 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 or up to 2.048 Mbps. Data is encrypted using Triple DES or an optional algorithm.

Each logical link 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 link encryption 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.



Datacryptor™ 2000

Technical Specifications

Maximum Data Transfer Rate	DC2K-S: up to 512 Kbps, full duplex, synchronous DC2K-HS: up to 2.048 Mbps (T1: 1.544 Mbps, E1: 2.048 Mbps)
Operating Modes	Standby (no data traffic) Bypass (unencrypted) Secure (Unframed: Encrypted data; Framed: Encrypted data composed of 24 [T1] or 31[E1] independently encrypted DS0's)
Encryption Algorithms	Triple DES as standard algorithm (ANSI X9.52, 168-bit key) Other commercial or government approved algorithms available Custom algorithms can be implemented All algorithms are soft-loadable as digitally signed firmware
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 KEK lifetimes are configurable from 1 minute to 99 days DEK lifetimes are configurable from 1 minute to 7 days KEKs and DEKs are exchanged automatically Certified hardware random number generation
Device Management	Out-of-band management using PPP protocol (9-pin D serial port) or IP protocol (10 base T RJ45 Ethernet port); in-band management over data path
Physical Interfaces	RS-232 (V.24), 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 2.048 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): RJ-45/RJ-48C connectors on both ends Smart cables (length 1m): 26-way, high-density D connectors terminating in RS-232, V.35 or V.11 connectors: - RS-232 (25-pin male and female D-type) - V.35 (34-pin male and female MRAC connector) - V.11 (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 Optional protection against compromise by theft
Date Integrity	Year 2000 compliant
Security Certification	ITSEC E3 and FIPS-140 Level 3
Power	+/-12V and +5V, less than 7W (external power supply)
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") Width 22.0 cm (8.7") Depth 23.0 cm (9.0") Weight 1.8 Kg (4.0 lbs.)

Specifications subject to change without notice

Racal Security and Payments



EUROPE, MIDDLE EAST, AFRICA

Racal Airtech Ltd.
Meadow View House
Long Crendon, Aylesbury
Buckinghamshire, HP18 9EQ, UK
Tel: +44 1844 201800
Fax: +44 1844 208550
Email: security@racalitsec.com
www.racalitsec.com

ASIA PACIFIC

Racal Security and Payments
10th Floor, Sun House
181 Des Voeux Road Central
Hong Kong
Tel: +852 2815 8633
Fax: +852 2815 8141
Email: itsecurity@racal.com.hk
www.racalitsec.com

AMERICAS

Racal Security and Payments
1601 North Harrison Parkway, Building A
Suite 100, Sunrise, FL 33323-2899, USA
Tel: +1 954 846 4700
Fax: +1 954 846 3935
Sales: +1 888 744 4976
Email: americas.sales@racal.itsec.com
www.racalitsec.com