IP ENCRYPTOR
Omnisec 423

The Omnisec 423 is a member of the family of IP Encryptors, which together constitute the **OmniCrypt™ IP-based VPN** – a reliable Virtual Private Network solution offering the highest level of security. It exemplifies Omnisec as the world's leading supplier of maximum-security, high-quality (ISO 9001 approved) communication solutions.

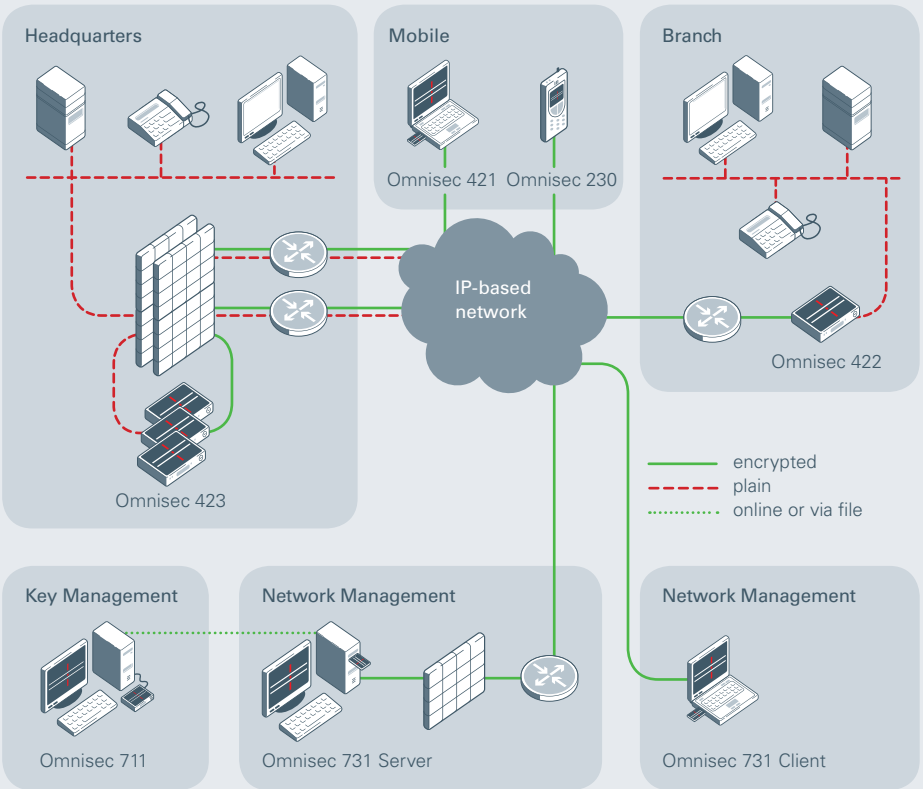
Communication security is based on the security architecture **OmniCrypt™**: unique, short-lived Session Keys are generated from secret, long-lived Master Keys stored in removable **Security Modules**. Every link owns its exclusive, bilateral Session Keys, which are renewed automatically after a preselected time interval or amount of encrypted traffic.

Customers are invited to assess and verify for themselves the implemented encryption procedures and algorithms.

Omnisec's IP-based VPN establishes extremely secure site-to-site communications for the exchange of e-mails, files, video or voice data over a corporate IP-based network or the Internet. Integrated **Route-based VPN** maximizes throughput by supporting redundant VPN communication paths with dynamic fallback and load-distribution mechanisms. Omnisec's high-quality devices integrate easily into existing networks which may include third-party products (e.g. firewalls, content inspection, intrusion prevention tools), and provide appropriate scalability to ensure the desired performance.

The IP Encryptor, Omnisec 423, is a 19" rack-mountable IP Encryptor with redundant power supplies. Its acceleration hardware makes it ideal for deployment in major sites, such as a headquarters. The NMC-Connect feature, and redundant storage of essential configuration data, facilitate system rollout and device replacement even by untrained personnel.

User-friendly management tools. The Key Management Center, Omnisec 711, defines the network, generates secret keys and programs the SMs; the Network Management Center (NMC), Omnisec 731, allows all devices to be configured and maintained very efficiently from a central location.



IP Encryptor
Omnisec 423, Release 4.5

Security Features

Security architecture OmniCrypt™
- Multi-barrier software and hardware architecture with supervision mechanisms
- Omnisec-proprietary algorithms

Encryption/Authentication
- Packet encryption: Omnisec block cipher
- Packet authentication: Omnisec MAC

Master Keys
- Derived from white-noise source
- Length: 256 bits; diversity: 10^{77}

Session Keys
- Diversity: 10^{77}
- Used once and only once
- Automatic renewal

Key Management
- Omnisec-proprietary
- Address and key storage for up to 3000 stations
- Secure, end-to-end online key distribution
- Blacklisting of stolen or lost SMs

Mechanical Lock
- Prevents unauthorized opening of the unit
- Locks in the Security Module

Emergency Erase Function

Networking Features

- Internet Protocol (IPv4)
- Routing functionality (static and dynamic, RIPv2 and OSPFv2)
- Dynamic Route-based VPN
- Redundant operation of communication paths, traffic load distribution and permanent tunnel monitoring
- Proprietary key management protocol
- IPsec Tunnel Mode
- NAT Traversal
- QoS support: TOS/DSCP forwarding and tagging

Network Management
- Enhanced test functions
- Event agent
- SNMPv1 support (standard MIB-II and proprietary MIB)

Device Management
- Configuration, monitoring and logging
- Firmware update

Technical Data

Performance
- Throughput up to 85 Mbit/s (depending on IP packet size and chosen encryption and authentication method)
- Up to 500 simultaneous partners in the secure VPN; optionally 3000

Controls
- 2 slots for Security Modules (SMs)
- 3 LEDs for system and interface status
- 1 LCD for management information
- 8 pushbuttons for menu navigation and to trigger Built-In Test Equioment (BITE), emergency erasure

Interfaces
- 2 Ethernet RJ45 10Base-T/100Base-Tx auto-sensing ports for trusted and untrusted areas
- Management ports (USB; RS232 RJ45)

Power
- Redundant power supplies: 100 ... 120/ 200 ... 240 VAC, 50 ... 60 Hz and/or 15 VDC
- Power consumption: ~40 VA
- Lithium battery for data retention

Safety Conformity
- EN 60950-1:2006
- RoHS compliant

Electromagnetic Compatibility (EMC)
- Radiation: EN 55022 class B
- Immunity: EN 55024

Environmental Test Specifications
- Temperature range (IEC 60068-2-1 Ad, IEC 60068-2-2 Bd): storage: -25 ... +70 °C; operation: 0 ... 45 °C
- Humidity (IEC 60068-2-78 Cab): 40 °C, 93% RH, non-condensing, 10 days; 8 days in operation
- Random vibration (MIL-STD-810E, method 514.4-7): 10 … 40 Hz, 0.015 g^2/Hz, 40 … 500 Hz, 0.00015 g^2/Hz, 3 axes each 1 h, equivalent to 1000 miles common carrier transportation (in transport package)
- Shock (IEC 60068-2-27 Ea): 100 g, 6 ms (all surfaces)
- Fall (IEC 721-3-2 2M2): 1.2 m (on concrete in transport package, 5 falls)
- Drop (IEC 60068-2-31 Ec): 0.1 m on concrete (all corners/edges)

Reliability
- MTBF (MIL-STD-217F, Notice 2, IC's: CF 0.1 [experience] according to IEC 62380) at t_{amb}= 25 °C: 46 000 h

Dimensions
- w × h × d: 482 x 43 x 410 mm
- Weight: 3.3 kg (incl. power supply)

Management Tools

- Key Management Center (KMC), Omnisec 711, and Security Module Programmer, Omnisec 704
- Built-in Key Equipment (BIKE) for up to 10 stations
- Network Management Center (NMC) Omnisec 731

We strive to continuously improve our offerings and therefore reserve the right to change specifications without notice.

Omnisec AG, Switzerland
info@omnisec.ch, www.omnisec.ch

omnisec