



Quantum-secure encryption

SecuriVPN®

Advenica's quantum-secure IP encryption modules, SecuriVPN, have been specifically developed for tactical and strategic defence use, and have been proven in defence engagements to provide versatile encrypted communications since 2006.

Designed to satisfy the most demanding defence requirements, and substantiated in combat zone theatres ranging between desert and arctic conditions, SecuriVPN is successfully deployed for Army, Navy and Air Force communications in many countries, certified to protect information up to TOP SECRET.

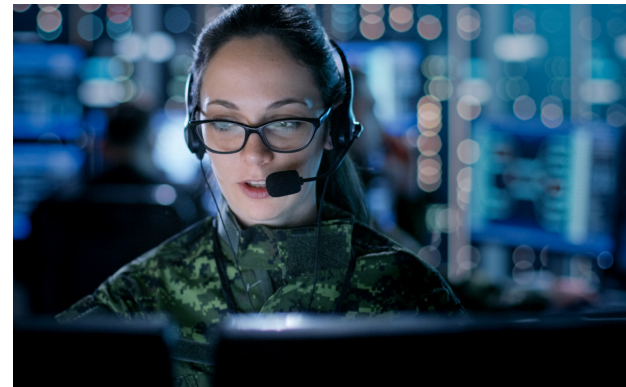
Simple future-proof key management, versatile high-availability features and ability to communicate over low and high quality transmission layers provides ease of use as well as resilient communications.

Tactical features include

- Silent mode reception to avoid detection
- Low band and jitter resilience
- Versatile high-availability including failover
- Power outage resilience
- Easy to declassify when not in operation
- Low power consumption to enable mobile mode

Tailored for long-term communication privacy

Long-term communication privacy is ensured by unique technology developed by Advenica. All IP communication, data transfer and key handling is protected by quantum-secure algorithms and protocols, exclusive for the SecuriVPN product range. SecuriVPN renders vital network security functionalities such as authentication of information origin, integrity control, and anti-replay mechanism. It also enables network architecture masking.



Benefits

- Quantum-secure technology
- Simple key management based on symmetrical encryption
- Red/black separation in hardware
- EU, national, Serpent256, AES256
- Guaranteed high availability with multiple redundancy options
- Receive only mode
- Applicable to land, sea and air operations
- Support dynamic routing
- Emergency erase
- Supports various networks such as ad-hoc and fully-meshed
- Full traceability is provided through both local and central logging

Integrated insider threat protection

To eliminate the risk of unauthorised disclosure of classified information by rogue administrative staff, Advenica has developed technology to separate classified information and transport networks from device administration, called Three Domain Separation. The patented Three Domain Separation technology introduces a third domain,

administration domain, in addition to the traditional Red/Black domain separation. Thus, classified information from the protected (RED) domain cannot be accessed from the administration domain. The Three Domain Separation technology effectively eliminates the insider threat in government, armed forces and intelligence organisations.

VPN basics

- IPsec enhanced
- 512 unicast + 512 multicast tunnels
- NAT traversal
- 100 Mbit/s linespeed

Modes of Operations

- Two-way tunnel
- One-way tunnel (diode functionality)
- Network modes: fixed, mobile and deployable

Ports

- 100Base-FX (LC connectors) for data, Optical interface for local configuration and log output
- Electrical interface RJ45 100Base-TX for data, 9-pin D-sub RS232 for local configuration and log output

Encryption Algorithms in hardware

- AES 256, Serpent 256
- Custom/national algorithms
- EU version: SECRET UE/EU SECRET
- Swedish version: HEMLIG/TOP SECRET

Device authentication

- X.509 certificates and CRLs
- Symmetric keys

Device management

- Front panel user interface
- Local configuration port
- Smart cards
- Secure in-band remote management
- Secure local or remote firmware upgrade

Key Management

- Session keys from Key Server System
- Authenticated Session key exchange
- Enhanced IKE using RSA-PSS signatures
- Keys distribution: smart card and online

Monitoring & Log handling

- Local interface for log output
- Remote management with event secure syslog
- SNMP remote monitoring and control

Security Features

- Hardware based random number generator
- Red/black separation in hardware
- Emergency erasure of keys
- Tamper evident chassis
- Active and passive tamper resistance
- POST (Power On Self Test)
- Replay protection
- Auto detection of local red/black circuit

High Availability and QoS

- Up to 10 units in parallel
- QoS, DiffServ
- Key backup
- Failover installation

Regulatory Compliance

- Common Criteria EAL 4+
- CE
- Versions available with Tempest EU/SWE MIL-STD approval up to Top Secret

Power source (dual)

- 85-264 VAC (standard)
- 10-66 VDC (optional)
- Dual power supply optional

Operating Temperature

- -5 °C – +40 °C, 5 – 95% rel. H

Physical Dimensions

- Measures:
 - 442 x 44 x 272 mm (19" rack device)
 - 257 x 44 x 272 mm (portable device)
- Weight: 4-5,8 kg

Models

- ED100 19" rack device (height 1U)
- Front Connector Module (option)
- ED100P portable device

MTBF

- >75 000 h