The HSNE9004 provides for secure communication of Virtual Private Networks over public network infrastructures using IPsec. The device is aimed at travelling members of defence and government organisations who wish to establish remote access connections to headquarters via public and / or satellite networks. It is designed to be suitable for communicating up to Top Secret classification level.

The HSNE9004 is a network encryption device with various levels of software that:

- encrypts network traffic flowing over public or shared networks
- enables commercial or proprietary (client supplied) cryptographic algorithms
- provides active hardware tamper protection of cipher and key material
- provides cryptographically authenticated secure administrative access
- offers a user friendly system, simple to use and visibly secure
- has a Secure Policy Management and Token Management feature
- provides VPN fire-walling.

The HSNE9004 is equipped with two network interfaces (red and black) to provide for separate connections to the public and private segments of the network. The device is securely managed through a dedicated management interface.

### HSNE9004 SPECIFICATIONS

<table>
<thead>
<tr>
<th>Transmission rates</th>
<th>Throughput with AES algorithm (maximum size packets) ≥ 4Mbps</th>
</tr>
</thead>
<tbody>
<tr>
<td>Transmission standards</td>
<td>Fast Ethernet, USB</td>
</tr>
</tbody>
</table>

### COMMUNICATION INTERFACES

<table>
<thead>
<tr>
<th>Interface types</th>
<th>Private Interface with support for the following media types:</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>• 100BASE-TX via RJ-45 connectors</td>
</tr>
<tr>
<td></td>
<td>• USB 2.0 via Type-B connectors</td>
</tr>
<tr>
<td></td>
<td>Public Interface with support for the following media types:</td>
</tr>
<tr>
<td></td>
<td>• 100/1000 BASE-TX via RJ-45 connectors</td>
</tr>
<tr>
<td></td>
<td>• USB 2.0 via Type-B connectors</td>
</tr>
<tr>
<td></td>
<td>One USB Type-A port for USB Token</td>
</tr>
<tr>
<td></td>
<td>One USB Type-B port for local management purposes</td>
</tr>
</tbody>
</table>

### OPERATOR INTERFACES

<table>
<thead>
<tr>
<th>Keypad</th>
<th>Keypad with 5 buttons (non scanned)</th>
</tr>
</thead>
<tbody>
<tr>
<td>LCD</td>
<td>Graphical LCD screen (non scanned)</td>
</tr>
<tr>
<td>LEDs</td>
<td>Three Tri-Colour LEDs for Status and Fault Indication</td>
</tr>
<tr>
<td></td>
<td>Green Power LED Indicator</td>
</tr>
<tr>
<td></td>
<td>Red Tamper LED Indicator</td>
</tr>
</tbody>
</table>

### OPERATIONAL SPECIFICATIONS

- Encrypted tunnels using IPsec Version 2
- Multicast traffic
- Able to operate in both bump-in-the-wire (bridging) and gateway (routing) modes
- VPN firewalling capabilities
- Bi-directional IPsec tunnels
- NAT traversal
- SCPS for accelerated data throughput on satellite networks (available on request)
HSNE9004
High Security Mobile Network Encryption

CRYPTOGRAPHIC ALGORITHMS

AES with 128, 192, 256 bit key length
One custom symmetric cipher similar AES
RSA with 4096 bit modulus
Diffie-Hellman with 4096 / 8192 bit MODP group
HMAC using SHA-256 hashing algorithm

AUTHENTICATION

PKI with private key stored in tamper protected memory
PKI with PIN protected private key for administrators
Customer cipher stored in protected memory
Tamper respondent shield protects Critical Security Parameters

MECHANICAL / ELECTRICAL / ENVIRONMENTAL

Storage temperature -40°C to 70°C
Operating temperature -5°C to 55°C
Size 135 x 32 x 180 mm
Power Supply Via USB
Or external supply 6 to 18 VDC
Power consumption <3 watt
Backup Battery Rechargeable backup battery for active tamper monitoring during power down
Ingress Protection IP-54

CERTIFICATIONS AND CLASSIFICATIONS

EMC FIPS 140-2 Level 4 EMC compliance
Security Active tamper protection is provided based on elements of FIPS140-2 level 4