

# Radio IP MTG™

## FIPS 140-2 Validated Encryption

Radio IP MTG™ is a FIPS 140-2 compliant Mobile VPN software. The software utilizes embedded Microsoft cryptographic modules which have been validated by the National Institute of Standards and Technology of the United States of America and the Communications Security Establishment of the Government of Canada for the Microsoft Corporation. You will find the FIPS 140-2 validation certificates, issued per type of Operating System, in the table below.

OS version	Certificate No.
Windows XP SP3	<a href="#">989</a>
Windows Vista SP1	<a href="#">1002</a>
Windows Server 2003 SP2	<a href="#">1012</a>
Windows Mobile 5.0	<a href="#">560</a>
Windows Mobile 6.0	<a href="#">560</a>
Windows Mobile 6.1	<a href="#">560</a>

You may click directly on the certificate number to access the NIST certificate. Further information regarding these certificates can also be found on the following web page, by entering the certificate number:

<http://csrc.nist.gov/groups/STM/cmvp/validation.html#01>

Data transmitted between the Radio IP MTG server and the Radio IP MTG clients are encrypted at all times with either AES (128-bit, 192-bit and 256-bit key sizes) or Triple DES (112-bit or 168-bit key sizes) encryption methodologies, using FIPS 140-2 validated algorithms.

Symmetric Secret Keys are encrypted with RSA asymmetrical encryption methodology which has been FIPS 140-2 validated under the same certificate number.

### Encryption Export Regulations:

Radio IP Software alternatively provides DES (56-bit key size) encryption modules for compatibility reasons and for unregulated usage outside of the USA and Canada. To comply with U.S. and Canadian *encryption export* laws, end-customers are required to have an export license in order to utilize AES or Triple DES encryption methodologies.