For Further Information Contact:
Graeme Durant
Helion Technology Limited
+44 (1223) 500 924
graeme@heliontech.com

FOR IMMEDIATE RELEASE

HELION CUTS THE RISK FOR EARLY ADOPTERS OF 802.11i SECURITY

7th August 2002, Cambridge UK

Data security IP provider Helion Technology Limited announces today the immediate availability of its 802.11 WLAN AES Security Acceleration core. This unique ASIC core has been specifically designed to enable forward-thinking silicon vendors to add the very latest security extensions into their chipsets now, yet is re-configurable to keep pace with the future requirements of the evolving standard, minimising both risk and time-to-market.

Security in wireless networks is an increasing concern, and the existing Wired Equivalent Privacy (WEP) algorithm used in 802.11 Wireless LAN (WLAN) systems had weaknesses exposed only after product deployment. The 802.11 Task Group I (TGi) has been debating new schemes using the Advanced Encryption Standard (AES) for over a year, but due to contentious issues ranging from security strength to licensing arrangements, have been unable to reach a unanimous conclusion. Just recently, the group voted to make one scheme mandatory and the other optional, although this could change before the draft standard is completely ratified. This current uncertainty has made it very risky for chipset vendors to provide hardware support for this enhanced security prior to final ratification, despite widespread customer demand.

"We believe our design provides implementers with a low-risk method of incorporating the latest AES-based security in their silicon", says Graeme Durant, CEO at Helion, "The flexibility of our soft-loadable solution allows any of the current proposed schemes to be addressed, and permits easy field upgrades should the standard evolve further, or security weaknesses be exposed".

The Helion Accelerator core has been built around highly efficient AES encryption hardware engines, controlled by a programmable datapath processor, into which firmware is loaded to define the exact scheme and protocol required. It supports soft-loadable implementations of many different AES schemes for authenticated encryption of packet data, including all those under discussion in the TGi. Integration of the core into typical MAC hardware is extremely straightforward. A Direct Memory Access (DMA) controller minimises the per-packet support needed from the host processor, and multiple keys can be loaded and cached ready for

immediate use. For Access Point (AP) products which must communicate with different stations having various security options, algorithms can be chosen dynamically.

"We have not compromised to attain this flexibility" says Durant, "The high performance of our mature and product-proven AES cores is now complemented by additional features which make system integration with typical 802.11 MAC hardware very easy. There is a healthy throughput margin even for the highest 802.11a data rates of 54Mbps".

The Accelerator core, which has already been licensed by one early adopter of the 802.11i draft standard, is supplied with an optional fully-functional interface wrapper providing ARM APB and AHB compatible bus interfaces, for direct connection into a typical MAC sub-system. The ASIC code has been designed with low gate-count and minimal local RAM requirements very much in mind, making it ideal for mobile and battery applications. A behavioural model and an FPGA version are also available for evaluation and rapid proto-typing.

More detailed information on the AES Accelerator, plus other leading-edge security solutions, is available from the Helion website at **www.heliontech.com**

---------------------------- ENDS ----------------------------

Helion – Background

Cambridge based Helion Technology was formed in 1992 to offer high quality ASIC and FPGA design services to a broad range of end clients. Having gained significant expertise in the data security industry, Helion has for a number of years been offering its proven data encryption solutions to a wider audience beyond its own design services customers, with a comprehensive range of high performance IP Cores for ASIC and FPGA applications. For more detailed information on Helion and its products and services, please visit the Helion website at **www.heliontech.com**.