



## **Summit First with 802.11i-Based FIPS 140-2 on CE/Mobile**

### **Partnership with Juniper Networks delivers support for federal security standard**

Akron, Ohio, August 15, 2008 – Summit Data Communications, a leading provider of Wi-Fi® radio modules and cards for mobile computers and other business-critical mobile devices, today announced that devices with its radios that run the Juniper Networks Odyssey® Access Client FIPS Edition (OAC FE) can be compliant with a federal government security standard known as FIPS 140-2. The partnership with Juniper Networks makes Summit radios the first to support FIPS 140-2 with IEEE 802.11i, the ratified standard for Wi-Fi security, on Windows CE and Windows Mobile®. Summit's support for Juniper Networks OAC FE makes its debut in V2.01 of Summit software, which runs with all Summit radios.

“Many federal government installations have standardized on 802.11i,” said Ron Seide, Summit's president. “But those installations also require FIPS 140-2 support and don't want to abandon 802.11i to get FIPS. Now, mobile computers and other business-critical devices that run Windows CE or Windows Mobile can use Summit radios and OAC FE to support FIPS 140-2 with 802.11i.”

The National Institute of Standards and Technology (NIST) issues Federal Information Processing Standards (FIPS) publications. The FIPS 140-2 publication “specifies the security requirements that will be satisfied by a cryptographic module utilized within a security system protecting sensitive but unclassified information.” In other words, the publication defines the requirements for software modules that perform cryptography, or encryption and decryption, of sensitive data.

Devices that pass all Wi-Fi Alliance® tests for 802.11i support are certified for the Enterprise version of Wi-Fi Protected Access 2™, or WPA2™ - Enterprise. AES-CCMP, the encryption algorithm required for WPA2, is sufficient for FIPS 140-2. Most of today's Wi-Fi radios provide hardware support for AES-CCMP, but NIST requires that AES-CCMP be implemented in software. Juniper Networks incorporates the Odyssey® Security Component, a cryptographic module that is FIPS validated, which implements AES-CCMP in software.

By default, a Summit radio performs all AES-CCMP encryption and decryption in hardware. When the FIPS validated cryptographic module in Juniper Networks OAC FE is invoked, the Summit radio passes control to the OAC FE cryptographic module for all encryption and decryption. Prior to Summit's implementation of support for OAC FE, only Wi-Fi devices running Windows XP or Windows 2000 could use OAC FE for 802.11i-based FIPS.

Support for Juniper Networks OAC FE is available with V2.01 of Summit software, which is generally available now. Mobile computers with Summit radios and Juniper Networks OAC FE will make their debut in Q4 2008.

#### **About Summit**

Summit Data Communications, Inc. is dedicated to providing high-performance wireless LAN radio modules and cards for today's business-critical mobile devices, such as mobile computers, portable printers, medical devices, and industrial automation equipment. Summit radios are optimized for the challenging radio environments in which business-critical mobile devices operate, including factories, warehouses, ports, hospitals, and retail stores. For more information, visit [www.summitdatacom.com](http://www.summitdatacom.com).

Wi-Fi® and the Wi-Fi Alliance® are registered trademarks, and Wi-Fi Protected Access 2 and WPA2 are trademarks of the Wi-Fi Alliance. Windows Mobile® is a registered trademark of Microsoft Corporation.



Juniper Networks, JUNOS and the Juniper Networks logo are registered trademarks of Juniper Networks, Inc. in the United States and other countries. All other trademarks, service marks, registered trademarks, or registered service marks are the property of their respective owners.

###