BlackBerry Advances Security For Government Sector

February 3 2005

BlackBerry® continues its lead as the wireless platform of choice in the government sector as Research In Motion (RIM) (Nasdaq: RIMM; TSX: RIM) today announces the availability of its S/MIME Support Package v4.0 for BlackBerry and FIPS 140-2 security certification for BlackBerry Enterprise Server v4.0.

With advanced security capabilities and a comprehensive wireless solution for managing email, phone, text messaging, organizer, Internet and intranet applications, BlackBerry is widely used by government personnel to enhance operations, productivity and responsiveness. Many government organizations are also using BlackBerry to support Continuity of Operations Planning (COOP) activities by enabling users to efficiently store emergency preparedness information, standard operating procedures, emergency call lists and other continuity of operations documents on their BlackBerry handhelds.

“The BlackBerry platform has consistently led the industry for secure wireless communications in the government sector and our new S/MIME Support Package and the FIPS 140-2 certification for our latest software further strengthens that position,” said Mike Lazaridis, President and Co-CEO at Research In Motion. “A broad range of government customers have come to rely on BlackBerry because of its advanced security architecture, support for government standards and the flexibility to support new and existing initiatives.”

FIPS 140-2 SECURITY CERTIFICATION:

BlackBerry Enterprise Server v4.0™ software and BlackBerry Handheld Software™ v3.8 and v4.0 have received the Federal Information Processing Standards (FIPS) 140-2 validation for the cryptographic modules embedded in the software. The FIPS 140 security standard is issued by the National Institute of Standards and Technology (NIST) and is recognized by both the Canadian and U.S governments. FIPS 140-2 (Security Requirements for Cryptographic Modules) provides the security requirements that are to be satisfied by a cryptographic module implemented within a security system.

“The Cryptographic Module Validation Program (CMVP) enables vendors to demonstrate the conformance of their cryptographic modules to FIPS 140-2, which is an important purchasing requirement for government organizations in North America,” said Randall J. Easter, Director, NIST CMVP. “RIM is being recognized for its BlackBerry validation and its continued support of the FIPS 140-2 program.”

Under the Information Technology Management Reform Act, the Secretary of Commerce approves standards and guidelines that are developed by NIST for U.S. Federal computer systems. NIST collaborates with national and international standards committees, users, industry groups, consortia, and research and trade organizations to get needed standards developed. These guidelines are issued by NIST as standards for use throughout government. NIST develops new standards when there are compelling Federal government requirements such as for security and privacy of sensitive information in Federal computer systems.

ENHANCED SUPPORT FOR S/MIME SECURITY STANDARD:

RIM also introduced its S/MIME Support Package v4.0 for BlackBerry® today. This add-on security software operates with the new BlackBerry Enterprise Server ™ v4.0 for Microsoft® Exchange and Java-based handhelds.

The S/MIME Support Package v4.0 for BlackBerry provides S/MIME (Secure Multipurpose Internet Mail Extensions) support for Java-based BlackBerry wireless devices. S/MIME is an email-system-independent, Internet standards-based protocol that uses public key cryptography to provide writer-to-reader security features, such as authentication, confidentiality and message integrity. This straightforward upgrade allows government and corporate organizations to wirelessly extend their existing email infrastructure, while maintaining both sender-to-recipient encryption and a simple and fast user interface.

New features of the S/MIME Support Package v4.0 running on BlackBerry Enterprise Server include:

Built-in Entrust Entelligence™ Messaging Server support, making it easier to send fully encrypted messages, especially to multiple recipients or recipients outside the corporate domain.
Long message signature checking, allowing users to rely on the server's verification of signatures for large messages.
Support for server-side encryption of S/MIME messages sent to the wireless handheld, increasing message security by allowing BlackBerry Enterprise Server administrators to encrypt signed messages to the handheld.
Automatic retrieval of digital certificates and certificate status when sending or receiving an S/MIME message, reducing process time for certificate requests.
Other features include an improved user interface, attachment viewing support for signed messages, extended IT policy support, enhanced CRL (Certificate Revocation List) support and enhanced certificate status

checking.

The S/MIIME Support Package v4.0 for BlackBerry integrates with advanced solutions from RIM's security partners including Entrust, Diversinet, Tumbleweed Communications and CoreStreet, offering users a choice of technology for their enhanced security needs.

ENTRUST:

Entrust's (Nasdaq: ENTU) Entelligence Messaging Server provides simplified secure messaging by managing certificate retrieval, distribution list expansion, content scanning integration and delivery methods. As a result of EMS integration with the S/MIME Support Package v4.0 for BlackBerry, it is simple and easy for users to send sensitive information from a BlackBerry handheld.

"RIM's integration of the BlackBerry wireless platform with the Entrust Entelligence Messaging Server is a significant extension of our relationship," said Leah MacMillan, Vice President of Solutions at Entrust. "As a result, customers using BlackBerry with the S/MIME Support Package v4.0 can now enjoy simplified secure email and benefit from strong integration with content scanning products and multiple secure email delivery methods."

DIVERSINET:

Diversinet's (OTCBB: DVNTF) Passport Provisioning Server speeds the provisioning of S/MIME and automates the S/MIME user enrollment process, enabling simple user set up.

"Combined with the S/MIME Support Package v4.0 for BlackBerry, Diversinet's over-the-air certificate provisioning offers a simple solution

for mobile enterprise users who need the additional security of S/MIME – the de facto industry standard for end-to-end secure email. By collaborating with wireless carriers, RIM and Diversinet enable enterprise users to comply with regulatory issues for privacy and security of email communications via BlackBerry," said Stu Vaeth, Chief Security Officer of Diversinet Corp.

TUMBLEWEED COMMUNICATIONS:

Tumbleweed Communications (Nasdaq: TMWD) has integrated its Tumbleweed Valicert Validation Authority with the S/MIME Support Package v4.0 for BlackBerry, which will offer users a solution for digital certificate validation that's based on the open standard OCSP (Online Certificate Status Protocol). The Validation Authority allows applications to wirelessly validate the status of a digital certificate; ensuring organizations do not rely on revoked credentials for secure email.

"Combining BlackBerry with the Validation Authority, email messages sent from wireless handhelds can be as secure as email messages sent from desktops on the enterprise LAN," said John Hines, Director of Identity Validation Product Development fro Tumbleweed Communications. "By using S/MIME and validating digital certificates, customers can ensure the security of their wireless email, allowing users to be certain about the identity of the party they are communicating with and the integrity of the messages they are sending."

CORESTREET:

Through the use of technology from CoreStreet, users can manage multiple privileges dynamically, in both offline and online situations. CoreStreet's OCSP (Online Certificate Status Protocol) solution allows

users quick response from the system when checking for certificate status.

“With CoreStreet's distributed OCSP technology, the world's largest and most security-conscious organizations are able use the BlackBerry solution to go beyond the typical approaches to e-mail security,” said Karl Weintz, Vice President of Products at CoreStreet. “Advanced security requires knowing that the message you are reading is both authentic and free of any sort of tampering, and CoreStreet’s technology allows users to validate the integrity of their S/MIME email messages.”