The Health Insurance Commission (HIC) of Australia Selects Rainbow's iKey Authentication Token for PKI-Based Internet Security

Submitted by: Strategic Public Relations Ltd
Tuesday, 4 December 2001

Rainbow eSecurity, a Rainbow Technologies (Nasdaq: RNBO) company and a leading solutions provider of digital content and transaction security solutions, today announced it has received a significant contract from the Health Insurance Commission (HIC) Australia, the nation's leading information management and payment agency for health care. The HIC selected the iKey 2032 authentication token for a panel contract for a Public Key Infrastructure (PKI)-based Internet security deployment to facilitate the introduction of HIC PKI-secured services across the nation's healthcare sector.

The HIC has established the Health eSignature Authority (HeSA) Pty Ltd to act as a PKI registration authority. PKI enables a secure means of sharing inter-clinic communications over the Internet. Users will be authenticated to verify their identity and then authorised to access health related information enabling a high degree of privacy. Rainbow's iKey will be used to store a digital certificate and private keys distributed by HeSA and this will provide powerful two-factor authentication. Users will be able to maintain message integrity and provide non-repudiation and confidentiality for all of their messaging.

“HIC PKI-secured software is internationally renowned for its innovative approach to secure online communication,” said Dr. Brian Richards, chief information officer, HIC. “The use of iKey to secure PKI keys complies with stringent policies to ensure the security and privacy of patient information by using a technology that is stable, robust, and easy-to-use. All Australians have the right to expect their health information to be managed securely.”

“This panel contract is a significant win for iKey and confirms its value in helping to ensure secure Internet communication,” said Shawn Abbott, president, Rainbow eSecurity. “Securing online communication is a critical requirement for the health care professionals of tomorrow. By placing these resources online, HIC is demonstrating how secure internal and external electronic communications can improve the care given to patients anywhere in Australia. We are pleased that HIC chose our iKey 2032 as a critical piece of the their workstation and network security solution.”

A message digitally signed with iKey enables the recipient to identify who has sent the message (authentication) and that the message content has not been altered in any way between the sender and the receiver (integrity). It also ensures the sender cannot, at some later stage, dispute that they created and sent the message (non-repudiation), and, most importantly, that only the person to whom the message is directed can open it (confidentiality).

The iKey 2032, a member of Rainbow's iKey 2000 product family, is specifically designed for use in Public Key Infrastructure (PKI) environments where on-board cryptographic capabilities and uncompromised need for securing private signing keys is critical. The iKey 2032 is FIPS 140-1 Level 2 certified for high assurance security environments. It supports enterprise, business-to-business and business-to-consumer applications built on all major PKI systems, including; Microsoft, Netscape, Entrust, Baltimore, Xcert, Verisign, CyberTrust, Check Point, Computer Associates, PGP from Network Associates, Aventail, KyberPASS and many others. The iKey Software Developer’s Kit (SDK) allows developers to customise the iKey 2032 to support virtually any HIC PKI-secured solution to provide full “plug-and-play PKI”.

Removing certificate storage and signing from vulnerable desktop systems and placing these functions in the token significantly reduces the risk of internal or external security attacks. The iKey 2032 provides a reliable, robust security solution that is easy to use and administer yet provides exceptional PKI-based security solution for desktop applications for the Internet, eCommerce, extranets and corporate intranets. Through user identification data contained in each device, network administrators can grant or deny access based on the user's authorisation level.

The iKey 2032 features 32K of memory to more easily store and manage digital certificates and digital signatures. It also features an added measure of security through new tamper-proof features that make access to iKey internal chips and electronics by hackers virtually impossible. In addition to the iKey 2032’s FIPS140-1 Level 2 certification, the iKey has been submitted to the Australian government’s Defence Signals Directorate (DSD) Evaluated Products List (EPL) for certification to EAL2. IDC recently recognised the iKey as the industry’s leading USB authentication token with a 35 percent share. IDC anticipates the market for USB authentication tokens will grow from million in 2000 to about 6.6 million by 2005.

-ends-

Contact:

Graham Peat
Rainbow Technologies
01932 579200
gpeat@rainbow.com

Dan Chmielewski
Rainbow Technologies
+1 (949) 450-7377
dchmielewski@rainbow.com

Catherine Eyres / Sarah Hewitt
Strategic Alliance International

01494 434434
catherinee/sarahh@strategicpr.net

About HIC

HIC operates one of the largest electronic health benefit and information networks in the world through the administration of government health programs such as Medicare, the Pharmaceutical Benefits Scheme (PBS), the Australian Organ Donor register and the Australian Childhood Immunisation Register (ACIR). As part of HIC's ongoing efforts to provide customers with more options for accessing services, HIC is moving to offer new and improved services on the Internet. The Health eSignature Authority Pty Ltd is an independent registration company established by HIC to facilitate the introduction and deployment of PKI within the health sector.

For more information, visit HIC's Web site at www.hic.gov.au or http://www.hesa.com.au

About Rainbow Technologies

Founded in 1984, Rainbow Technologies is a leading provider of security solutions for the Internet and eCommerce. Rainbow applies its core technology to a variety of Internet applications from securing software, to the acceleration of secure communication for eCommerce and Virtual Private Networks (VPNs). Rainbow's products include; secure Web server and VPN acceleration boards; anti-piracy and Internet software distribution solutions; PKI-based security solutions; voice, data and satellite security systems; and USB-based Web authentication tokens. Rainbow eSecurity is headquartered in Irvine, California, and has offices throughout the United States, United Kingdom, France, Germany, Australia, China, India, The Netherlands, Brazil, and Taiwan. A network of nearly 80 authorized distributors sell Rainbow products worldwide.

For more information, visit our Web site at http://www.rainbow.com

Rainbow Technologies and iKey are trademarks of Rainbow Technologies, Inc. All other company and product names are trademarks of their respective organisations.

The Private Securities Litigation Reform Act of 1995 provides a “safe harbor” for forward-looking statements. Certain information included in our Annual Report on Form 10-K and other materials filed with the Securities and Exchange Commission (“SEC”) (as well as information included in oral statements or other written statements made or to be made by the Company) contain statements relating to the following: dependence upon existing and new product offerings, competition, intellectual property and licensing, future growth, rapid technological and market change, manufacturing and sourcing risks, Internet infrastructure and regulation, the inclusion of network security functionality in hardware or system software, international operations, among others. These conditions involve important factors that could cause actual results to differ materially from those expressed in any forward-looking statements made by or on behalf of the Company. Any forward-looking statements are made pursuant to the Private Securities Litigation Reform Act of 1995 and, as such, speak only as of the date made. Statements made in this document that are not purely historical are forward-looking statements, including any statements as to beliefs, plans, expectations, or intentions regarding the future. The Company assumes no obligation to update information concerning its expectations.