

Media Release

New Cryptlib 3.3 Release Meets TLS Standard

-Open-source security toolkit leads the way in ease-of-use and protection

November 6, 2006 - The latest version of the popular Cryptlib security toolkit is now available. Cryptlib 3.3 is the first open-source software development toolkit to support the TLS-PSK standard*. By building strong mutual authentication into the existing TLS process, TLS-PSK provides a high level of security against phishing attacks that existing HTTP and TLS solutions can't provide.

"Phishing is a multi-billion dollar growth industry that shows no signs of slowing down, because there are almost no effective defences against it. TLS-PSK is a direct drop-in upgrade to TLS that provides a high level of resistance to any phishing attack, and Cryptlib is the first open-source security toolkit that allows you to implement this defence" says Peter Gutmann, Ph.D., creator of Cryptlib, security specialist and international crypto-consultant.

A recent survey of CIO's in US Federal Agencies** revealed that ensuring system security and privacy remains their highest priority. Cryptlib allows even inexperienced crypto-programmers to easily add strong, robust encryption and authentication services to software applications, without needing to know any of the complex low-level details, by providing powerful and easy-to-use digital signature, encryption, key management, and secure session routines. These provide implementations of complete security services such as SSL/TLS, SSH, S/MIME, PGP, and various PKI services that can be easily dropped into existing applications. In this manner Cryptlib enhances system security and privacy, helps to reduce development costs significantly and protects vital commercial information.

Christopher D. Leidigh, Director of Communications and Technology Research at American Power Conversion Corp., (www.apcc.com) says "Cryptographic libraries are at the heart of secure communication systems. If these libraries are poorly designed, or difficult to use, they could be the Achilles heel in any system. However, Cryptlib's architecture has been carefully crafted to protect systems at all levels. The compact and modular nature of Cryptlib enabled APC to implement multiple secure protocols in a very small platform. The wide range of Cryptlib code and extensive documentation make this library the only complete choice for cryptographic needs."

Cryptlib has been used and trusted for over 10 years by significant organizations worldwide including American Power Conversion Corp., Lexmark International, the Netherlands Internal Revenue Service, and Mutual & Federal Insurance Co., among others.

Visit www.cryptlib.com for more information, or to download a free evaluation copy of the software.

###

* TLS-PSK is an enhanced secure connection and authentication mechanism used with TLS, the widely-used Internet security technology formerly known as SSL.

** Information Technology Association of America's Sixteenth Annual Survey of Federal CIO's. February, 2006.

Contact:
Shayne Jones
Business Development Manager
Digital Data Security Limited
Ph: +64 9 411 7297
<mailto:shayne.jones@gmail.com>