

## **Cylink To Provide End-to-End Security for WAP e-Business Transactions**

### ***Company Plans to Offer Both Software and Hardware Solutions to Close 'The Gap in WAP'***

**SANTA CLARA, Calif.--(BUSINESS WIRE)--Oct. 25, 2000**

Cylink Corporation (NASDAQ: CYLK), today announced that it plans a series of initiatives to provide increased security for data transmissions made over wireless mobile devices employing WAP (Wireless Application Protocol) technology. Cylink's new technologies will, for the first time, provide a single, end-to-end security solution, resolving vulnerabilities inherent in current WAP data transmission paths and greatly improving the security of e-business transacted over wireless devices.

Cylink's new solutions will ensure end-to-end security from the wireless device to the final destination, the Web server. This eliminates the ability of malicious operators to intercept, tamper with or redirect the data at the WAP gateway and thereby compromise key information such as end users' phone numbers and account data. Cylink's new offerings will also offer a variety of architectural advantages that ease implementation as well as migration from wired and wireless networks.

"Security will be a key issue in the future success of wireless e-business, given that business-to-business applications and personal financial applications are driving the demand for wireless Web-enabled devices," said William Crowell, President and CEO of Cylink. "Problems will emerge when new WAP phones enter the market unless security solutions that work with the proposed WAP standards are in place."

#### **The GAP in WAP**

To protect data sent over the Internet by wireless devices (such as cellular phones, laptop computers, or personal digital assistants), two different security protocols are used. First, the Wireless Transport Layer Security (WTLS) protocol provides limited security from the WAP-enabled device to the WAP server, typically housed at the telecommunications provider. Second, the Secure Sockets Layer (SSL) protocol provides security from the WAP server over the Internet to the recipient's Web server.

When the WTLS-to-SSL protocol translation occurs in the WAP server, the data is unencrypted and temporarily exposed to attack. This point, The Gap in WAP, makes data vulnerable to malicious intruders. Programs can be used to send end-user data elsewhere, including phone identity and account information. In addition, any authentication of the user that was done in the device would likely stop at the WAP gateway. So while adoption of the two standard protocols has been widespread, the two-part nature of this solution opens up a security risk.

## **Cylink's Advantages**

Cylink's wireless security strategy addresses these problems with end-to-end security offerings that include virtual private networking (VPN) software, VPN hardware, Public Key Infrastructure products, smart cards, smart chips and smart tokens. With Cylink, companies hosting e-business applications, wireless providers, and phone manufacturers will be able to implement a solution that is compliant with WAP Forum Standards, creating a secure environment for the exploding wireless market.

Customers using Cylink's approach to WAP security, the first of which will be commercially available in September 2000, will benefit in many ways:

### **-- Application-Layer Encryption. Unlike WAP-to-TCP/IP security**

solutions available today, Cylink's solutions will encrypt above the WTLS protocol level at the application layer. The solution is then "wireless provider independent" so customers and business partners can choose whichever network infrastructure and WAP device suits their needs. Any WAP 1.1 or later device is supported.

- No Pre-Loading of Software on the Wireless Client. End-users of WAP-enabled devices will not have to initiate downloads or install additional software.
- Flexible Security Policy Deployment. Since financial institutions and other e-commerce service providers will likely administer and deploy WAP servers along with their e-commerce Web servers, Cylink's solution is designed so that the WAP server can be located and administered by either the telco or the bank/e-commerce provider, closing the security gap. This way, banks and the telecommunications providers may deploy their respective services in a manner that suits them, or their corporate security policies, best.
- Eliminates Application Modification or Integration Expense. Cylink technology enables the migration of more security-sensitive applications from wired and wireless networks without requiring modifications to the applications or integration work. Many single source public key infrastructure (PKI) providers, on the other hand, are proposing expensive, unnecessary, and overly complicated implementations to secure wireless technology. This combination of PKI products and developers' toolkits require extensive technical integration to fit a company's needs. And none of the solutions being proposed today fill the vulnerability of "The Gap in WAP."

## **Cylink Experience in Wireless, A Market about to Explode**

Cylink was one of the first companies to offer cryptography-based solutions for commercial e-business applications. In addition, it was one of the first companies to provide security for wireless and satellite communications. Cylink's royalty-free security algorithm, SAFER+, was adopted last year for use in Bluetooth, the new European wireless standard which enables short

range, RF-based devices to conduct mobile or m-business. Manufacturers are expected to ship more than 1.7 billion Bluetooth-enabled devices a year by 2005, creating a \$3.4 billion market, according to Merrill Lynch & Co.

In addition, the Yankee Group predicts the expected growth of WAP-enabled devices to be robust: total wireless subscribers will top 1.26 billion by 2005, up from 469 million at year-end 1999. Hundreds of millions of wireless handsets will be able to access the Internet through WAP-based technologies. WAP is the platform that makes added services such as stock prices, email, flight schedules and electronic commerce available to mobile devices, linking them to Web sites that have been reconfigured for this purpose. The Gartner Group predicts that at least 95% of the mobile phones shipped in 2004 will be WAP-enabled.

---

[ [Home](#) | [Contact](#) | [MobiChat](#) | [Experts database](#) | [Let's do it](#) ]

Comments to the content of this page can be posted on the [MobiChat](#) discussion group



**Signature Security. - Free Online Library**