FT-18-7425
Ray Wagner

Gartner FirstTake
7 November 2002

Quantum Key Distribution: Advanced Technology But Few Applications

MagiQ's new cryptographic system uses quantum key distribution (QKD) technology. New approaches to key distribution secured by quantum physical phenomena are interesting but won't end traditional key-based security.

Event: On 4 October 2002, MagiQ Technologies announced a cryptographic system that uses QKD technology to secure communications over fiber-optic lines. MagiQ plans to introduce a commercial product based on this technology in 2H03. A competitor, ID Quantique, has already introduced a commercial QKD system.

First Take: The development of QKD technology can raise the level of security in some real-world applications. Enterprises that are extremely security-conscious — for example, government agencies and financial services providers — may find highly specialized uses for QKD. However, Gartner believes widespread commercial adoption will occur only if providers can overcome serious shortcomings, including:

- **Limited reach:** QKD can serve only for point-to-point communication, has a current reach of only 67 kilometers and requires a direct fiber-optic link. The technology's usability within Internet infrastructure (vs. add-on infrastructure) remains unproven.

- **Technological difficulty:** As with most new and highly complex technologies, the problems of early implementation will limit QKD's effectiveness.

- **Cost:** QKD technology and the infrastructure to support it (including a private fiber channel) carries a prohibitive cost for most enterprises.

However, the principal obstacle to widespread QKD adoption is that current key-distribution mechanisms will provide acceptable security for all but the most risk-averse enterprises into the foreseeable future. These announcements do not signal the demise of current security and encryption systems. True quantum computing technologies can theoretically provide massive increases in processing power as well as computational tools that may render traditional asymmetric cryptography (that is, public-key infrastructure) obsolete. However, QKD technologies do not use quantum computing. Gartner believes quantum computing will not achieve even limited usability by commercial enterprises before 2010 (0.7 probability).

Analytical Source: Ray Wagner, Gartner Research

Written by Terry Allan Hicks, Gartner News

Recommended Reading and Related Research

- “Laptop/Disk Encryption in a World Without PGP” — The withdrawal of Pretty Good Privacy products means enterprises must consider alternative security measures. **By Ray Wagner**

- “Enterprise IT Security Management Defined” — Enterprise security often requires compromises between best-of-breed products and broader suites. **By Mark Nicolett and others**

(You may need to sign in or be a Gartner client to access all of this content.)