

# NetworkWorld Reprint

The leader in network knowledge ■ [www.nwfusion.com](http://www.nwfusion.com)

February 23, 2004 ■ Volume 21, Number 8

## Tops in innovation

**NetworkWorld 2004**  
**Category Breaker**

Selected by five of our columnists, these products step beyond the norm with interesting solutions for today's enterprise network problems.

### Adding a jolt to PKI-based messaging

Voltage Security's Voltage Security Platform (Voltage SecurePolicy Suite, Voltage SecureMail and Voltage SecureFile)



**James Kobielus**  
*Above the Cloud*

Secure messaging still hasn't broken into the enterprise mainstream, in spite of considerable vendor innovation over the past several years. Among deployed secure-messaging systems, public-key-infrastructure-based solutions predominate.

However, PKI-based secure-messaging products are still too complex to set up and administer within and among diverse organizations. Automatic and transparent handling of key issuance, management and retrieval, on demand, would help considerably. Identity-based encryption (IBE), implemented in Voltage Security's Voltage Security Platform product family, is a breakthrough PKI approach that does this.

The fundamental innovation behind Voltage's IBE is that a message sender doesn't need to know whether an intended recipient has a public-key certificate. Users needn't ever obtain an X.509 certificate to participate in IBE-based secure communications. Instead, people can use any arbitrary character string — such as their e-mail address — as their public key. Consequently, public-key issuance becomes an implicit, latent and automatic component of e-mail account setup. Any recipient can simply

assume a public key based on identity information retrieved from existing directories.

Under this IBE-based architecture, companies don't need infrastructure components such as certificate authorities and repositories. The sender simply addresses and sends the secure message to recipients as he normally would, using the recipient's e-mail address. The sender's e-mail client uses the recipient's e-mail address as the public key when encrypting or signing messages bound for the recipient. The Voltage server-side infrastructure — the SecurePolicy Suite or hosted SecurePolicy Service — takes care of binding IBE-based public keys to freshly minted, short-lived private keys, and distributing private keys to recipients, on demand.

To read secure e-mail, the receiver requests a private key from the sender's SecurePolicy Suite (or the hosted Voltage SecurePolicy Service). The server-side infrastructure provisions plug-in software — Voltage SecureMail — to recipient desktops, and authenticates senders and recipients against existing directories.

Voltage's IBE approach simplifies key management. Other secure-messaging vendors surely will take note and attempt their own IBE-based solutions (an approach that has been around since the 1980s, but Voltage introduced the first commercial version last July).

However, Voltage doesn't appreciably simplify the configuration of secure-messaging environments. Users must have Voltage client



When integrated with an e-mail client, Voltage SecureMail eases encryption and decryption of secure messages.

software integrated with leading e-mail clients, including Microsoft Outlook. And it doesn't provide qualitatively superior secure-messaging features. Many of Voltage's other secure-messaging features — including short-lived private keys, server-side key revocation, and ad hoc enrollment and provisioning — can be found elsewhere.

Voltage SecurePolicy Suite costs \$50,000 per server; SecureMail, \$50 per user; and SecureFile, \$20 per user. Clients are available in packages ranging from 1,000 to 100,000 users, and in corporate volume discounts. The company also provides subscription pricing as an alternative.

*Kobielus is a senior analyst in Alexandria, Va., with Burton Group. He can be reached at [jkobielus@burtongroup.com](mailto:jkobielus@burtongroup.com).*