



when infrastructure starts with you,
count on **hp storage** for:
increased efficiency **GO**



To print this page go to your File menu and select Print (or use Ctrl (Control) + P on your keyboard)

[< Return to Previous Page](#)

February 11, 2002

Kyberpass Plugs PKI Into Outlook

By *Dennis Fisher*

PKI products have a reputation for being expensive, tortuous to implement and lacking in applications.

But an Ottawa developer is hoping to change that with a public-key infrastructure plug-in for Microsoft Corp.'s Outlook mail client.

Kyberpass Corp. next week at the RSA Conference in San Jose, Calif., will unveil Secure E-mail TrustPlatform, a package comprising K2 E-mail Agent Plug-in and Validation TrustPlatform.

The K2 agent is the first e-mail plug-in compliant with Identrus LLC, a network of banks and financial institutions that uses a PKI system for payments, nonrepudiation and validation of parties involved in e-business transactions.

During a typical message creation process with TrustPlatform, the K2 agent prompts the user for a password, which can be used to access the private key for signing. The message is condensed using a hash function, and the hash is encrypted with the sender's private key.

The system then retrieves the recipient's public key through an LDAP lookup or local storage and encrypts the message with a one-time session key (which is encrypted with the recipient's public key). The message can then be sent to the recipient.

Validation TrustPlatform performs the certificate and digital signature validation processes.

The key difference between Kyberpass' product and underlying PKIs is that Secure E-mail TrustPlatform handles all the certificate and digital signature operations in the background so that they are transparent to the user.

Security experts who have tested the product said it may finally show IT managers that PKIs can be useful.

"I've been around PKI since the spec was written, and the problem has always been applications," said Layton Peck, vice president of e-security at BCE Emergis Inc., an Ottawa-based business-to-business software provider. "We see e-mail as something that can aid downstream adoption of PKI, and this is a very solid approach to that problem. It's a very secure and intuitive product."

Kyberpass officials said their goal was to create a product that is secure yet doesn't require swarms of systems integrators to implement. To that end, there is a central policy management feature and support for secure local and remote administration.

The system, due March 4, is interoperable with certificate authorities from major PKI vendors, including RSA Security Inc., Baltimore Technologies plc. and VeriSign Inc. The K2 agent supports all S/MIME (Secure Multipurpose Internet Mail Extension)- compliant e-mail clients but is designed to integrate seamlessly with Microsoft's Outlook 98, Windows 2000 and Windows XP.

Copyright (c) 2001 Ziff Davis Media Inc. All Rights Reserved.