



Network Computing

Driving IT Decisions

Search

NWC TechWeb | [Site Guide](#)

IT help & resources available for victims of 9-11-2001

Get Network Computing on your mobile device. FREE. AvantGo

- [▶ Getting Started](#)
- [▶ Tech Industry & Finance](#)
- [▶ Government](#)
- [▶ Research Center](#)
- [▶ Sales & Marketing](#)
- [▶ Current Issue](#)
- [▶ Past Issues](#)
- [▶ Tech Library](#)
- [▶ Free Newsletters](#)
- [▶ Manage your Subscription](#)
- [▶ RFP Solution Center](#)
- [▶ Browse by Topic](#)
- [▶ Ask the Experts](#)
- [▶ IT Pro Downloads](#)

Security

SNEAK PREVIEW

Kyberpass Helps Make Microsoft Outlook an E-mail Platform You Can Trust

April 29, 2002
By [Mike Fratto](#)

Given the complexity of the tools in today's e-mail packages -- and the lack of good documentation -- it's no surprise that users frequently have trouble sending and receiving digitally signed or encrypted e-mail. Also consider that most e-mail programs don't include native support for security, and you're looking at an uphill battle to make digital signatures and encryption seamless facets of messaging.

- [Issue TOC](#)
- [Print full article](#)
- [E-Mail this URL](#)

But Kyberpass Corp. makes impressive headway with its Secure E-mail TrustPlatform, a Microsoft Outlook 98, 2000 and 2002 plug-in aimed at reducing user stress while keeping communications secure. Truth be told, the most compelling part of TrustPlatform is its encryption-certificate-storage and OCSP (Online Certificate Status Protocol) functionality, which is missing from Outlook.

I tested TrustPlatform in our Syracuse University Real-World Labs® and found it a welcome addition when used with Outlook's certificate handling. It should be especially useful if your organization requires support for OCSP, local encryption-certificate repositories and password retention.

To generate digital certificates, I used a Microsoft Windows 2000 server configured with Certificate Server and Active Directory. I also used certificates from Thawte and demonstration certificates issued by Kyberpass. The certificates I generated on my own CA (Certificate Authority) and via Thawte were multiuse, meaning the public/private keys and the associated certificate were used for both signing and encrypting. The certificates I obtained from Kyberpass (two per user) were single use -- one certificate and public/private key pair were used for digital signatures, and the other certificate and key pair were used for digital encryption.

An examination of the pros and cons of single-use certificates is beyond the scope of this article, but, essentially, it's OK to escrow a certificate and key pair used solely for encryption so you can later decrypt data encrypted by that key pair. It is not OK to escrow a certificate and keys used for digital signatures, because more than one person has access to the signing key; therefore, no one person can be identified as the sole owner. Both Kyberpass and Outlook support single and multiuse keys.

As soon as TrustPlatform is installed, it enhances the certificate services in Outlook. However, you need to warn users not to make adjustments in Outlook's Security tab, because those configurations will conflict with the Kyberpass configurations. Once the keys are added to TrustPlatform, a number of configuration options are available for reading and sending secure e-mail, and for configuring password retention.

Your digital certificates and associated public/private key pairs are your digital ID. When you perform any action using your keys, such as signing or decrypting an e-mail message, you need to enter a password to authorize that action. Although you should keep

Advertisement

Compare IT

Compare [Firewall](#) solutions from:

- Cisco
- Nokia
- WatchGuard



Tech Library Spotlight

White Paper: IP Virtual Private Networks -- [Allowing companies, institutions, and government to leverage productivity gains and competitive advantages.](#)



[< more spotlights >](#)

RFP/RFQ Builder

- [▶ Browse Products](#)
- [▶ Build a Custom RFP](#)
- [▶ View Current RFPs](#)

White Papers & Research Reports

- [▶ Browse White Papers](#)
- [▶ Browse Research Reports](#)
- [▶ Search for Documents](#)
- [▶ Get Free E-mail Updates](#)

Expert Advice Forum

- [▶ Browse Current Posts](#)
- [▶ Check Out Our Experts](#)

Vendor News

- [▶ Telecommunications](#)
- [▶ Multimedia](#)
- [▶ Internet Technologies](#)

Get NWC

- [▶ Free Newsletters](#)
- [▶ Free Magazine Subscription](#)
- [▶ Security Alert Consensus](#)
- [▶ AvantGo for your PDA](#)
- [▶ Manage your Subscription](#)

IT Pro Downloads

- [▶ Editor's Pick](#)
- [▶ New Arrivals](#)
- [▶ Browse All Downloads](#)

Interactive Buyer's Guide

- [▶ Browse Guides](#)
- [▶ Company Listings](#)
- [▶ Search for Products](#)

They rely on Intel®-based servers to power their enterprise solutions.

- ▶ DELL
- ▶ FIAT
- ▶ BARCLAYS
- ▶ EASY LINK

your keys password protected at all times, you may want to use TrustPlatform's password-retention option: Enter a password once, then continue to sign or decrypt e-mail for up to 60 minutes without having to re-enter that password. The trade-off for this convenience is that anyone can send signed e-mail from an unattended Outlook client while the password is retained. Fortunately, you can adjust the password-retention time to meet the needs of your security policy.

You read my MIME

As part of its read options, TrustPlatform lets you choose how to store messages after you've decrypted and read them. You can opt never to store decrypted messages, be prompted whether to store a decrypted message or always store decrypted messages. I suggest you store your messages encrypted to be on the safe side. Another read option is selecting the certificate that will decrypt messages you receive; it can be a disk file or a hardware token.

Vendor Information

By default, Outlook 98 and 2000 don't check certificate revocation, which means that OSCP options bear examination. You can download and manually install a CRL (Certificate Revocation List) from the CA, or you can add a registry key (and apply the latest service packs) to make Outlook automatically check the CDP (Certificate Distribution Point) for revocation. Unfortunately, the CDPs, which are published periodically, are as current only as their latest publishing. In my case, Microsoft's Certificate Server can publish on ly as frequently as every hour. OSCP tries to solve the time issue by providing revocatio 1 data as soon as it becomes available. When a digital certificate is received, client software, such as TrustPlatform's E-mail Plug-in Agent, queries the OSCP responder 3 see if the certificate is revoked. (For more information, see "[Certificate Revocatiom: When Not To Trust.](#)")

Kyberpass Secure E-mail TrustPlatform, \$30 per client for deployments of 1,000 or more. Kyberpass Corp., (800) 845-1140, (613) 727-6556; fax (613) 727-8238. www.kyberpass.com

At minimum, TrustPlatform needs to know an OSCP responder address and port number to work. Optionally, OSCP requests can be signed by the user and employ SSL (Secure Sockets Layer) for added security. I configured my options to prompt me to authenticate a signature and sign all requests. When I tried to open a signed e-mail message, TrustPlatform prompted me to verify the signature, which I did, and it sent an OSCP query to the responder. Once that was done, I knew I had a valid signature from a current certificate. Certificate-status checking is critical if you want to know if the signer is still authorized to use the certificate.

Sign, Sealed, Delivered

TrustPlatform can be configured to sign all outgoing messages by default, which means one less step for end users. In addition, TrusPlatform can request a signed receipt from message recipients who use TrustPlatform. Another handy feature is the ability to send a user's encryption certificate with his or her message, which is useful if that person wants others to send encrypted e-mail.

One important option is choosing to send a signed e-mail as a multipart e-mail or as a signed attachment. If you send a signed e-mail message as multipart, then the recipient will be able to read your message even if he or she can't verify your signature. This is useful when sending to someone outside your administrative domain. If you send your e-mail as a signed attachment, then the recipient will need to have an e-mail client that supports S/MIME (Secure MIME)

Encryption options are fewer. As with signing, TrustPlatform can be configured to encrypt all messages by default, though unless you are always sending e-mail within a single community of interest, you should probably manually encrypt each e-mail message that requires privacy. This is easily done with a press of a button.

Once TrustPlatform is installed, sending e-mail is a snap. Just compose a message, then choose the sign and encrypt buttons on the menu bar. If you're encrypting e-mail, TrustPlatform will first check to see if it has an encryption certificate in the local store. If it does not, the product will start searching through the configured directories until it finds a match or fails. If you elect to get return receipts, message recipients who have TrustPlatform installed will automatically send back signed receipts.

TrustPlatform can store user encryption certificates locally and search for them in a directory. If an intended recipient's certificate can't be found, TrustPlatform either will prompt the sender to return to the message and modify his or her recipient list, or it will automatically remove the recipients who don't have certificates and then send out the e-mail.

Configuring LDAP with this product is easy if you know all the options. For example, Kyberpass gave us our certificates and the directory entry so TrustPlatform could look up recipient encryption certificates. All I needed to do was enter the directory IP address, port number and search base (the part of the directory where my certificates are stored). I accepted the default search-size limit, which defines the number of entries the search will return. Most often that number will be less than five.

Considering TrustPlatform's ease of use and relatively low price of \$30 per unit for

Site Navigator

- ▶ [Site Guide](#)
- ▶ [Browse by Category](#)
- ▶ [Past Issues](#)
- ▶ [Current Issue](#)
- ▶ [Daily Blog](#)
- ▶ [Advanced Search](#)

MicroSites

- ▶ [UnixWorld](#)
- ▶ [CMP Metrics](#)
- ▶ [Network Design Manual](#)
- ▶ [NWC Radio](#)



Get NWC

- ▶ [Subscribe to Network Computing magazine](#)
- ▶ [Sign up for our free, weekly newsletters](#)
- ▶ [Subscribe to our Security Alert service](#)
- ▶ [Manage your existing subscriptions](#)

TechQuiz

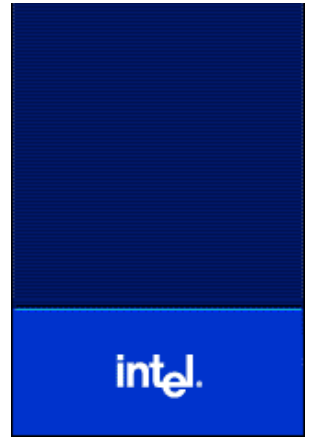
Take our [TechQuiz](#) on Microsoft's .NET platform. Correct answers will qualify you to win one of two nifty USB-based keychain hard drives from our sponsor, Epicor.



Spotlight

[Guess which products and services](#) we'll honor at our annual Well-Connected Awards ceremony during N+I 2002 next month, and you could win a Creative Labs Nomad Jukebox "C".

Also, be sure to check out [our list of finalists](#).



Current Issue



Site Services

- ▶ [Build and submit RFPs, RFQs, and RFI](#)
- ▶ [Download white papers and research reports](#)
- ▶ [Compare products, side-by-side](#)
- ▶ [Browse products and services](#)
- ▶ [Download shareware, freeware, and demoware](#)

Technology Guides

- ▶ [Data Management and Storage Technology](#)
- ▶ [Digital Convergence](#)
- ▶ [Mobile & Wireless Technology](#)
- ▶ [Business Applications](#)
- ▶ [Infrastructure](#)
- ▶ [Network and Systems Management](#)
- ▶ [Security](#)
- ▶ [Service Providers and Outsourcing](#)
- ▶ [The Business of IT](#)



Choose a platform:

1,000 clients, this product may be just what you need to secure your Outlook communications.

Mike Fratto is a senior technology editor based in Network Computing's Syracuse University Real-World Labs®; he covers all security-related topics. Prior to joining this magazine, Mike worked as an independent consultant in central New York. Send your comments on this article to him at mfratto@nwc.com.

Network Computing



Sites:

[Home](#) | [IT Pro Downloads](#) | [RFP Solution Center](#) | [Ask the Experts](#) | [UnixWorld](#) | [Learn IT](#) | [Interactive Buyer's Guide](#) | [Tech Library](#) | [CMPmetrics](#) | [Compare IT](#) | [Network Design Manual](#) | [Vendor News](#) | [NWC Radio: Streaming Audio Shows](#)

Services:


[Free Newsletters](#) | [Events](#) | [Sales & Marketing](#) | [Magazine Subscriptions](#) | [Site Map](#) | [FAQ](#) | [Contact Info](#)

Magazine:

[Current Issue](#) | [Past Issues](#) | [Article Index](#) | [Technology Guides](#) | [Real-World Labs](#) | [2001 Edit Calendar](#) | [2002 Edit Calendar](#)

Other CMP Sites:

[Bank Systems & Technology](#) | [eBusiness Expo](#) | [InformationWeek](#) | [Insurance & Technology](#) | [InternetWeek](#) | [PC Expo](#) | [TechCalendar](#) | [TechEncyclopedia](#) | [TechLearning](#) | [TechWeb News](#) | [TechWeb Webcasts](#) | [Wall Street & Technology](#)



tech LEARNING MORE>>
Your custom-configured system
is on the way. The same day.

TechWeb is brought to you by [CMP Media LLC](#), Copyright © 2002 - [Privacy Statement](#) [Ad Info](#)