CertiPath
www.certipath.com

Trust Validator: Extended Validation for Email

Trusted Impersonation: Data loss & Malware detection across Desktops and Enterprise

Man-in-the-Mailbox attacks continue to be the most prevalent malware distribution channel supporting advanced persistent threats (APT) to organizations. The most commonly deployed defensive strategy requires users to send digitally signed email and to trust only those emails similarly digitally signed.

However, the use of low assurance commercially issued identity credential to digitally sign emails has allowed the MITM to appear just as trustworthy as a federal credential holder.

"...the use of low assurance commercially issued identity credential to digitally sign emails has allowed the MITM to appear just as trustworthy as a federal credential holder."

- Universally security policy has been implemented to recognize an email as either signed or unsigned. Users are unfamiliar or untrained with using and understanding secure email
- There are 'levels of assurance' assigned by issuers that determine some signature certificates are more trustworthy than others ... but this is not visible to users, they all appear identical.

Secure email has also introduced a second threat to enterprises; bad internal or external actors misusing email encryption. Detecting data exfiltration and malware veiled by encryption through secure encrypted email with unknown keying material is a growing threat.

- Users can encrypt email to unknown recipients that can't be inspected by outbound mail server/gateway.
  - No key escrow policy
  - Self-generated key-pairs/certificates
  - Otherwise, no central access to keying material
- Masquerading Malware
  - The largest attack surface for malware entering enterprise is the inbox. In-bound encrypted email cannot be scanned if it is encrypted with unknown keying material

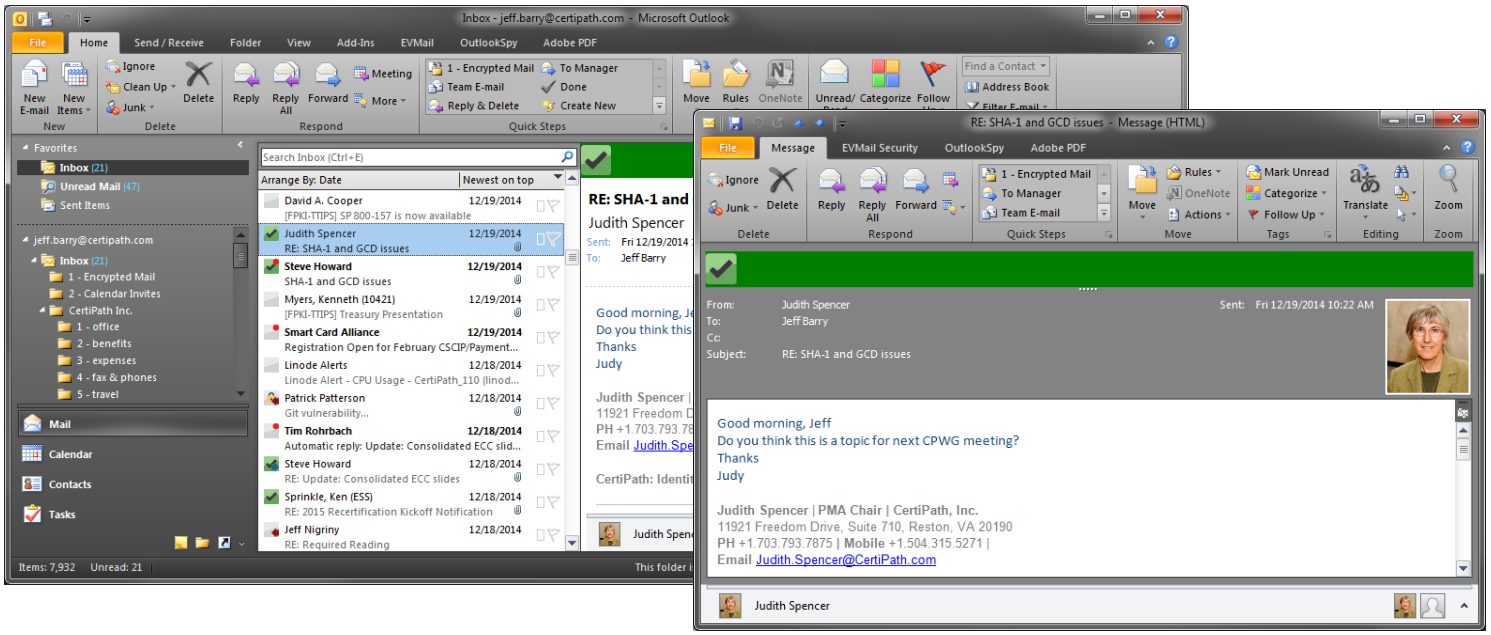
11921 Freedom Drive, Suite 710, Reston, VA 20190
Phone: (703) 793-7870 Web: www.certipath.com

CertiPath
www.certipath.com

Trust Validator: Extended Validation for Email

Trust Validator combats Trusted Impersonation and the use of untrustworthy credentials by allowing administrators to centrally manage inbox trust polices and giving users the ability to visually differentiate an email's security level based on commonly accepted assurance levels such as PIV, PIV-I, or those defined locally by an Agency or Organization.

- Central Policy Management
- Validate the authenticity of the signer to combat:
  - Advanced Persistent Threat attacks on the inbox
  - Malware senders
- Centrally store in-bound/ outbound encrypted mail separate from plaintext email for forensic analysis focused on:
  - Data Loss
  - Malware
  - Internal bad Actors



NEW INBOX ICONS! SIMPLE USER INTERFACE!

THE FULL SECURITY OF PKI BROUGHT TO YOUR INBOX.

For more information on CertiPath's Trust Validator plugin and how it can improve email security in your organization, please contact us at Info@CertiPath.com.

11921 Freedom Drive, Suite 710, Reston, VA 20190
Phone: (703) 793-7870 Web: www.certipath.com