



***Implementing Transparent Security
for Desktop Encryption Users***

Solutions to automate e-mail encryption with external parties

February 2008

Entrust is a registered trademark of Entrust, Inc. in the United States and certain other countries. Entrust is a registered trademark of Entrust Limited in Canada. All other company and product names are trademarks or registered trademarks of their respective owners. The material provided in this document is for information purposes only. It is not intended to be advice. You should not act or abstain from acting based upon such information without first consulting a professional. ENTRUST DOES NOT WARRANT THE QUALITY, ACCURACY OR COMPLETENESS OF THE INFORMATION CONTAINED IN THIS ARTICLE. SUCH INFORMATION IS PROVIDED "AS IS" WITHOUT ANY REPRESENTATIONS AND/OR WARRANTIES OF ANY KIND, WHETHER EXPRESS, IMPLIED, STATUTORY, BY USAGE OF TRADE, OR OTHERWISE, AND ENTRUST SPECIFICALLY DISCLAIMS ANY AND ALL REPRESENTATIONS, AND/OR WARRANTIES OF MERCHANTABILITY, SATISFACTORY QUALITY, NON-INFRINGEMENT, OR FITNESS FOR A SPECIFIC PURPOSE.

© Copyright 2008 Entrust. All rights reserved.

Table of Contents

1	Introduction	1
2	The Challenges of Client-based E-mail Encryption	2
3	Entrust Entelligence Messaging Server Overview	3
4	Simplifying the User Experience	4
	4.1 Certificate Lookup	4
	4.2 Sending Encrypted Messages Offline	6
	4.3 Offloading Message Encryption.....	6
5	Virus- and Content-Scanning Encrypted E-mail.....	7
6	Summary	9
7	About Entrust	9

1 Introduction

Desktop e-mail encryption has been used by organizations for many years to secure sensitive data. Traditional use has been confined to communication between users within a trusted network — either in the same organization or between two organizations that have established a trust relationship by cross-certifying their public key infrastructures (PKI). The advent of the Internet and electronic communication has encouraged more and more organizations to seek methods that will enable them to exchange secure e-mail with users outside of their trusted network.

With the increase of electronic communication with external parties, organizations must consider how their sensitive corporate information will be kept secure while pushing forward with e-enabled processes designed to improve service and reduce cost. From protecting confidential corporate financial information, intellectual property and client data, to adhering to emerging compliance regulations, e-mail encryption has become a fundamental tool to secure data — not only within the organization but with external users as well.

While desktop e-mail encryption users can technically send e-mails to external users, the real-life usability leaves much to be desired. From obtaining recipient certificates to dealing with encryption incompatibility or recipients without certificates, desktop e-mail encryption users often encounter significant challenges when attempting to e-mail external recipients. Productivity is severely hindered or, worse yet, users avoid encrypting to avoid the difficulties. This document outlines these challenges and approaches that can help streamline the encryption process, making it simple and transparent for desktop encryption users throughout the organization.

2 The Challenges of Client-based E-mail Encryption

Client-based e-mail encryption — sometimes referred to as desktop or end-to-end encryption — occurs when e-mail messages are encrypted using the client e-mail software on their device (e.g., personal computer or handheld mobile device such as RIM's BlackBerry). Once encrypted, the message is sent through the e-mail network for delivery to the external recipient. Upon receipt, the recipient opens the encrypted message and decrypts the contents through some form of user authentication (e.g., password).

Client-based e-mail encryption introduces several new user considerations that are not encountered when sending clear-text (un-encrypted) e-mails. Some of these considerations include:

- In order to encrypt an e-mail message for a given recipient, you must have that recipient's credentials (i.e., public key or certificate)
- Users often do not know how to obtain and store recipient encryption credentials or, worst yet, a recipient may not even have encryption credentials at all
- Encrypting a message on the client device requires CPU processing and, depending on the situation, can introduce frustrating delays as the user waits for the completion of the encryption process
- Users cannot send messages in offline mode if they do not have all the recipients certificates

The result is that client-based e-mail encryption introduces barriers that make encryption not only frustrating for end-users, but also difficult for organizations to enforce since the decision of when and what to encrypt resides with the individual user.

Another key consideration with client-based e-mail encryption relates to the IT and security managers who have content scanners deployed within their e-mail network. Since e-mails are encrypted locally on the sender's device (e.g., BlackBerry or PC), messages cannot be deciphered until they reach the intended recipient. This means that corporate security processes such as antivirus scanning and content analysis cannot be performed on encrypted mail traffic. The result is that critical IT processes are circumvented and security policies may be breached.

Fortunately, the Entrust Entelligence Messaging Server (EMS) is designed to address these issues and dramatically simplify e-mail encryption for not only desktop encryption users, but for also for virtually any type of e-mail deployment including standard Microsoft Outlook or Lotus Notes clients, RIM BlackBerry clients or even environments based on a Web mail infrastructure. EMS not only automates the process for end-users, but also centralizes an organization's encryption function to ensure that corporate policies are adhered to and activity can be logged and audited from a common platform.

3 Entrust Intelligence Messaging Server Overview

As a pioneer of e-mail encryption who understands the importance of user experience and seamless technology integration, Entrust developed an e-mail encryption server designed to automate the encryption process, thus making secure communication simple for both senders and recipients. Supporting a broad range of sending and delivery options, including leveraging the capabilities of client-based e-mail encryption clients such as Entrust Intelligence Desktop Solution (EDS) or Entrust Intelligence Security Provider (ESP)¹, Entrust facilitates the process of sending encrypted e-mail to make it virtually identical to sending clear-text (un-encrypted) messages.

Entrust Intelligence Messaging Server is an e-mail encryption appliance that integrates into an existing e-mail infrastructure. EMS works on behalf of e-mail senders to conduct a variety of tasks traditionally performed by the end-user during the e-mail encryption process.

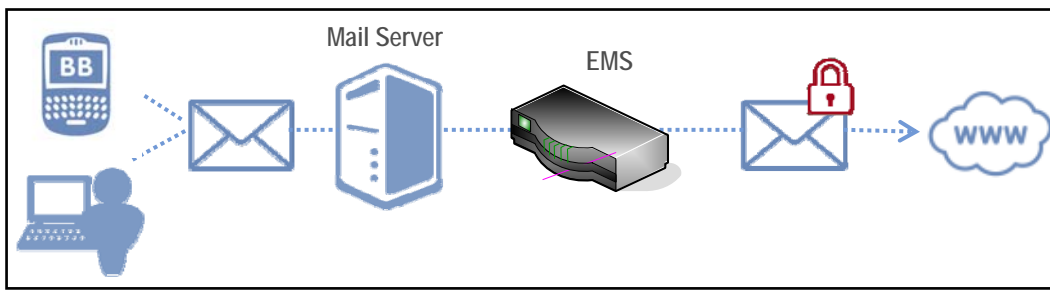


Figure 1: EMS deployed at the boundary of a corporate network

While the above diagram has been simplified to describe the solution concept, it shows how EMS can be deployed at the edge or boundary of a corporate network to handle all outbound and inbound encryption requests. In addition to streamlining e-mail encryption within the organization, EMS contains a variety of features that make e-mail encryption simple for external recipients outside of your organization.

¹ EDS and ESP are desktop client applications that allow organizations to easily deliver a managed digital ID to the user's desktop for authentication, encryption and digital signature capabilities to protect sensitive information, either in transit or stored on disk.

4 Simplifying the User Experience

4.1 Certificate Lookup

E-mail encryption is based on the premise that the message must be encrypted specifically for each intended recipient. To do this, the sender must have the external recipient's public credentials — encryption key, certificate, password, etc. — stored in their e-mail application address to perform the encryption process.

While desktop encryption users may have access to encryption credentials for internal recipients through their corporate directory, they rarely possess credentials for external recipients and the process of sending the encrypted e-mail is stopped dead in its tracks. As seen in the following image, this user has attempted to send an encrypted message but has encountered a problem.

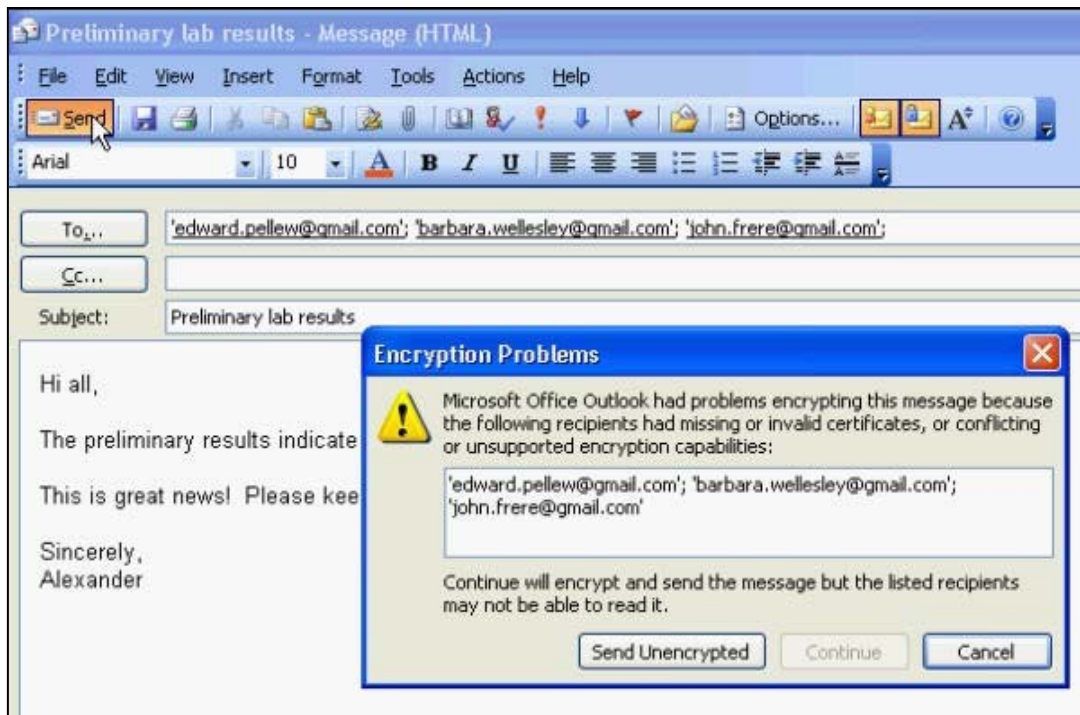


Figure 2: Microsoft Outlook warning message

As noted in the image above, the message cannot be sent because the sender does not possess certificates (i.e., public credentials) for the intended recipients. When a user encounters such warning messages, they must now manage the manual process of contacting the recipients — either through a separate, unsecured e-mail or through a phone call, etc. — to request the required credentials. While frustrating and often confusing for senders, the business process stops and productivity is compromised. Senders may have to wait several hours — or perhaps even several days — until they receive each recipient's certificates. In fact, there is the real possibility that the intended recipients do not even possess encryption credentials, making it impossible to send the message securely.

While some users may have the discipline to acquire recipient certificates and send the encrypted e-mail at a later date, others, in their frustration and need to keep business moving, may choose to reverse their decision to encrypt the message and send the sensitive information in clear-text format.

The result? At best productivity and communications are slowed down; at worst, your organization may knowingly be violating regulatory legislation by compromising corporate or client information and risk severe financial loss and public trust.

Users who have deployed Entrust desktop software such as EDS or the ESP for Outlook feature on their PC can use EMS to act as an “encryption assistant.” EMS operates on the sender’s behalf to automatically execute all steps involved in delivering an encrypted e-mail to an external recipient.

Once EMS is deployed in the organization, users select the “encrypt for EMS” feature on their device; from that point forward, sending encrypted e-mails is seamless. Users simply create e-mail messages as they normally do and select the “encrypt” button. The e-mail message will be encrypted and sent to EMS, which then executes a number of tasks to get the message securely delivered to all recipients.

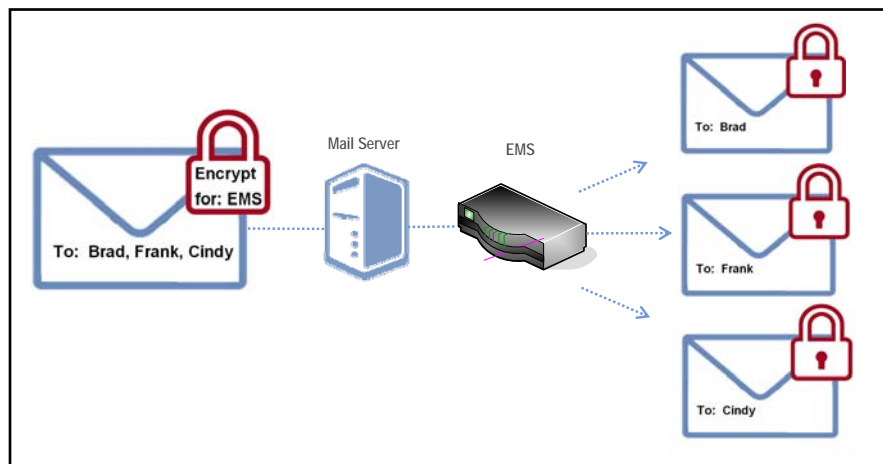


Figure 3: An encrypted message sent to three recipients via EMS

Once received, EMS first attempts to harvest encryption credentials from all the intended recipients. In a case where recipients do not have credentials, EMS automatically sets up secure message delivery capabilities to ensure all recipients can receive the encrypted message. Once credentials are in place, EMS encrypts the message for the various recipients according to their individual encryption capabilities and delivers the message securely. The result is that encryption has been dramatically simplified for the desktop encryption users using a centralized e-mail encryption gateway that automates and logs all encryption activity.

4.2 Sending Encrypted Messages Offline

Mobile users frequently encounter situations when they are not connected to the network, such as when they are on an airplane or in vicinities where network coverage does not exist. One of the primary benefits of mobile computing, however, is to be able to execute basic tasks such as creating e-mails in offline mode and having them automatically delivered when a network connection is re-established.

Sending encrypted e-mail can be difficult to use when offline because the sender's e-mail application must have all the recipient credentials stored in the local address book. If certificates are not available, the e-mail cannot be sent and the user is forced to wait until they are connected to the network to retrieve certificates, or will often take the path of least resistance and revert to unencrypted e-mail.

Unfortunately, in order to avoid the dialog box warnings, this often encourages the sender to stop using encryption in the future. With the EMS credential stored on the local address book, offline users simply compose the e-mail, encrypt the message for EMS and send it to the "outbox." When the user re-connects to the network, all the messages in their "outbox" — both clear-text and encrypted — are transmitted through the network. Encrypted messages are intercepted by the EMS server, which, in turn, proceeds with the certificate lookups, encryption and message delivery to all recipients as outlined in the previous section.

4.3 Offloading Message Encryption

Another consideration of encrypting e-mail locally on the client is the processing required to actually encrypt the message. Encrypting an e-mail involves running the text and associated attachments through a specific process that uses the recipient's public key to cipher (i.e., encrypt) the message.

Consider a use case where a new e-mail message contains attachments and is addressed to a number of recipients. Since the encryption process for the message must be cycled for each individual recipient and takes longer based on message size, the message encryption process can introduce significant delay in completing the sending process. This delay can lead to user frustration and potentially cause them to avoid encryption in the future. With EMS, a high-speed e-mail encryption experience is introduced as the message is encrypted only for EMS, which, in turn, handles all encryption for the entire list of recipients, thereby offloading this process for the client.

In the end, with EMS deployed, secure e-mail becomes simple for users and allows them to communicate securely with virtually anyone, from anywhere — all while protecting sensitive data. The following table summarizes the various tasks that EMS can execute on behalf of the sender to dramatically simplify the e-mail encryption experience.

Function	Description
Determine Delivery Type	EMS will verify if the recipient is currently in the directory and, if so, will send the message in the preferred delivery method. EMS also can be programmed to enforce a delivery type based on customizable policies.
Harvest Existing Recipient Credentials	EMS will notify new recipients (i.e., not listed in the EMS directory) that a secure e-mail is waiting for them and will request their S/MIME or OpenPGP credentials.
Store Recipient Credentials for Shared Use	Once EMS receives a user's credentials, it will store them in a local directory and make use of them for all future outgoing encrypted e-mail from any user within the organization.
Set Up Encryption Capabilities for Recipients without Encryption in Place	For recipients who do not have credentials, EMS can automatically generate an S/MIME certificate or set up secure delivery via Web mail pull or Web mail push. ²
Encrypt and Deliver Messages to Recipients	EMS will handle the encryption process using the recipient's credentials and send the e-mail on for delivery.
Notify Sender of Delivery Issues	EMS will notify the sender, based on system configured parameters, when e-mails are not delivered to end-users.
Logging of Encryption	EMS logs all encryption activity providing corporate administrators with a centralized, auditable and enforceable encryption system

5 Virus- and Content-Scanning Encrypted E-mail

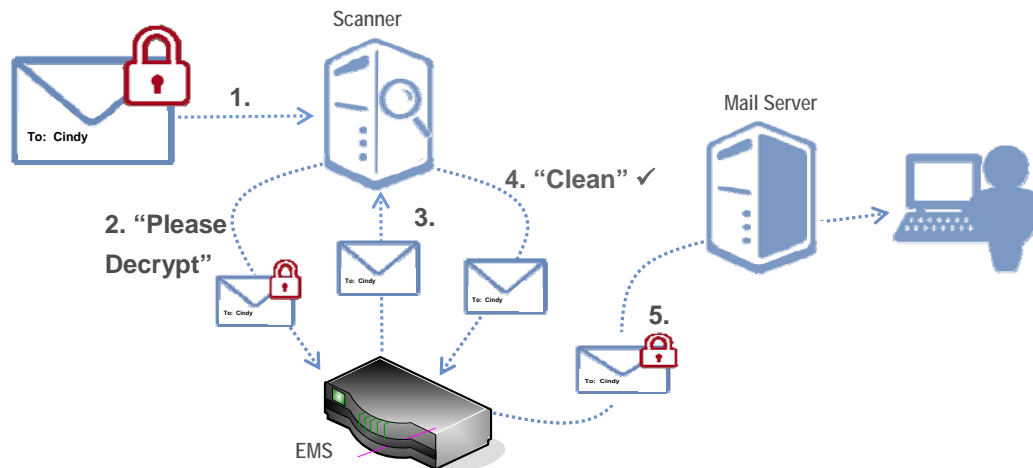
In addition to end-user considerations, organizations must also consider the impact that encryption may have on their existing e-mail security processes, such as virus- and content-scanning. The challenge manifests itself in that encrypted data is unreadable; to both man and machine, an encrypted message is nothing but a series of random characters. To that end, scanning applications that look for pre-defined message content such as word, numbers or virus patterns, or even file types would never detect a “match” within an encrypted message.

Without the ability to scan encrypted e-mails, organizations cannot identify and block viruses, malicious code or perhaps sensitive information that may be contained in e-mails. Content-scanning is a fundamental element of e-mail processing with organizations and, unfortunately, client-based e-mail encryption negates the ability for this process to occur ... or does it?

² For a complete description of Web mail pull and Web mail push, please see the Entrust “Secure E-mail Tutorial” at <http://www.entrust.com/entelligence/tutorial.htm>.

As described in the preceding section, desktop encryption users with EDS or ESP can be configured to have encrypted e-mail processed by EMS. One of the capabilities of EMS is the support of “Plain Text Content Scanning.” This feature provides tight integration with scanning applications by temporarily decrypting e-mail messages to allow scanning of the message prior to re-encrypting and sending them to their final destination.

In the following diagram, we see how an outgoing encrypted message can be processed effectively by the scanner while maintaining the security of the e-mail message.



Step 1: The process begins when an outbound encrypted message arrives at the content scanner

Step 2: The content scanner identifies that the message is encrypted and, based on predefined routing rules, forwards³ encrypted message to EMS for decryption

Step 3: EMS decrypts the message and forwards it to the content scanner for analysis

Step 4: Once the message is appropriately scanned — assuming the message is “clean” and no policy violations have occurred — the content scanner forwards the message back to EMS

Step 5: At this point, the message is then re-encrypted by EMS and sent to the intended recipient(s)

With the ability to now deploy e-mail encryption alongside content-scanning, IT managers, security officers and compliance personnel no longer have to choose between encryption or virus-scanning, but can safeguard communication against the multitude of security threats that exist today.

³ The connection between the EMS server and the content scanner can be encrypted with SSL if desired.

6 Summary

As organizations expand their electronic communications with external parties, concerns about keeping information sent to and from the organization confidential will become an increasing priority. While securing the information itself is a key priority, ensuring the process is simple for internal users and external recipients is equally important.

Deploying an e-mail encryption appliance such as the Entrust Entelligence Messaging Server cannot only help make e-mail encryption easy for all users, but also provides organizational managers with the capability of deploying a centralized e-mail encryption solution and will help ensure information security policies are automatically enforced and auditable.

7 About Entrust

Entrust [NASDAQ: ENTU] secures digital identities and information for consumers, enterprises and governments in 1,700 organizations spanning 60 countries. Leveraging a layered security approach to address growing risks, Entrust solutions help secure the most common digital identity and information protection pain points in an organization. These include SSL, authentication, fraud detection, shared data protection and e-mail security. For information, call 888-690-2424, e-mail entrust@entrust.com or visit www.entrust.com.