Entrust® Securing Digital Identities & Information

Securing Your Digital Life

Looking Beyond the Boundary:

Simplifying Secure Email with Partners, Customers, and Suppliers

February 2005

Entrust
Securing Digital Identities & Information

TABLE OF CONTENTS

Entrust®
Securing Digital Identities & Information

Executive Summary

Working environments have come to depend on quick, reliable and efficient communication methods between employees, customers and partners. With the advent of the Internet, business critical communication mechanisms have grown from traditional phone and fax systems to include email, Web (http), file transfer (ftp) and instant messaging approaches. These new communication mechanisms have made it easier for companies to reach more customers, faster, and expand into new markets. However, enterprises and governments must balance the need to extend deeper access to stakeholders with the need to protect information assets and comply with regulations pertaining to privacy and governance, all while addressing investor expectations for cost control and Return On Investment (ROI).

Email is the dominant method for Internet-based communication. Originally, email was an efficient tool for internal corporate communications, but its ubiquity and low cost has transformed it into a critical tool for communicating externally, with customers and partners. The result is that email is now considered a core component of an organization's mission-critical infrastructure for corporate communication. The importance of email has also begun to raise concerns about its security. As companies begin to use email for more sensitive and higher value transactions with customers and partners, secured email is becoming an important corporate IT issue.

The goal of this white paper is to discuss the decisions corporate IT departments are required to make when adding security to their email infrastructures. It investigates the different requirements for sending secured email to employees, customers and partners and presents some potential solution options. Finally, the white paper discusses the Entrust Entelligence™ Messaging Server (hereto also referred to as Messaging Server), which is part of the broader Entrust® Secure Messaging Solution. Messaging Server builds upon Entrust's existing messaging solution suite, but addresses the requirements of securing email for communication with a wider range of customers, partners and employees.

Entrust
Securing Digital Identities & Information

Why Do We Need to Secure Email?

The benefits of basic email communication are numerous and widely recognized. However, secured email can provide additional benefits by helping to allow organizations to move more sensitive and higher value transactions online. Messages that were previously limited to more traditional methods of communication due to concerns about information security—such as the concern that email can be intercepted or read by unintended audiences—can now be moved online with a similar level of assurance of confidentiality and data integrity as that which exists in the paper world. Many people have a false sense of security with respect to email, based largely on the feeling of anonymity provided by the Internet and the sheer volume of data flowing through it. Due to this false sense of security, individuals within organizations are already exchanging sensitive information online, but at what cost?

In order to mitigate risk while helping to enable new and higher sensitive communications online, security and trust are essential. Unauthorized access to client records, sales forecasts, intellectual property or other valuable information can do significant damage to an organization's brand and competitive position. And—with recent government regulations, the need to secure email communications becomes an important element of regulatory compliance.

The ability to add strong identification, privacy and verification to email solutions can provide organizations with a competitive advantage by helping to enable new business processes, protect and build a company's brand equity, and strengthen relationships with its suppliers, partners and customers—all while helping to contribute to good internal controls and compliance with government regulations surrounding the protection of information privacy.

Protection of Brand

Examples abound of private and public organizations whose brand and reputation has been tarnished by the exposure, real or potential, of sensitive information contained in unsecured email on stolen or lost employee laptops - credit card databases, military secrets, intellectual property, government plans.

Corporate Governance

With the current focus on corporate governance, notably in Sarbanes-Oxley Section 404, organizations must consider secure email as a means to address internal controls for data access and data integrity. Email encryption and digital signatures can be employed to avoid security breaches and to provide transaction integrity.

Risk Mitigation and Compliance

Heightened regulatory requirements are forcing businesses and governments to better protect communications containing confidential information. A global awareness about privacy issues has resulted in numerous privacy-related regulations such as HIPAA, Gramm-Leach-Bliley, and California SB-1386 in the US, PIPEDA in Canada, and the European Data Directives. Several of these specifically refer to the need for email encryption as a means to protect the privacy of customers and some prescribe regulatory penalties for non-compliance.

As the risks of doing business online become well understood through numerous publicized breaches, emphasis must be placed on mitigating those risks through tighter security practices and procedures. Encryption and digital signatures significantly reduce the risks of exposure or tampering with sensitive information as it is exchanged or stored in email systems.

> ***"During the next four years, e-mail will increasingly be treated as a mission-critical business communication system, with emphasis on uptime, tuning, hygiene, and security."***
>
> *Source: META Group "E-Mail Concerns in 2007", Matt Cain, June 5, 2003*

In addition to these factors, a number of other key drivers are encouraging organizations to deploy secure email solutions:

Time-to-market and cost pressures are forcing organizations to use email-based solutions to

replace more expensive communication methods such as courier, long distance telephone and fax typically used for sensitive and high-value communications.

Competitive pressures are forcing organizations to accelerate business processes through the rapid exchange of sensitive and/or high-value information.

Market pressures are rewarding organizations with tight supply chain relationships that are being enabled with secure email based collaboration.

Public concern over the privacy issue is mandating protection of the organization's brand equity by protecting sensitive customer information and taking measures to prevent the loss or compromise of sensitive data.

Types of Secure Messaging Environments

Generally speaking, messaging environments can be broadly classified by the nature of the exchange:

Communication between Employees
Communication with Partners
Communication with Customers or Citizens

Each of these environments has its own unique characteristics that govern its requirements. Typically, organizations need to provide security in one or more of these environments, which defines the type of solution they need and the types of compromises they are forced to make with existing solutions.

Communication Between Employees

Email generated in day-to-day communication between employees within an enterprise constitutes the vast majority of communications. These environments are relatively homogeneous and are usually based on a single email infrastructure, such as Microsoft® Exchange® or Lotus® Notes™, although many companies must manage multiple messaging platforms as a result of consolidation, mergers, or acquisitions. The requirement for security is often departmentalized in areas such as Legal, R&D, HR and Finance, or at the Senior Management level, where sensitive information is exchanged frequently.

Some of the key characteristics of an enterprise-messaging environment are:

- The majority of email is exchanged within the enterprise;
- Email is a primary tool for collaboration;
- Employees often have to work off-line with email;
- Email reach within the enterprise is expanding to the mobile workforce through the use of email-enabled wireless devices; and
- Security is provided as an extension to the existing email infrastructure—usually via Secure Multipurpose Internet Mail Extensions (S/MIME).

Communication With Partners

Inter-organizational email is growing rapidly as organizations exploit the business advantages of closer relationships with their customers, partners and suppliers. In this type of exchange, we are more likely to encounter a heterogeneous environment where organizations are communicating between two interoperable, yet different email infrastructures. Typically these environments can be characterized by the following:

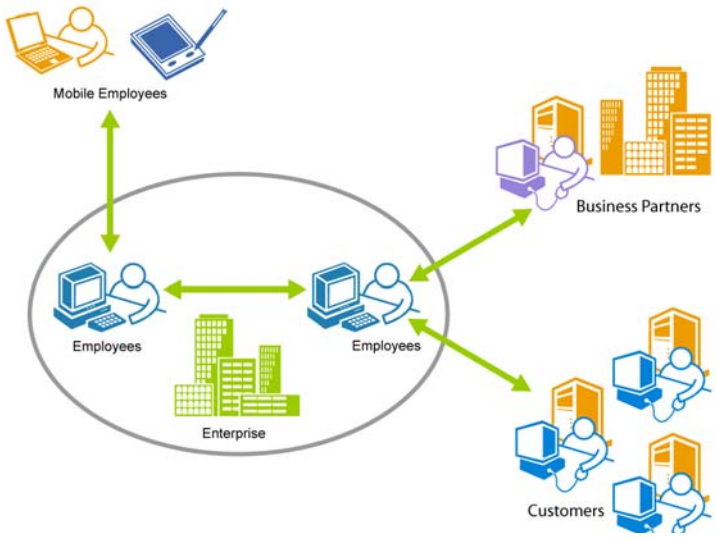

Figure 1: Types of Secure Messaging Environments

- Information exchanges tend to be collaborative and flow both ways;
- Both parties have a vested interest in securing the information;
- The partner has an existing email environment that they expect to utilize during the collaboration;
- Communications are between individuals collaborating to accomplish a specific goal; and
- Security is dictated by standards-based protocols that are mutually supported by each organization's email infrastructure (primarily S/MIME).

Examples of this type of information exchange are wide-ranging, covering service engagements ranging from financial auditing, legal counseling and management consulting to more cooperative ventures like joint design and development, organizational mergers, or inter-governmental collaboration on horizontal policy initiatives.

Communication With Customers or Citizens

Email environments where businesses or government are communicating with their customers and citizens exhibit yet another set of characteristics. In this environment, the technology used for communication is fragmented, with the lowest common denominator being a Web browser. From a secured messaging perspective, this environment is further characterized by:

- Secured email flow is often one-way, such as electronic statements being pushed out via email from the organization to the individual;
- The onus for security is placed primarily on the organization, as it is acting as a caretaker of confidential client information;
- The communication is between the organization and the individual (not individual to individual); and
- Security is governed by the lowest common denominator—generally Secure Sockets Layer (SSL) / Transport Layer Security (TLS)—protected Web mail.

Striking a Balance: Risk Mitigation vs. Productivity

Regardless of the type of messaging environment, for email to succeed as a medium of communication for sensitive or valuable information, it must be able to provide security capabilities that are comparable to those provided in the physical world. However, security features by themselves are not enough. While a Compliance Officer or Chief Security Officer (CSO) may naturally be concerned with mitigating exposure to regulatory non-compliance and mitigating risks, they must also take into careful consideration productivity of the organization. To remain successful, security must be easy-to-use and interoperable so that users do not have to change the way they work to securely collaborate and exchange information.

Ease of Use and Administration

Ease-of-use poses a significant potential barrier to securing email. If security cannot be applied easily and transparently for end users, they will most likely circumvent the policy. From the user's perspective, ease-of-use can be simply defined as requiring no more effort to send a secured email than is required to send a regular email, other than the desire to do so in a secure manner. From an organizational perspective, ease-of-use has a different meaning. A secured email solution should be easy to configure and deploy, and support mobile workers, where off-line use and limited bandwidth connections are common. When considering the external parties that an organization is dealing with, a secure email solution should not require customers or partners to install new software, change a customer's or partner's email behavior or defeat or interfere with their security systems (such as content and virus scanning) or their ability to delegate to co-workers, the right to read and respond to emails. Users should be able to establish secure communications with recipients without requiring administrator intervention.

Interoperability

One major challenge for a secured email is interoperability. If the security provided by one infrastructure or email client is not interoperable with another email client or infrastructure, secured messages cannot be exchanged. This can either

pose a barrier to collaboration or, even worse, drive users to exchange information without security.

Although it is more straightforward to achieve interoperability within an organization where there is some level of control over the types of systems deployed to users' desktops, the same cannot be said when communicating with your customers or business partners. Reaching consensus among supply chain partners on a non-standards-based security scheme can be extremely difficult. Using a non-standard approach often locks all participants into a particular vendor and limits ongoing flexibility. When analyzing the market acceptance of security protocols, research indicates that no single lowest common denominator exists for all types of messaging environments. When communicating between organizations, S/MIME seems to be the preferred protocol, whereas SSL seems to be the most widely accepted approach when communicating with individual customers or citizens. Unless you are willing and able to insist that your customers and partners switch to an email solution that supports your chosen standard, or change their email behavior, finding a single interoperable delivery mechanism can be a challenge. Solutions should support flexible, alternative delivery methods.

Requirements based on Messaging Environment

While the types of challenges facing secured email can be easily categorized, key requirements are significantly different depending on the type of messaging environment.

REQUIREMENTS	ENTERPRISE	INTER-ORGANIZATIONAL	CUSTOMER/CITIZEN
Types of Security	• Strong identification of sender and recipients (hierarchical trust) • Ability to entitle delegates with the ability to read and respond to email • Individual selected message signature and verification • Individual selected message privacy	• Peer to peer identification of sender and recipients (associative trust) • Ability to entitle delegate applications (ie. content scanner) to process email • Individual selected message signature and verification • Policy-based privacy enforcement	• Strong identification of sender through public root of trust (third-party trust) • Organization based message signature or receipt • Protection of recipient's privacy
Ease of Use	• Integrated with common security infrastructure • Support for mobile workforce (i.e. Off-line use, bandwidth constrained connections) • Security functionality easy and virtually transparent to end user	• No requirement for partner to deploy new software • No change in partner's email behavior	• No requirement for software to be deployed • No change in recipients email behavior
Interoperability	• Support for email enabled devices (ie. PDAs and smartphones)	• Support for a common message security protocol (S/MIME)	• Support for a common communication protocol (SSL)

Your Choices for Securing Email

Based on your internal security requirements and the messaging environments of your target recipients, there are several potential scenarios for enabling secure communications. The diagram below breaks these scenarios down based on where encryption and decryption occurs—whether at the desktop or at the boundary.

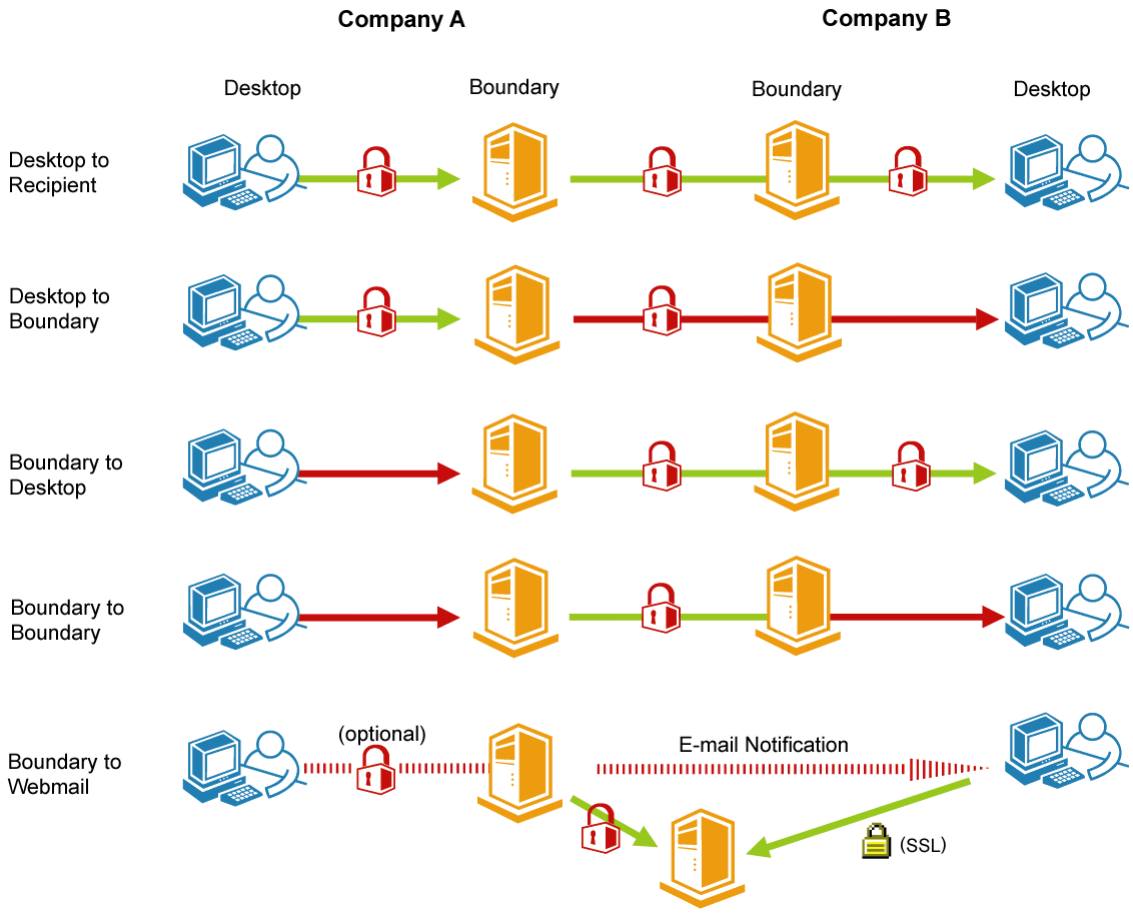

Figure 2: Choices for Securing Email

Desktop Solutions

Desktop-to-desktop secured email is widely recognized as being the most secure method of electronic communication. Email exchanged in this manner can be encrypted and/or signed at the sender's desktop and remain that way throughout its journey to the recipient's desktop where it can continue to remain encrypted. Desktop-to-boundary type solutions are required when the recipient's organization has not deployed or does not allow encryption to the desktop. Generally this is not the case, but is being encountered more and more, where organizations are weighing trade-offs between email security and the need for boundary services such as virus protection and content scanning.

These types of solutions can be deployed using either of the following:

Native S/MIME capabilities found in off-the-shelf email clients, or an **email plug-in** with enhanced security functionality and typically designed to work with a specific security implementation such as Public Key Infrastructure (PKI), or **S/MIME capable email gateways,** in the case of external boundary-based solutions.

Native Email Clients

Although this is the least difficult desktop solution to deploy, native email client solutions generally suffer from a lack of enhanced security features as well as relying heavily on the user to understand how the security works. Specifically, these types of solutions generally suffer from:

- No key update;
- No key recovery;
- No maintenance of key histories;
- No Certificate Revocation List (CRL) checks; and
- No centralized management.

In order to for this type of deployment to be successful, each user requires a significant amount of understanding to be successful. Generally speaking, this type of solution would only be recommended for small groups of knowledgeable users or individual point solutions.

Security Plug-ins

Unlike native email client capabilities, security plug-ins are typically designed to work with a specific security infrastructure and remove much of the burden placed on the individual user, making plug-ins virtually ideal for enterprise deployments. Factors that make these types of solutions less than ideal are:

- They suffer from the same deployment problems of any desktop client software;
- Some vendors have used proprietary security schemes instead of S/MIME or SSL;
- Unless the certificates for all possible recipients are automatically cached locally, off-line secured usage will require a change in user behavior; and
- Certain security operations, such as encrypting for a large recipient list, can add significant size to an email and impair performance when working over a low-bandwidth connection.

In summary, clients and plug-ins have several challenges. Both require some degree of end user knowledge when managing and conducting secured communications with external parties. Another challenge involves the task of associating boundary-type certificates with multiple external recipient emails—advanced features that alert senders when the email address found in the certificate is not the same as that of the recipient—as well as manually associating a single certificate with multiple people. Lastly, not all email systems support S/MIME. Web messaging services such as Hotmail are primary examples.

Boundary Solutions

Boundary-based solutions are generally found in organizations that are reluctant to deploy desktop security or have had to manage trade-offs between email security and the need for virus protection and content scanning capabilities. These types of solutions are generally deployed with hardware (appliance) or software solutions installed at the boundary of an organization. In their simplest form, they are used to encrypt all outgoing and decrypt

any incoming emails based on straightforward sets of rules. More elaborate solutions offer policy-based configurations that allow the system to encrypt and sign an email on a sender's behalf as well as decrypt and verify incoming messages. The boundary approach has the advantage of enabling easier deployment relative to desktop-based solutions, and providing policy-based security vs. individual-decided security.

Boundary-based solutions do, however have some disadvantages: A lower level of privacy, as the email message is not secured until it reaches the organization's boundary—a critical issue since 60-80% of all security breaches are internal— and loss of strong sender identification and verification, as the sender (message creator) is not actually signing the message. Some boundary-based solutions may also suffer from an inability to deliver secured email to recipients who don't have S/MIME-interoperable clients.

Web Mail Solutions

Instead of using S/MIME, Web mail systems use SSL/TLS-based protocols in the delivery of secured messages. There are two primary models for secure web mail delivery—pull and push.

Pull Models

Within pull models, a notification message along with a URL is sent to the recipient to ***pull*** the user back to a portal where a secure 'inbox' is displayed. The recipient can then view the secured message using a common browser authenticated via a SSL/TLS session. Solutions using this approach should integrate well with an organization's existing web portal and authentication systems. Capabilities and requirements will vary among vendors, such as those for securing attachments, replying securely, using desktop clients, etc.

Push Models

Within push models, a secured message is delivered i.e., ***pushed***, as an attachment along with executable code to decrypt and display the message in the recipient's Web browser. Decryption keys are managed by the sending organization and delivered through an authenticated SSL connection.

Web mail-based security implementations have the benefit of providing a solution with the lowest common denominator in terms of system requirements for an external recipient. For this reason, these solutions are a recommended approach for ad hoc messaging and certain types of messaging applications such as consumer-based statement delivery. Customers considering this approach should take into account certain trade-offs inherent to Web mail-based delivery, including:

- Users are asked to change their email behavior since the message is not displayed in their normal mail client;
- Offline usage is not possible with the pull model;
- Secured mail messages, or the corresponding keys, must be stored on a server for a period of time; and
- User ID and password authentication of the SSL session does not provide the same level of enhanced identification that is provided by digital certificates.

Entrust® Secure Messaging Solution: A New Approach

Entrust has been a leading provider of secured email solutions for the last five years. Companies have successfully deployed Entrust Entelligence™ Email Plug-in to send secured email text and attachments within their organizations and with partner organizations. As companies expand their email usage to integrate more transactions with customers and business partners outside their corporate boundaries, Entrust is enhancing its approach to securing email for the extended enterprise. Entrust's next generation email solution is called the Entrust Entelligence™ Messaging Server. The Entrust Entelligence Messaging Server will address many of the issues and requirements of sending secured email to employees and business partners. It is based on a new server component that offloads much of the complexity of secure email from the desktop to a central server. The Messaging Server architecture provides flexible secure delivery methods, is based on open standards, and supports boundary services such as anti-virus and content scanning. It will continue to work with a much simpler desktop client while also reducing the complexity of sending secured email, making the process seemingly transparent to partners and employees.

The Role of Entrust Entelligence Messaging Server

A key component of the Entrust Secure Messaging Solution is the **Entrust Entelligence Messaging Server**, which is a centralized server for offloading much of the processing typically done by desktop clients, improving performance in both Microsoft Exchange/Outlook and IBM Lotus Domino/Notes environments. Messaging Server streamlines and automates many of the tasks necessary for sending secured email, such as management of digital certificates containing users' security credentials that are used for encryption, and management of secure delivery.

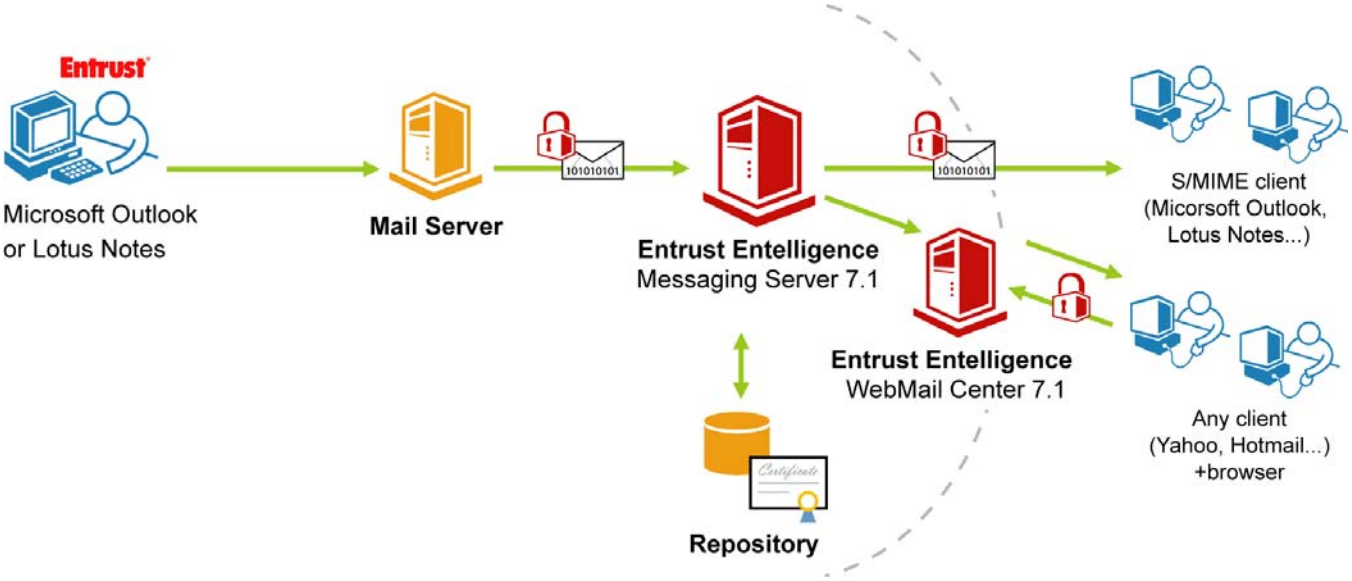

Figure 3: Entrust Entelligence Messaging Server

Sending an Email

The operation of the system is simple and transparent to the email user. Users sending secured messages need only create the email as they normally would, and indicate that it should be secured. As an example, the following describes what happens behind the scenes as the Entrust Entelligence™ Email Plug-in for Microsoft Outlook sends the message to Messaging Server:

- Package the recipient list;
- Perform any specified security operations like message encryption and digital signature;
- Re-address and encrypt the message for the Messaging Server; and
- Send the message as it would normally.

Upon receipt of the secured message, Messaging Server will:

- Unpackage the recipient list and re-address the message to the original recipient list;
- Look up and validate encryption certificate information for the recipients as required;
- Re-encrypt the symmetric key for all of the recipients and any known users or applications that have been entitled to decrypt the message (e.g.anti-virus scanners); and
- Deliver the message to recipients using their preferred secure delivery method.

Although the process is very simple, it provides some major benefits:

- Security is provided all the way to the user's desktop and is transparent to the user since the server is handling the complex operations;
- Employees working off-line can utilize security functions without the need to manually cache certificates for all possible recipients—messages are also encrypted on the laptop, further enhancing security; and
- Fewer operations are performed at the desktop, resulting in smaller messages and faster processing.

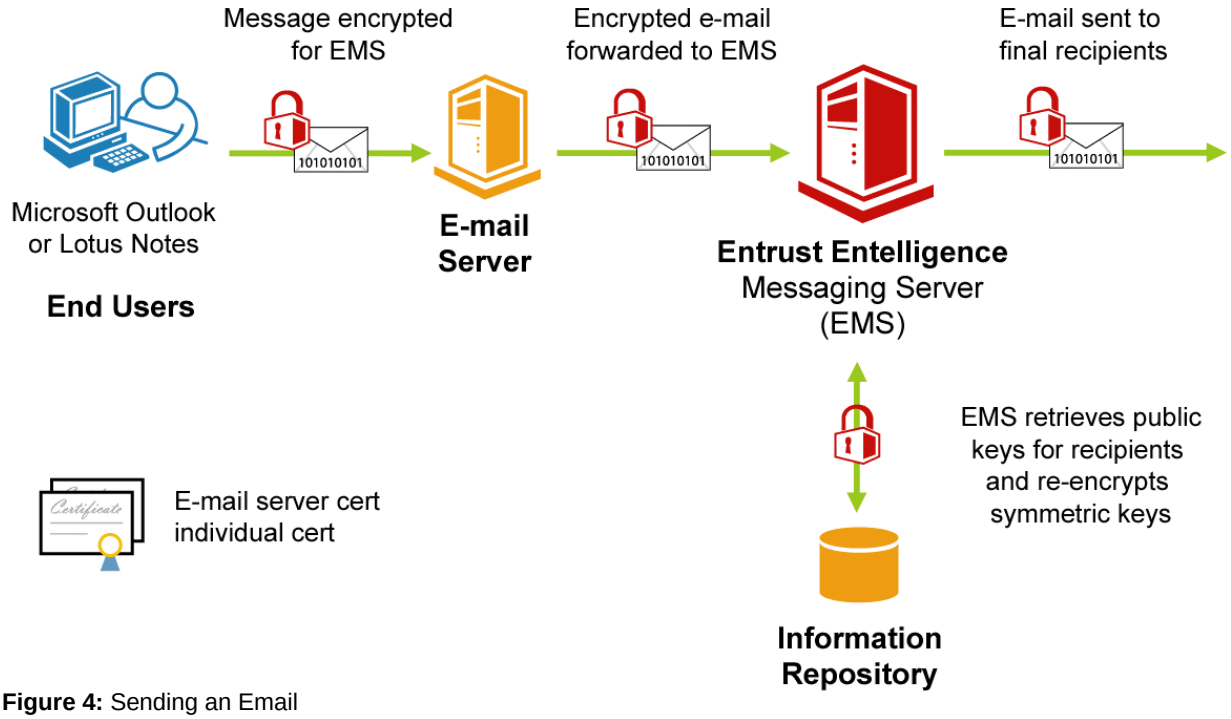

Figure 4: Sending an Email

Communicating Securely with External Parties

The Entrust Entelligence Messaging Server provides improved capabilities when sending secured email externally. For instance, if a certificate is not found for a recipient, the Messaging Server can take responsibility for queuing the message while it initiates a request for a recipient's (usually external) certificate, and will send the message once that certificate is received. Messaging Server also makes trust decisions on any certificate it receives, based on a number of configurable options, including the involvement of an administrator or the message sender. With this type of capability, what was once a manual operation requiring a user to perform key exchanges with everyone with whom they wish to securely communicate outside their organization, is now automated by Messaging Server.

Managing Digital Identities

The Entrust Entelligence Messaging Server manages digital identities for internal and external recipients as messages flow through the server. Once a digital identity, in the form of a digital certificate, is received for an external recipient, the Messaging Server makes that certificate available for all internal users as required.

Another form of digital identity management performed by the Messaging Server is referred to as 'Proxy Certificates'. In the example of the Messaging Server's support for Lotus Notes, a Proxy Certificate is created and mapped to the Notes ID of internal users. This enables inbound and outbound translation between the internal Notes security format and the Internet standard S/MIME or SSL secure delivery methods. This simplifies secure communications with external recipients without changing the Notes user's behavior.

The Value of Entrust Entelligence Messaging Server

Organizations can expand their electronic communication capabilities using end-to-end enhanced security to help allow more high-value, paper-based communications to be moved online. Traditionally, many highly sensitive paper-based communications could not be moved online due to confidentiality, and the need for integrity and verification. As mentioned in the introduction section of this white paper, the Entrust Entelligence Messaging Server builds upon Entrust's existing messaging offering—the Entrust Secure Messaging Solution. The Entrust Entelligence Messaging Server provides support for message privacy, integrity and sender identification. These capabilities can help allow organizations to have the confidence to implement more trusted electronic communications. Messaging Server also has capabilities that can be used for securing email to a wider range of customers, partners and employees. The following are some of the benefits of utilizing the Entrust Entelligence Messaging Server within your organization.

Reduce Costs

Messaging Server can help organizations to reduce costs associated with costly manual-intensive, error prone, paper-based processes. By accelerating business processes with secured online communications, it is possible to work more efficiently with business partners and geographically distributed co-workers. End-to-end enhanced security allows more business processes to be moved online, and can help to save users and organizations both in terms of time and resources. One of the ways organizations can become more "market agile" is to cut the time and costs of conducting contract negotiations with business partners. Using secured email with digital signatures can be more cost-effective way to do this as compared to expensive and time-consuming courier, registered mail or fax options.

Improve Productivity and Accessibility

Messaging Server can help organizations to reduce costs associated with manual-intensive, error-prone, paper-based processes. By accelerating business processes with secured online communications, it is possible to work more efficiently with business partners and geographically distributed co-workers. End-to-end enhanced security allows more business processes to be moved online, and can help to save users and organizations both time and resources.

Improve Ease of Use

Employees, customers or partners do not have to change the way they currently work or the messaging environment they are using in order to enhance their messaging security. The comprehensive Messaging Server is easy-to-use, configurable and interoperable with a range of messaging solutions. In addition, its flexibility allows it to be combined with Entrust Ready solutions to

add additional capabilities for a secured environment such as content or virus scanning.

Extend Security Beyond the Organization

Automatic certificate management can help enable organizations to extend high-value secured communications beyond their traditional boundaries. Business partners and customers who do not yet have a digital ID required for secured email are directed to a certificate service, where they can obtain a digital ID, or they can use the Entrust Entelligence™ WebMail Center. This further extends secured email communication from B2E into B2B and B2C environments, helping to improve the benefits associated with an investment made in a secure email solution.

Entrust Secure Messaging Solution Components

Entrust Entelligence™ Messaging Server

Secures communications with the extended enterprise via a central email gateway. Handles much of the complexity of key management and secure delivery for external mail recipients. Seamlessly integrates with applications including Microsoft Exchange/Outlook and Lotus Notes.

Entrust Entelligence™ WebMail Center

Adds alternative secure Web-based delivery method for external recipients, who only need a web browser to access, read and reply to secure emails. Offered as an optional extension to Entrust Entelligence Messaging Server.

Entrust Entelligence™ Email Plug-in for Outlook

Enables users to encrypt and digitally sign messages via an easy-to-use plug-in for Microsoft Outlook that integrates with Entrust Entelligence™ Desktop Manager.

Entrust Entelligence™ Security Provider

Delivers managed Entrust digital IDs across applications via thin-client enterprise desktop security software. Can be used in conjunction with Microsoft Outlook's native S/MIME email encryption capabilities.

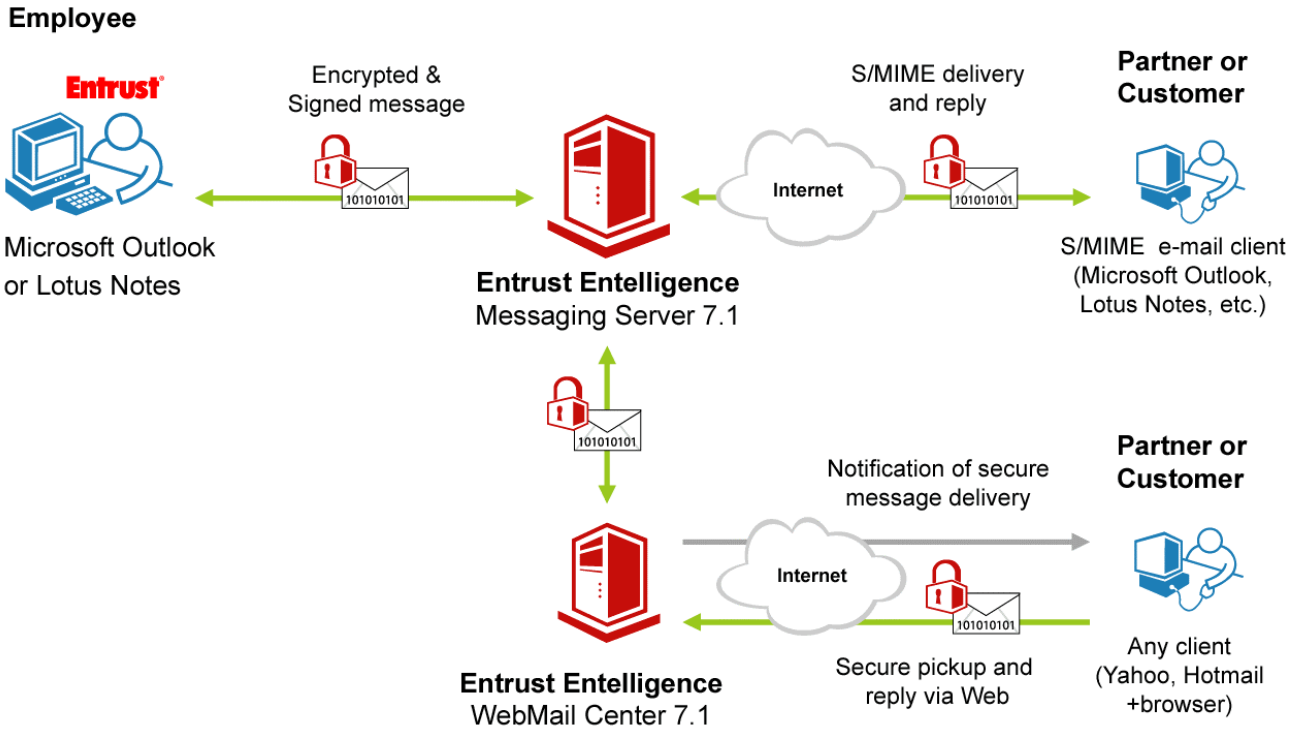

Figure 5: Entrust Secure Messaging Solution Architecture

Benefits of Entrust Secure Messaging Solution

The Entrust Secure Messaging Solution delivers the ability to encrypt and digitally sign important communications, including attachments, so that only recipients with the necessary decryption keys can access the message, both in transit and at its final destination(s). The Entrust Secure Messaging Solution can help turn popular email software programs into secure, reliable communication vehicles. Entrust's enhanced security services, built on encryption and digital signature technology, allow an organization and its employees to help:

- Identify the sender and recipient of email communications using digital IDs;
- Keep message contents confidential through encryption;
- Verify whether the contents of a message have been changed; and
- Scan the contents of encrypted messages without compromising security.

Because the Entrust Secure Messaging Solution is centrally managed, organizations can:

- Enforce certain email rules or policies throughout the user base;
- Issue and maintain the digital IDs needed for identification of email users, in a way that is not onerous on the IT team or the users themselves; and
- Leverage the same technology to help secure other processes that the organization commonly uses, if desired.

Reduce Costs

The Entrust Secure Messaging Solution works with a range of messaging environments and can be extended for use with customers and partners. This capability can enhance the security of an organization's communications and transactions while helping to reduce the costs of doing business. The Entrust Secure Messaging Solution's flexibility and interoperability allow organizations to add other critical security capabilities such as virus and content scanning solutions, which can help to reduce downtime costs resulting from outbreaks and inappropriate use of IT assets.

Accelerate Time-to-Market

The Entrust Secure Messaging Solution can help strengthen and grow business relationships by enabling secured communications and transactions that are more verifiable, identifiable and confidential, helping to enable business counterparts to share and collaborate more quickly and easily. Not only can this help allow for stronger relationships, but it can also help to build and protect company brand equity with quicker response times, automated processes and more protected and verifiable communications.

Scale Security Capabilities from Today, into Tomorrow

The Entrust Secure Messaging Solution can help reduce an organization's total cost of ownership by offering a comprehensive security solution that can be used to solve the needs of today or be extended across the enterprise to provide security solutions across a range of applications and devices. Organizations can install the Entrust Secure Messaging Solution today to secure email communications. The Entrust Solution can then be extended tomorrow to provide enhanced security to other messaging environments such as mobile messaging. This security infrastructure can further be leveraged to support other applications such as electronic forms or documents such as Adobe PDFs, Secure Web Portals or Secure VPNs. With a single common infrastructure that provides enhanced security management, the Entrust Secure Messaging Solution provides a low cost security solution that is easy to manage.

Competitive Advantages of Entrust Solutions

In order to help improve the cost and productivity savings associated with email, organizations need to be able to transition highly sensitive communications online. This requires a level of privacy and trust in the electronic world that is comparable to that provided by traditional media such as phone, fax, courier and registered mail.

Ease of Use—Securing Email Becomes Automatic and Transparent

Many competitive security solutions require users to understand and manage their own security. The Entrust Secure Messaging Solution provides automatic security management, a transparent mechanism for users of secure messaging. Some solutions can be so difficult to manage that users end up reverting back to traditional methods of communication. The ease of use associated with Entrust Secure Messaging encourages ongoing utilization of email as a transport vehicle for sensitive communication, which can help improve productivity gains while helping to reduce the risk of loss by users not following security guidelines. Reducing the time spent communicating through traditional channels and moving towards secured email communications can help increase efficiency and productivity.

Unlike competitive solutions that require users to understand and manage their own security, sending a secured email using the Entrust Secure Messaging Solution is no more difficult than sending a regular email. Security is managed transparently and automatically on behalf of the user. This ease of use, coupled with privacy and trust, encourages employees to move away from more expensive forms of communication (registered mail, private courier, etc.) and move towards using faster, less expensive, secured email communication. Broader adoption of security can add up to greater savings.

End-to-End Security

Unlike solutions limited to “boundary-based” security or solutions that simply maintain message encryption during transit, the Entrust Secure Messaging Solution can provide end-to-end encryption that secures messages in transit from desktop to desktop and maintains this encryption for stored messages. This capability is particularly valuable for widely used portable devices that are more prone to loss or theft (i.e. laptop computers). The Entrust Secure Messaging Solution encrypts messages stored on such devices, thereby protecting corporate information at all times.

Flexibility and Interoperability

The secure messaging market has been characterized by a lack of standards and the introduction of non-integrated, patchwork solutions that solve specific messaging issues. This lack of interoperability causes problems with messaging systems and makes it difficult for organizations to communicate with partners and customers. With its strong standards support, Entrust’s flexible and interoperable solution for secure messaging provides enhanced security across a broad range of messaging environments—including widely deployed enterprise email systems such as Microsoft Exchange and Lotus Notes. In addition, the Entrust Secure Messaging Solution interoperates with a variety of third party solutions to enable additional capabilities such as virus and content scanning.

Extensibility

While organizations can use the Entrust Secure Messaging Solution to add security to communications for widely deployed enterprise email systems such as Microsoft Exchange and Lotus Notes, Entrust Secure Messaging Solution is designed with a broader range of usage in mind. Organizations can further extend their security implementations not only to add security to their messaging, but they can use the same infrastructure to support other desktop, Virtual Private Networks (VPNs) and Web applications including e-Forms and Web portals.

Scalability

The Entrust Secure Messaging Solution is a comprehensive offering that can scale quickly and easily as an organization and its business needs grow. In addition to easily adding users and having the support of an automated security management system, additional capabilities can be added for future messaging needs.

For more information on the **Entrust Secure Messaging Solution**, please visit: http://www.entrust.com

The Need to Act Now

Regardless of whether organizations are being driven by competitive pressures, corporate governance and regulatory requirements or an increased need for sharing sensitive information, the added value and lower costs of using secured email are clear. Most organizations trying to satisfy these constantly evolving requirements are searching for security solutions that address more than just the enterprise-messaging environment. The approach used by the Entrust Entelligence Messaging Server meets the security, ease-of-use and interoperability requirements for success in the enterprise and inter-organizational messaging environments. Messaging Server is easy to deploy, transparent to end users, and leverages existing email infrastructures. Organizations can reduce the risk posed by the common practice of exchanging sensitive or valuable information insecurely as well as benefit from the added value and lower cost of moving other types of secured communication processes to email.

About Entrust

Entrust, Inc. [NASDAQ: ENTU] is a world-leader in securing digital identities and information. Over 1,400 enterprises and government agencies in more than 50 countries rely on Entrust solutions to help secure the digital lives of their citizens, customers, employees and partners. Our proven software and services help customers achieve regulatory and corporate compliance, while turning security challenges such as identity theft and email security into business opportunities. For more information on how Entrust can secure your digital life, please visit: **www.entrust.com.**