



Secure Messaging Buyer's Guide

Entrust, Inc.
North America Sales: 1-888-690-2424
entrust@entrust.com

EMEA Sales: +44 (0) 118 953 3000
emea.sales@entrust.com

December 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

Introduction	1
1 Key Considerations When Selecting a Secure E-mail Solution	2
1.1 Usability	2
1.2 Message Delivery Options.....	2
1.3 Standards Support.....	3
1.4 Flexibility of Delivery Options.....	4
1.5 Integration to existing infrastructure	4
1.6 Mobile Solutions Support.....	5
1.7 Platform Architecture	5
1.8 Auditing, Reporting and Administration	5
1.9 Hardened Appliance	6
2 Vendor	7
2.1 Corporate Information	7
2.2 Technical Support.....	7
2.3 Documentation and Training.....	7
2.4 Strategic Partnerships	7
2.5 Services	7

Introduction

This guide has been developed to assist organizations in identifying their requirements for a secure e-mail solution to meet business and security needs. It outlines key questions that should be considered during the selection process to ensure the chosen solution addresses the organization's requirements from business and operational perspectives.

Government and commercial organizations are being challenged to implement cost-effective security solutions that meet the operational needs of their end-users while complying with regulatory requirements. Given this context, a secure e-mail solution should address an organization's need to transparently manage encryption functions and enforce corporate secure e-mail policies, while making it easier to communicate securely with external business partners and customers. It should also enable — not hinder — organizations to develop secure online business processes to reduce cost while improving online services through the addition of security.

To attain these goals, a secure e-mail solution must be a flexible, scalable platform that can simultaneously support a multitude of secure e-mail configurations to meet diverse business needs today and in the future.

This document provides questions and issues to reflect upon during the vendor solution evaluation process, which have been organized into key areas of consideration. These questions have been provided to assist your internal project team to determine what questions need to be asked of a potential vendor. This is not intended to be an exhaustive list. It is meant as a starting place to assist you in your review process.

1 Key Considerations When Selecting a Secure E-mail Solution

1.1 Usability

- 1.1.1 Is the solution simple to use for senders and recipients?
- 1.1.2 Does the solution simultaneously support multiple languages based on the user's localized language settings? For example, when a user with a browser configured for French accesses webmail, is the interface French?
- 1.1.3 Does the solution leverage existing user-desktop encryption software? Does it support existing credentials that internal and external users may already have?
- 1.1.4 Are all certificate management processes automated? Does the solution support:
 - Automatic harvest of certificates for external recipients
 - Automatic generation of credentials for internal users when sending to recipients with differing encryption capabilities
 - Automatic generation of credentials for external users in a variety of methods (S/MIME, PDF, Webmail)
- 1.1.5 Does the solution support a simplified interface for consumer-based messaging? It should not force software or script downloads to users.
- 1.1.6 Does the solution provide password hints and password history to unburden administrators?
- 1.1.7 Does the solution offer a choice of boundary- or desktop-based encryption buttons so that users can easily flag a message for encryption?

1.2 Message Delivery Options

- 1.2.1 Does the solution offer a variety of secure e-mail delivery methods to meet the needs of a wide variety of recipients? These should be supported concurrently and support offline decryption of messages.
- 1.2.2 Are there any requirements for recipients to download software, plug-ins or scripts? Recipients should not have to download any non-standard software extensions, plug-in or scripts.
- 1.2.3 Does the solution offer flexible configuration options on behalf of recipients? For example, the system can be configured to enable/disable the ability to forward, reply, access address books, etc.
- 1.2.4 Does the solution support ad hoc message delivery to allow senders to define a password on-the-fly without having recipients register on the system? (This is useful for securely messaging to prospective clients or to those for "one-off" communications.)
- 1.2.5 Does the solution support standards-based delivery directly to desktop e-mail clients (e.g., Microsoft Outlook and Lotus Notes) using industry-standard methods such as S/MIME, PGP or PDF?

- 1.2.6 Does the solution offer the ability to generate standards-based credentials for external recipients who do not have existing certificates?
- 1.2.7 Does the solution have the ability to deliver e-mail in an encrypted Web-based envelope (webmail push)?
- 1.2.8 Does the solution have the ability to provide a secure webmail inbox for external recipients (webmail pull)?
- 1.2.9 Does the solution offer full mailbox capability, including folder management, ability to reply securely, sent history, etc.?
- 1.2.10 Does the solution have the ability to send secure encrypted messages to non-certificate users, allowing them to decrypt using existing desktop applications such as PDF readers?
- 1.2.11 Does the solution provide support for standard secure e-mail capabilities such as encrypted replies or encrypted attachments?
- 1.2.12 Is the solution an integral part of the messaging system for account creation, management, etc.?
- 1.2.13 Does the solution support custom branding templates on secure e-mail?
- 1.2.14 Is the solution easily integrated to other gateway-based systems for gateway-to-gateway encryption?

1.3 Standards Support

- 1.3.1 Does the solution support standards based encryption methods to ensure external users can decrypt using existing desktop applications such as Microsoft Outlook, Adobe Acrobat, Internet Explorer, etc.?
- 1.3.2 Does the solution ensure all recipients (with or without credentials) can decrypt messages with existing desktop technology?
- 1.3.3 Does the solution support all industry standard e-mail encryption standards?
- 1.3.4 Does the solution ensure that senders and recipients can manage e-mail natively in Microsoft Outlook or other clients?
- 1.3.5 There should not be a need for external users to load custom extensions/applets on the PC. Does the solution support this requirement?
- 1.3.6 Does the solution support digital signatures? This can be key to future e-enablement of business processes.
- 1.3.7 Does the solution interoperate with other standards-based encryption gateway appliances to provide gateway-to-gateway encryption?

1.4 Flexibility of Delivery Options

- 1.4.1 Does the solution support end-to-end encryption as well as boundary-based encryption? Can it support both simultaneously based on user groups?
- 1.4.2 Does the solution interoperate on behalf of desktop encryption users to automate external delivery and certificate management?
- 1.4.3 Does the solution interoperate with content-control systems such that when a message contains sensitive information, it is automatically encrypted without user intervention?
- 1.4.4 The solution should provide options for users to flag messages to be encrypted at the network boundary. This can be done by setting message attributes (header information) or with an optional e-mail client plug-in. Does the solution support this functionality?
- 1.4.5 An interface should be available to allow senders to define a message-specific password and flag that message for encryption for "ad hoc" secure messaging. Is this supported?

1.5 Integration to existing infrastructure

- 1.5.1 Does the solution support integration to off-board certification authorities (CA) and provide the ability to:
 - Leverage existing certificates within the organization
 - Allow the messaging server to interoperate with existing desktop encryption solutions within the organization to extend secure messaging outside the network and automate message delivery, certificate harvest, etc.
 - Leverage existing Certificate Revocation Lists (CRLs) and investments in corporate certification authorities
 - Utilize the certificate creation and management capabilities provided by the existing certification authority infrastructure/PKI
- 1.5.2 Does the solution provide secure interoperability with any content-scanning vendor for automated encryption?
- 1.5.3 Does the solution integrate with existing portal authentication systems such that external users or system administrators can gain secure access to the system using their usual way of authentication?
- 1.5.4 Does the solution integrate to standard SNMP management systems? (SNMP monitors hardware, operating system and application with definable thresholds and traps.)
- 1.5.5 Does the solution support multifactor authentication?
- 1.5.6 Does the solution integrate with both boundary and end-to-end archiving solutions? Desktop-encrypted messages should be decrypted on their way into the archive to support full-text scanning, e-discovery and retrieval, etc.
- 1.5.7 Does the solution integrate with complementary e-mail applications such as content analysis, e-mail hygiene, etc.?

1.6 Mobile Solutions Support

- 1.6.1 Is the solution capable of automating encryption for BlackBerry users, leveraging the existing user certificates and BlackBerry features?
- 1.6.2 Does the solution support mobile phone users? If so, are they able to access and read secure webmail in a mobile browser interface?
- 1.6.3 Does the solution support Microsoft Windows Mobile?

1.7 Platform Architecture

- 1.7.1 Describe how the solution is hardened, including the hardware, operating system and application environment.
- 1.7.2 Does the solution include hardware and/or software redundancy and fault tolerance capabilities? If so, please list them.
- 1.7.3 Solution architecture should support out-of-box clustering for simple scalability and management. As needs increase, the system should easily incorporate cluster nodes for increased capacity. Pricing should support this per-cpu scalability model. Does the solution meet these requirements?
- 1.7.4 Does the solution support the ability to have Web-only nodes so that critical components can be located securely while Web interfaces can be accessed within a DMZ environment?
- 1.7.5 Does the solution support a disaster recovery plan so that nodes may be located in separate geographic locations while being managed through a single management console?
- 1.7.6 Does the solution enable administrators to define password length and characteristics for external mail recipients?

1.8 Auditing, Reporting and Administration

- 1.8.1 Does the solution provide complete audit capabilities to monitor all system configuration or administration changes?
- 1.8.2 Does the solution allow definition of roles-based access to restrict and report on administrative and configuration responsibilities?
- 1.8.3 Does the solution provide the ability to monitor/manage cluster-wide from a single interface?
- 1.8.4 Does the solution support comprehensive management of user mailboxes for webmail pull, including message expiry and automated mailbox cleanup?
- 1.8.5 Does the solution provide detailed reporting that can be run on a scheduled or ad hoc basis for all aspects of the messaging server's use? Are these reports viewable within the management interface or exportable to standards-based reporting systems?

1.9 Hardened Appliance

- 1.9.1 Is the solution based on a hardened OS that ensures it is secure (.i.e., weak security portions of the OS and hardware have been removed)?
- 1.9.2 Is the solution FIPS-validated to ensure the utmost in security as validated by an external organization?
- 1.9.3 Does the solution have a defined security process to facilitate updates and patches to ensure maintenance of the solutions hardware and software?
- 1.9.4 Does the solution support roles-based access to critical system administration functions, ensuring only those authorized access the appliance and the configuration remains secure?
- 1.9.5 Does the solution have the capability to fully audit configuration and administration functions in order to track changes?

2 Vendor

2.1 Corporate Information — briefly describe the following

- 2.1.1 Corporate profile
- 2.1.2 Number of employees
- 2.1.3 Corporate headquarters and other office locations
- 2.1.4 Financials (copy of 10k report or annual report)
- 2.1.5 List any product awards won in the last five years
- 2.1.6 List any relevant experience and customer deployments. Are these customers referencable?
- 2.1.7 Describe your corporate quality and security assurance process.

2.2 Technical Support

- 2.2.1 Describe your technical support options, policies and procedures.

2.3 Documentation and Training

- 2.3.1 Describe your method of providing documentation and training for your products.

2.4 Strategic Partnerships

- 2.4.1 Describe your strategic relationships or vendor alliances you have regarding the delivery of digital signatures, authentication and encryption products and services.

2.5 Services

- 2.5.1 Does your company provide professional services capabilities on a global basis?
- 2.5.2 Does your company have a dedicated solution design and deployment team to enable customer input to product enhancements?