Offer Specifications
Dell Email Management Services (EMS): Encrypted Mail

Services Overview

Dell Encrypted Mail gives organizations the ability to enforce email encryption right at the desktop, completely eliminating the possibility of confidential information being read by the IT department or anyone other than the intended recipient.

With Encrypted Mail managers and executives can be confident that their confidential information is never exposed to their IT department or potential hackers.

With one click, employees can manually encrypt their own emails. This end point solution enables users to digitally sign, encrypt and decrypt messages, and can be implemented without the upfront investment in additional hardware or software.

Organizations need Encrypted Mail product because

- Ensure the confidentiality of email communications
- Simple to use – no end user training required
- No capital expenditure and low monthly / annual per user cost
- Fully hosted and scalable solution
- Low Monthly subscription helps control costs
- Digital signatures deliver non-repudiation of e-mails
- Reduce the costs associated with couriers and mailings
- Meet the requirements of privacy legislation
- Ensures the integrity of the message content and authenticates the sender
- Gain a competitive advantage by associating the company brand with security

How Encrypted Mail works?

- Users simply compose an email and click the “secure” icon to encrypt the message before sending. The user enters their password to digitally sign and encrypt the message
- The email will arrive in the recipient’s inbox encrypted.
- To decrypt the message the recipient opens the message, enters their password which decrypts the message
- Recipients who do not subscribe to Encrypted Mail:
  - Are notified to pick up their encrypted messages from a secure web portal
  - After a one-time registration, user have access to all encrypted message sent to them
  - They can then send and receive encrypted messages from within the secure portal
Benefits / Features

Benefits

- Protect the privacy of their email communications
- Implement a cost-effective corporate-wide email privacy service
- Send Encrypted Mail to any email address
- Send Encrypted Mail messages to non-subscribers such as customers and partners
- Create brand impressions each time a Encrypted Mail message is sent, associating the company’s brand with secure communications

Key Differentiators of Encrypted Mail

- Send Secure Messages to anyone with a valid email address
- Easy to install and use
- Provides proven true end-to-end S/MIME encryption
- Messages are secured on the desktop of the sender, and unlocked on the recipient’s computer.
- Messages remain encrypted when stored.
- Ensures message integrity through the application of PKI, S/MIME-based digital signatures and delivers non-repudiation
- User control over which messages are encrypted
- Integrated with existing Outlook and Outlook Express, Lotus Notes Webmail client
- Designed to support millions of subscribers and be highly available
- Enterprise branding
- Delivered as a fully managed and hosted security service
- Based on industry trusted public key infrastructure (PKI), X.509 certificates and S/MIME standards

Features

- Simple to Use - End users click an “Encrypt Button” to encrypt all messages.
- Simple Installation - Simply download the Encrypted Mail plugin and install on your desktop or laptop computer
- Send Encrypted Email to anybody
- Use Encrypted Mail to send encrypted messages to any email address including Gmail, Yahoo, and Hotmail accounts
- Easily Unlock Encrypted Mail
- Simply click on the Encrypted message and enter your password to open Standards Based
- Industry standard encryption including digital signatures, PKI, RSA, and AES Certificate Authority
- No need to deploy and maintain expensive third party PKI or Certification Authorities Confirm Sender’s ID
- Digital signatures guarantee the identity of the sender
- Truly Secure - Trusted encryption standards including PKI, X.509 digital certificates, and S/ MIME

Technical Requirements

Dell Email Management Services (EMS): Encrypted Mail

- Web Browser: Microsoft TM Internet Explorer ® 6.0 or above
- Internet Connection: LAN-based using standard TCP/IP DSL, ADSL, Cable Modem
- Computer Hardware: 5-10 MB of hard drive space Pentium 233 MHz (minimum) 128 MB RAM (minimum)

Provision of Services

The Customer will receive a welcome email with a request for provisioning information. Once the information has been received, it will be used to provision the Customer onto the Services. As part of the provisioning process, the Customer will receive on-boarding information and a training session to review the application's functionalities.

Once individual end-users are registered to the service, each user will receive an activation email with instructions on how to activate their Encrypted Mail plug-in. Contained within the activation email is a unique activation code which will be used by each individual user.

The Encrypted Mail plug-in can also be packaged as a gold image MSI install package that then can be pushed down to each desktop within the company through standard MSI install processes.

Customer Responsibilities

- Provide all necessary information, and authorizations as required and ensuring that a dedicated technical resource with administrative rights is available for provisioning of service
- Depending on the deployment option chosen, Customer may be required to execute a disclosure agreement related to export compliance.
- Customer acknowledges that information processed in the course of performing the Services may contain personally identifiable information of individuals and associated metadata and that the processing of such information may therefore involve the processing of personal data. With respect to any and all data, including, but not limited to, third party data, personally identifiable information and associated metadata obtained by Dell pursuant to Customer’s use of the Services (collectively, the “Data”), Customer shall take all necessary measures to ensure that it, and all its employees, are aware that their personal data may be processed as part of the Services and that they have given their consent to such processing as well as complied with their responsibilities as data controller or data subjects, as applicable, in accordance with applicable privacy laws and/or regulations (“Privacy Laws”). Customer understands and agrees that Dell has no control or influence over the content of the Data processed by Dell, and that Dell performs the Services on behalf of Customer. Notwithstanding the generality of the foregoing obligation, as required by the Privacy Laws, Customer shall use all reasonable efforts to ensure that it informs individuals who use any communications system covered by the Services that communications transmitted through such system may be intercepted.
Customer Agreement

Customer’s purchase and use of this Service is governed by and subject to the following terms and conditions: 1) the Dell Cloud Solutions Agreement (or Customer’s separate-signed services agreement); 2) this Specification Sheet; and 3) an Order Form for this Service. Collectively, these documents comprise Customer’s Dell Email Management Services Policy Based Encryption-E Service Agreement or the “Agreement.”

The Dell Cloud Solutions Agreement

The Dell Cloud Solutions Agreement is available via www.Dell.com/cloudterms and in hardcopy upon request. The parties acknowledge having read and agree to be bound by such terms. In lieu of the Dell Cloud Solutions Agreement, Customers may purchase these Services under their separate-signed services agreement with Dell, but only to the extent such agreement explicitly authorizes Customer to purchase these Services, as identified on the Order Form or other mutually-agreed upon form of invoice, order acknowledgement, or purchase order.

For more information about any of our service offerings, please contact your Dell representative or visit dell.com/services. Availability varies by country. To learn more, customers and Dell Channel Partners should contact your sales representative for more information.

© 2013 Dell Inc. All rights reserved. Trademarks and trade names may be used in this document to refer to either the entities claiming the marks and names or their products. Specifications are correct at date of publication but are subject to availability or change at any time, without notice. Dell and its affiliates are not responsible for errors or omissions in typography or photography. Dell service offerings do not affect a consumer’s statutory rights.

Dell Email Management Services: Encrypted Email; April 19, 2013