Offer Specifications
Dell Email Management Services (EMS): Policy Based Encryption-E

Service Overview

The Policy Based Encryption-E service ("PBE-E" or the "Service(s)"), provides the ability for organizations to send sensitive email content safely and in compliance with regulations by automatically encrypting specific emails based on a Customer’s email security policy – that is, a set of rules designed to analyze all outbound email, and encrypt any email that matches the pre-defined conditions. In order to receive PBE-E, the Customer must subscribe to the following services included in the offer:

- **Email Content Control Service** –
  - The Email Content Control Service enables the Customer to configure, in line with its acceptable computer use policy or equivalent, a rule-based filtering strategy for filtering incoming and outgoing email. A rule is an instruction set up by the Customer that identifies specified content or a particular format of message/attachment and follows the course of action prescribed for that content or format. Policy Based Encryption uses Email Content Control rules to identify which email needs to be encrypted.

- **Email Boundary Encryption Service** –
  - The Email Boundary Encryption Service ("BE") provides encrypted communication channels that enable the Customer to form a secure private email network (SPEN) with nominated partner organizations. This configuration is known as "enforced" encryption. The Customer can also receive encrypted emails sent from organizations that have transport layer security (TLS)-capable mail servers, but no enforced encryption with the Customer. This configuration is known as "opportunistic" encryption.

  - Email exchanges between the Dell EMS Email Security Service, (powered by Symantec.Cloud formerly MessageLabs), and Customer’s Secure Connection mail servers shall be secured by TLS encryption. Whether onward routing will be performed in unencrypted or encrypted format will depend on (i) Customer specified TLS enforcements and (ii) destination server capability to receive Emails over Opportunistic TLS.

  - If the Customer is using BE in conjunction with the PBE Service, the recommended best practice is for the Customer to implement the Secure Connection model of BE on all its mail servers.

  - CUSTOMER ACKNOWLEDGES AND ACCEPTS THAT IF THE SECURE CONNECTION MODEL IS NOT APPLIED TO A PARTICULAR MAIL SERVER, CUSTOMER’S INBOUND AND OUTBOUND EMAILS ORIGINATING FROM OR RECEIVED BY THAT MAIL SERVER SHALL NOT BE SECURED BY TLS ENCRYPTION. ACCORDINGLY, THE CUSTOMER
ACKNOWLEDGES AND ACCEPTS THAT IT SHOULD NOT SEND OR RECEIVE SENSITIVE DATA VIA SUCH MAIL SERVERS AND DOES SO ENTIRELY AT ITS OWN RISK.

Policy Based Encryption-E provides the following functionality:

- Ability to use the Email Content Control Service to define outbound encryption policies for emails.
- Delivery of encrypted emails to the external recipient’s inbox.
- Recipient access to encrypted email via a secure web portal.
- Recipient access to the secure web portal to respond to email in an encrypted format.

Policy Based Encryption-E provides the following features:

- **Push-**
  - PBE allows the Customer to send an encrypted Email directly into a recipient’s inbox without the need to download software.
  - The “PBE Push” variant of the PBE-E Service sends the recipient an email notification with the original Email saved within it as an encrypted attachment. Following initial registration online, the recipient is able to view the decrypted Email offline using a Java application on their desktop.

- **Pull-**
  - An email recipient retrieves email via a secure web based portal.
  - The customer can configure the encryption method to either Push or Pull. The default encryption method for the Policy Based Encryption-E option is Pull but can be changed to Push by the recipient by downloading the Secure Reader functionality within the recipient’s secure web portal.
  - The “PBE Pull” variant of the Service sends the recipient an email notification. The recipient is able to view the decrypted Email online via a secure SSL session in their browser when they log on to a secure web portal and enter their password.
  - PBE also enables a recipient to enter a secure web portal and respond to an encrypted Email in an encrypted format.

- **Branded Portal** – The Customer may brand the portal that recipients use to read their encrypted Emails (for example to include the Customer’s logo).

- **Secure reply and compose** – The recipient of an encrypted Email may also send a brand new Email to any of the Customer’s PBE Users.

Note: A third party Outlook Plug-In is available which adds an “encrypt” icon to the recipient’s Outlook toolbar. The Customer acknowledges and agrees that Dell is not responsible for such third party software.
Policy Based Encryption-E provides the following additional capabilities:

- A recipient can choose the language of the recipient’s secure web portal and notification emails from a list of supported languages.
- Recipients can log into their accounts without opening a specific message, even if they have no active messages.
- Recipients can view all of their previous messages (that have not been permanently deleted) in their inbox, including messages they have sent.
- If using the Pull method, a message composed in the web portal may have multiple recipients provided that such recipients share a domain from which the User has previously received a secure email.
- If using the Push method, recipients can reply to any email address under the same domain.
- Initial notifications to new Users are available in more than one language.
- It is possible to use a third party certificate/key to encrypt an outbound Email using the recipient’s public key and decrypt an inbound Email using the recipient’s private key, rather than the default certificates/keys generated by the PBE Service.

Service Parameters: Policy Based Encryption–E

- The number of secure Emails the Customer may send in any month using PBE-E may not exceed four hundred and eighty (480) times the Registered Usage for PBE. When sending to multiple recipients, each unique address will be counted as a secure Email. In the event that the Customer exceeds the number of permitted secure Emails in any month, Dell shall increase the Registered Usage accordingly.
- Emails routed through PBE E are limited to a maximum size of fifty megabytes (50 MB) per Email post-encryption.

PBE ONLY OPERATES WHEN USED IN CONJUNCTION WITH THE BOUNDARY ENCRYPTION AND EMAIL CONTENT CONTROL SERVICES. THE EMAIL CONTENT CONTROL SERVICE IS AVAILABLE FOR CUSTOMERS WHO PURCHASE PBE AS A STANDALONE SERVICE OR FOR CUSTOMERS THAT PURCHASE PBE AS AN ADD ON TO THE DELL EMS EMAIL SECURITY SERVICE. EACH INDIVIDUAL PBE USER MUST BE AN EMAIL CONTENT CONTROL USER.

Support Procedures

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.
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 including editing of Customer’s public Mail Exchanger (MX) records within the Domain Name System (DNS).
- Setting and managing email security policies. The Customer is responsible for implementing the configuration of PBE according to the Customer’s needs. The Customer configures PBE via ClientNet by selecting the options available under the Email Content Control Service.
- Customer needs to have a X.509v3 digital certificate issued by a recognized public Certificate Authority such as Verisign for establishing the TLS connection between the customer and the Dell EMS Email Security Service.
- Dell emphasizes that the configuration of PBE is entirely under the control of the Customer and that the accuracy of such configuration will determine the accuracy of PBE. Dell can therefore accept no liability for any damage or loss resulting directly or indirectly from any failure of PBE to fulfill the Customer’s encryption obligations.
- Depending on the deployment option chosen, Customer may be required to execute a disclosure agreement related to export compliance.

Data Privacy Acknowledgement

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 and its licensor Symantec 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 its licensor Symantec 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.

Important Supplemental Terms & Conditions

These supplemental provisions also apply to Customer's use of this Service. If there is a conflict between the terms of this Specification Sheet and any of the other documents that comprise the Agreement ("Conflicting Terms"), the terms of this Specification Sheet ("Prevailing Terms") will take precedence over the Conflicting Terms solely with respect to Customer’s use of this Service. Moreover, the Prevailing Terms shall be construed as narrowly as possible to resolve the conflict while preserving as much of the Agreement as possible, including but not limited to preserving non-conflicting provisions contained within the same paragraph, section or sub-section as the Conflicting Terms.

1. If, at any time, continued provision of the Services would compromise the security of the Services, due to (without limitation) hacking attempts, denial of service attacks, mail bombs, or other malicious activities either directed at or originating from Customer's domains, Customer agrees that Dell or its licensors, software suppliers, and delivery partners may suspend Services to Customer. In such an event, Dell will promptly inform Customer and will work with Customer to resolve such issues and reinstate the Services.

2. Dell, through its licensor Symantec, may update the Service at any time in order to maintain the effectiveness of the Service.

3. Unless otherwise agreed to in writing with Dell, the Services are provided to Customer for its internal use only, and Customer shall not resell the Services to any third party.

4. Customer agrees to provide and maintain a list of all email addresses registered to receive the Services (the "Validation List"). It is Customer's responsibility to verify the Validation List prior to the Services being made available and throughout the term of the Agreement. Customer acknowledges that inbound email sent to email addresses not specified or incorrectly entered in the Validation List will be blocked automatically. Customer agrees that neither Dell nor Dell's suppliers will be liable for damages arising out of or in connection with the non-delivery of email resulting from the Customer's errors in or omissions of email addresses.

5. Customer will provide Dell with all technical data and other information Dell or its licensor Symantec may reasonably request from time to time to allow Dell to supply the Services to Customer. All information Customer supplies will be complete, accurate, and given in good faith.

6. Customer shall not allow its systems to: (i) act as an Open Relay or Open Proxy; (ii) send or receive Volume Mail instigated by Customer (unless the Customer has purchased the Volume Mail Service, in which case the Customer may send and receive Volume Mail strictly in accordance with the terms and
conditions applicable to the Volume Mail Service); or (iii) send spam. Dell reserves the right at any time to verify Customer’s compliance with this section. Customer agrees to indemnify Dell and its suppliers against, and hold Dell and its suppliers harmless from, any and all claims, actions, losses, costs, and expenses Dell and its suppliers may incur as a result of Customer’s breach of this section.

7. Customer acknowledges that information sent to and from Customer will pass through the Service. Accordingly, Customer agrees to use the Service for legitimate and lawful business purposes only.

8. **IN NO EVENT WILL EITHER PARTY OR ITS SUPPLIERS BE LIABLE, WHETHER IN CONTRACT, TORT OR OTHERWISE, FOR ANY INCIDENTAL, CONSEQUENTIAL, SPECIAL, EXEMPLARY OR INDIRECT DAMAGES, LOSSES, EXPENSES OR COSTS OF ANY KIND, COSTS OF PROCUREMENT OF SUBSTITUTE OR REPLACEMENT GOODS OR SERVICES, LOST BUSINESS PROFITS OR REVENUE OR LOST OR CORRUPTED DATA ARISING OUT OF THIS AGREEMENT OR USE OF THE SERVICES OR DELIVERABLES, EVEN IF ADVISED OF THE POSSIBILITY. NOTHING IN THIS AGREEMENT WILL LIMIT EITHER PARTY’S LIABILITY FOR ANY DAMAGE THAT CANNOT BE EXCLUDED BY LAW. EXCEPT FOR BREACHES OF THIS AGREEMENT RELATING TO INDEMNITY OBLIGATIONS OR ACTS OF FRAUD DETERMINED BY A COURT OF FINAL JURISDICTION, DELL’S AND ITS SUPPLIERS’ TOTAL LIABILITY UNDER THIS AGREEMENT WILL BE LIMITED TO THE FEES PAID BY CUSTOMER FOR THE SERVICES GIVING RISE TO THE LIABILITY.**

9. The intellectual property rights in the Services and any hardware or software used in connection with the Services is and will at all times remain Dell’s property or that of Dell’s licensors.

10. Customer agrees to comply with all relevant laws including, without limitation, the U.S. Export Administration Regulations (EAR) and the laws of any country from which the Services are exported or re-exported.

11. Customer agrees to indemnify Dell and its suppliers against, and hold Dell and its suppliers harmless from, any and all claims, actions, losses, costs, and expenses Dell and its suppliers may incur as a result of: (i) any third party claim in relation to information passing through the Services to or from the Customer; (ii) any third party claim in relation to the interception of communications by the Services; and/or (iii) any third party claim in relation to the Customer’s use of the Services in breach of privacy laws.

12. The Customer acknowledges that: (a) Dell is the reseller of the Services described herein and the sub-licensor of worldwide intellectual property rights that are owned by third-party licensors; and (b) the acknowledgements, obligations, restrictions, and undertakings given or accepted by the Customer are for the benefit of Dell and its licensors, and such licensors are third-party beneficiaries under this Agreement and may enforce those provisions directly against the Customer or through Dell.

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.
© 2012 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: Policy Based Encryption-E Offer Specifications; September 6, 2012