Microsoft Exchange Hosted Services

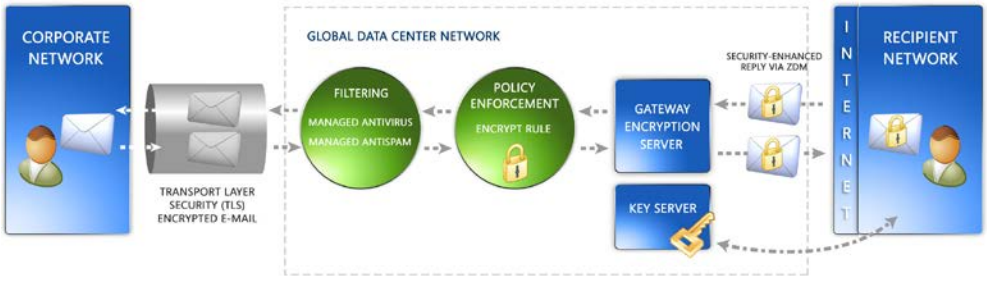
Microsoft

MICROSOFT EXCHANGE HOSTED ENCRYPTION

Microsoft® Exchange Hosted Encryption is a convenient, easy-to-use e-mail encryption service that helps to safely deliver your confidential business communications.

Government and industry regulations—such as those posed by the Health Insurance Portability and Accountability Act (HIPAA) and the Gramm-Leach-Bliley Act (GLBA)—offer even more compelling reasons for corporations to increase the security of messages to help meet compliance requirements. However, existing solutions—such as server-to-server level encryption, public key infrastructure (PKI), and password-protected files—can be expensive and complicated to integrate and to deploy for communication with parties outside of your organization. These solutions do not provide the flexibility, sophistication, or ease of use that corporate users need to deploy e-mail encryption for external communications.

Exchange Hosted Encryption is one of four distinct services in the Microsoft Exchange Hosted Services portfolio. The service enables users to send and receive encrypted e-mail directly from their desktops as easily as regular e-mail. Using a simple process, users can encrypt and deliver any business communication without complex hardware and software to purchase, configure, and maintain. Exchange Hosted Encryption is deployed over the Internet, which helps minimize up-front capital investment, free up IT resources to focus on value-producing initiatives, and mitigate messaging risks before they reach the corporate network.



Microsoft Exchange Hosted Encryption Flow Diagram

HOW IT WORKS

In traditional encryption systems such as PKI, certificates bind public keys to identities. Users must pre-enroll in server systems to receive a certificate, which is signed by a Certification Authority, so that they can send and receive secure messages.

Exchange Hosted Encryption incorporates Identity-Based Encryption (IBE) technology in a managed service platform. Developed by Voltage Security, a Microsoft technology partner, IBE is a breakthrough in security and usability for message encryption. Exchange Hosted Encryption eliminates the need for certificates and uses a recipient's e-mail address as the public key, IBE automatically binds the user's identity to the public key and eliminates the need for certificates.

- Send encrypted e-mail messages to anyone, regardless of the recipient's system configuration
- Decrypt and read e-mail with confidence, without installing client software
- Provide strong, automated encryption with a cost-effective infrastructure.
- Consistently and automatically help protect sensitive information and data leaving your e-mail gateway,
- Help manage compliance with security and privacy requirements such as HIPAA and GLBA
- Eliminate need for key and certificate management
- Generate keys on the fly
- Minimize up-front capital investment
- Integrate with existing e-mail infrastructure
- Help free up administrator time to focus on other projects`

Microsoft Exchange Hosted Services

SOLUTIONS OVERVIEW

Transparent Encryption and E-Mail Delivery

When a user sends an e-mail message, it travels to the Microsoft global network through a TLS-encrypted tunnel, and is automatically encrypted at the gateway according to rules created and managed within the Microsoft Exchange Filtering module.

When a message is encrypted, a private key for the recipient is created and stored in a security-enhanced environment on the Microsoft network. The private key is made available to the message recipient when the recipient decrypts the message. The recipient does not have to pre-enroll to receive and decrypt the message. In fact, the recipient may have never received a prior e-mail from the sender.

The Microsoft encryption process is transparent to the sender, who does not need to do anything other than write and send the message as usual.

Simple Authentication and Security-Enhanced, Web-based Decryption

Upon receiving a Microsoft Exchange encrypted message, the recipient completes an easy two-step authentication process through e-mail answerback to verify the recipient's identity.

After completing the authentication process, the recipient decrypts and views the message using the Voltage Zero Download Messenger. The Zero Download Messenger is a clientless, browser-based method that enables a recipient to have confidence decrypting and reading a message and its attachments and then to reply with confidence. Furthermore, the encrypted message remains in the recipient's e-mail inbox for access at any time.

- Lower total cost of ownership than on-premise solutions
- Offers a predictable subscription-based payment
- Simplifies IT environment by minimizing the need to deploy, configure, monitor, and update in-house e-mail security servers and applications
- Helps increase available bandwidth
- Helps free up server resources and lower load on CPU
- Scales to meet the needs of virtually any enterprise

FEATURES

- Policy-based encryption encrypts messages at the gateway based on policy rules
- IBE technology uses a common ID for public key.
- Encrypted e-mail delivered directly to recipients' inbox and not to a Web service.
- The Zero Download Messenger enables Web-based decryption and encrypted replies for any recipient of encrypted messages.
- Managed key server eliminates the need for certificate maintenance.
- Communication through TLS-enabled network further enhances message security.

"Security, compliance, and business continuity requirements in industries such as healthcare and financial services are placing greater demands on the messaging infrastructure. It's not enough to handle these challenges with a growing array of stand-alone appliances or point solutions. Managed services are a fundamentally sound method for deploying multiple, integrated services."

Michael Osterman,
President and Founder,
Osterman Research

ABOUT MICROSOFT EXCHANGE HOSTED SERVICES

Microsoft Exchange Hosted Services offer a cost-effective way for enterprises to actively ensure the security and availability of their messaging environment, while instilling confidence that their messaging processes satisfy internal policy and regulatory compliance requirements. A seamless extension of Microsoft Exchange that operates over the Internet as a service, the complete line of services includes hosted filtering for spam and virus protection; hosted archiving to satisfy compliance requirements and internal policies; hosted encryption to preserve e-mail confidentiality; and, hosted continuity for ongoing access to e-mail during and after disasters. Microsoft Exchange Hosted Services provide value to corporate customers by eliminating upfront capital investment, freeing up IT resources, and removing incoming e-mail threats before they reach the corporate firewall. For more information, visit

http://www.microsoft.com/exchange/services

Microsoft