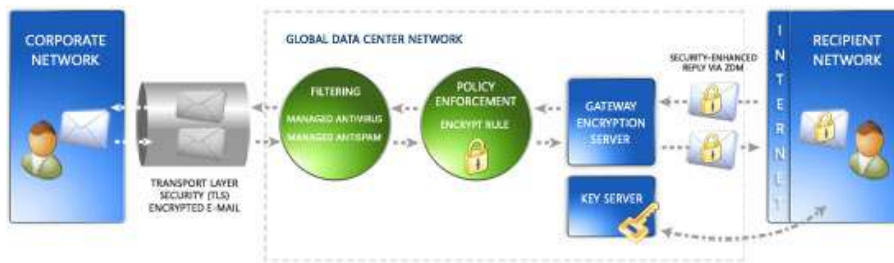


## MS Hosted Exchange Encryption

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 Health Insurance Portability and Accountability Act (HIPAA) and Gramm-Leach-Bliley, 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 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.



### 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.

### Solution Overview

#### Transparent Encryption and E-Mail Delivery

When a user sends an e-mail message, it travels to the Microsoft global network through a Transport Layer Security (TLS)-encrypted tunnel, and is automatically encrypted at the gateway according to rules created and managed within the Microsoft Exchange Hosted 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 entirely 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 an encrypted message, the recipient authenticates their identity and sets a password to securely open encrypted messages from the Hosted Encryption service. Once this password is created, the recipient can use the same password to quickly authenticate and view protected email. Password-based authentication provides an easy and secure method to authenticate and verify a recipient's identity.

After completing the authentication and password setup 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.

### **Benefits**

- Sends encrypted e-mail messages to anyone, regardless of the recipient's system configuration
- Decrypts and read e-mail with confidence, without installing client software
- Provides strong, automated encryption with a cost-effective infrastructure
- Consistently and automatically helps protect sensitive information and data leaving your e-mail gateway
- Helps manage compliance with security and privacy requirements such as HIPAA and Gramm-Leach-Bliley
- Eliminates need for key and certificate management
- Generates keys on the fly
- Minimizes up-front capital investment
- Integrates with existing e-mail infrastructure
- Helps free up administrator time to focus on other projects