WHITE PAPER: TECHNICAL

symantec™

Confidence in a connected world.

Enterprise Vault 8.0 Security Model for Secure Messaging 8.0

Rob Forgione
Technical Field Enablement
February 2009

Contents

If you have any comments on this Whitepaper please email EV-TFE-Feedback@Symantec.com

Purpose

The purpose of this document is to detail how the Enterprise Vault Secure Messaging Adapter:

- Securely decrypts Exchange data to allow for indexing

This document will give readers a better understanding of how the Enterprise Vault (EV) Secure Messaging Adapter can securely decrypt messages encrypted by RMS, PGP, and Liquid Machines Document Control.

This whitepaper assumes the reader has already read the Enterprise Vault 8.0 Security Model for Enterprise Vault 8.0 and SQL server whitepaper and is familiar with the security concepts of Enterprise Vault. The Security Model series consists of:

- Enterprise Vault 8.0 Security Model Enterprise Vault 8.0 and SQL server
- Enterprise Vault 8.0 Security Model for Microsoft Exchange Archiving
- Enterprise Vault 8.0 Security Model for Lotus Domino Archiving
- Enterprise Vault 8.0 Security Model for File System Archiving
- Enterprise Vault 8.0 Security Model for Microsoft SharePoint Archiving
- Enterprise Vault 8.0 Security Model for SMTP Archiving
- Enterprise Vault 8.0 Security Model for Discovery Accelerator 8.0
- Enterprise Vault 8.0 Security Model for Compliance Accelerator 8.0
- Enterprise Vault 8.0 Security Model for Automatic Classification Engine 8.0
- **Enterprise Vault 8.0 Security Model for Secure Messaging 8.0**

This whitepaper is intended to train the reader the concepts behind Enterprise Vault 8.0 security for archiving encrypted content through Rights Management.

Enterprise Vault Services

Enterprise Vault uses the following service for Secure Messaging and Rights Management:

- Enterprise Vault Gateway Service for Secure Messaging and Rights Management

This service does not have a dependency on any other Enterprise Vault services.

A service account must be created within Active Directory in which the RMS installation and the Enterprise Vault server reside. This account is referred to as the ***Gateway Service account*.**

Do not configure this service to run within the context of the Vault Service account. RMS permissions given to the Vault Service account will extend security privileges beyond what is appropriate and secure.

Refer to the Enterprise Vault Adapter for Secure Messaging and Rights Management documentation for more information on the additional requirements of the Gateway Service account.

Rights Management through Encryption

Rights management is an important concept in protecting email and documents. **Rights management** means that access controls, along with rules about how data can be used, travel with copies of that data. Taking a copy out of a server and placing it onto a workstation or sending it out of a company's infrastructure and into the Internet does not remove the controls from the data. A **rights management service** determines who gets the rights to open each message or document. Rights-managed client applications allow recipients to view and manipulate the data and to send copies elsewhere, if the controls allow.

Organizations that are concerned with security of data when sent outside the enterprise, are welcome to use gateway-level encryption, which does not affect the ability to archive and search email. If they are concerned with security of data “at rest” in the archive, storage-level encryption such as NetApp Decru or Microsoft Windows Encrypted File System could be used which operates underneath the system and is transparent to the archive. Organizations that are concerned with security of data inside and outside the network, should consider enterprise PKI-based encryption or rights management systems.

Control is accomplished through encryption. Documents and messages are protected by encrypting them, and access to them is controlled by permitting or denying access to the key that was used to encrypt them.

Any encrypted item archived in Enterprise Vault can still be retrieved by the user as long as they possess the appropriate keys. In addition, message properties are typically not encrypted and are therefore searchable. Enterprise Vault flags all encrypted content so customers can identify “rogue” encryption systems internally. Enterprise Vault also provides an API to allow encryption systems to decrypt content prior to archiving thus allowing for indexing and searching for the item.

Enterprise Vault Adapter for Secure Messaging and Rights Management

The Secure Messaging and Rights Management Adapter works with any or all of the following security services:

- Microsoft Windows Rights Management Services
- Liquid Machines Document Control
- PGP

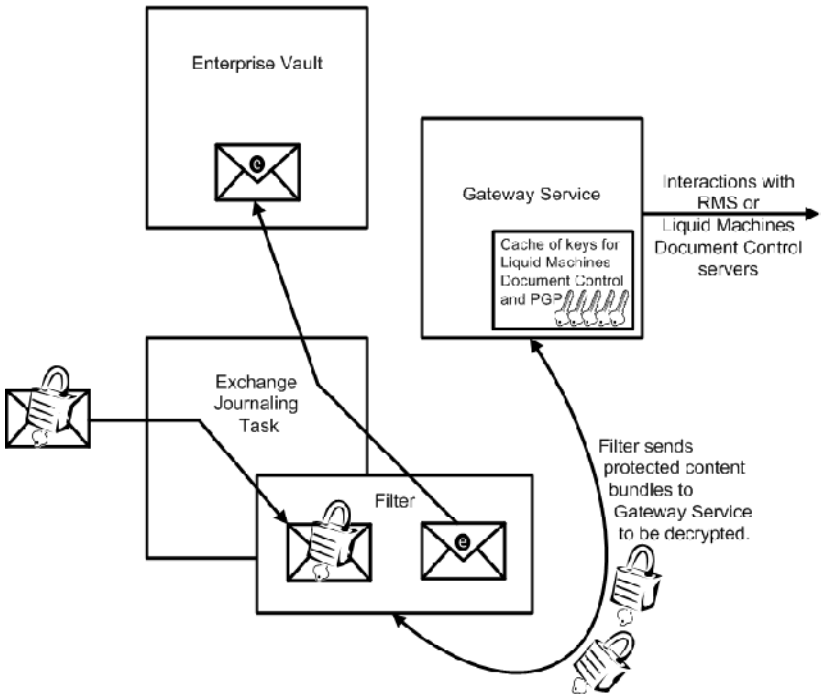
Refer to the Enterprise Vault Adapter for Secure Messaging and Rights Management.pdf for more information on the specifics of these security services.

The Symantec Enterprise Vault Adapter for Secure Messaging and Rights Management decrypts email messages and attachments, to ensure that journaled email messages are stored in Enterprise Vault in a way that is compliant with company policies as well as the ability to be discoverable via e-discovery searches.

The Adapter is installed on the Enterprise Vault servers running an Exchange Journaling task. The Adapter acts as a gateway, changing the contents of mail messages as they cross the boundary from the main flow of mail messages into the archive. The gateway provides unprotected versions of the protected content of email messages or attachments, in supported formats, allowing that content to be stored and indexed in an unencrypted form. It also provides indexable metadata that describes the original protection of the message.

When the Adapter is installed, two distinct components are involved, the Filter and the Gateway Service. Figure 1 illustrates the association between the Enterprise Vault server, the Exchange Journaling task, the Filter, and the Gateway service.

Figure 1 – Filter and Gateway service interaction with EV Exchange Journaling



Upon installation, the Adapter is fully functional and running. However, it contains support for several security services that can be used independently, each with its own prerequisites, so none are enabled by default. Instead, after installation, the Configuration Tool can be used to enable and configure the appropriate protection types and other relevant security settings.

Gateway Service and Statistics Ports

The **Gateway Service** listens on TCP Port 7888 for requests coming from the Filter. The **Gateway Statistics Service** gathers performance statistics which listens on Port 7889. These ports can be changed if some other program is already using them.

Conclusion

In this whitepaper we have discussed the security aspects of the Enterprise Vault Adapter for Secure Messaging and Rights Management. We discussed how the adapter securely plugs into the archiving stream to decrypt message contents so they can be indexed. We also illustrated how the Filter and Gateway service interact with the Enterprise Vault Exchange Journaling Task.

Below is a list of the other Security Model topics in this series that may be of interest.

- Enterprise Vault 8.0 Security Model for Discovery Accelerator 8.0
- Enterprise Vault 8.0 Security Model for Compliance Accelerator 8.0
- Enterprise Vault 8.0 Security Model for Automatic Classification Engine 8.0
- Enterprise Vault 8.0 Security Model for Microsoft Exchange Archiving
- Enterprise Vault 8.0 Security Model for File System Archiving
- Enterprise Vault 8.0 Security Model for SMTP Archiving
- Enterprise Vault 8.0 Security Model for Microsoft Sharepoint Archiving

About Symantec

Symantec is a global leader in providing security, storage and systems management solutions to help businesses and consumers secure and manage their information. Headquartered in Cupertino, Calif., Symantec has operations in 40 countries. More information is available at www.symantec.com.

For specific country offices and contact numbers, please visit our Web site. For product information in the U.S., call toll-free 1 (800) 745 6054.

Symantec Corporation
World Headquarters
20330 Stevens Creek Boulevard
Cupertino, CA 95014 USA
+1 (408) 517 8000
1 (800) 721 3934
www.symantec.com