M86 SECURITY™

SYSTEM REQUIREMENTS

HARDWARE

Processor	Pentium 4 class processor
Memory	512MB (NTFS) or higher
Operating System	Windows Server 2003 or Windows XP Professional (32-bit only)
Database (Optional)	Microsoft SQL 2005 or SQL Express 2005
	Recommended: M86 MailMarshal SMTP version 6.4.5 or later OR other compatible email gateway with S/MIME routing capabilities

SUPPORTED ENCRYPTION STANDARDS

HARDWARE

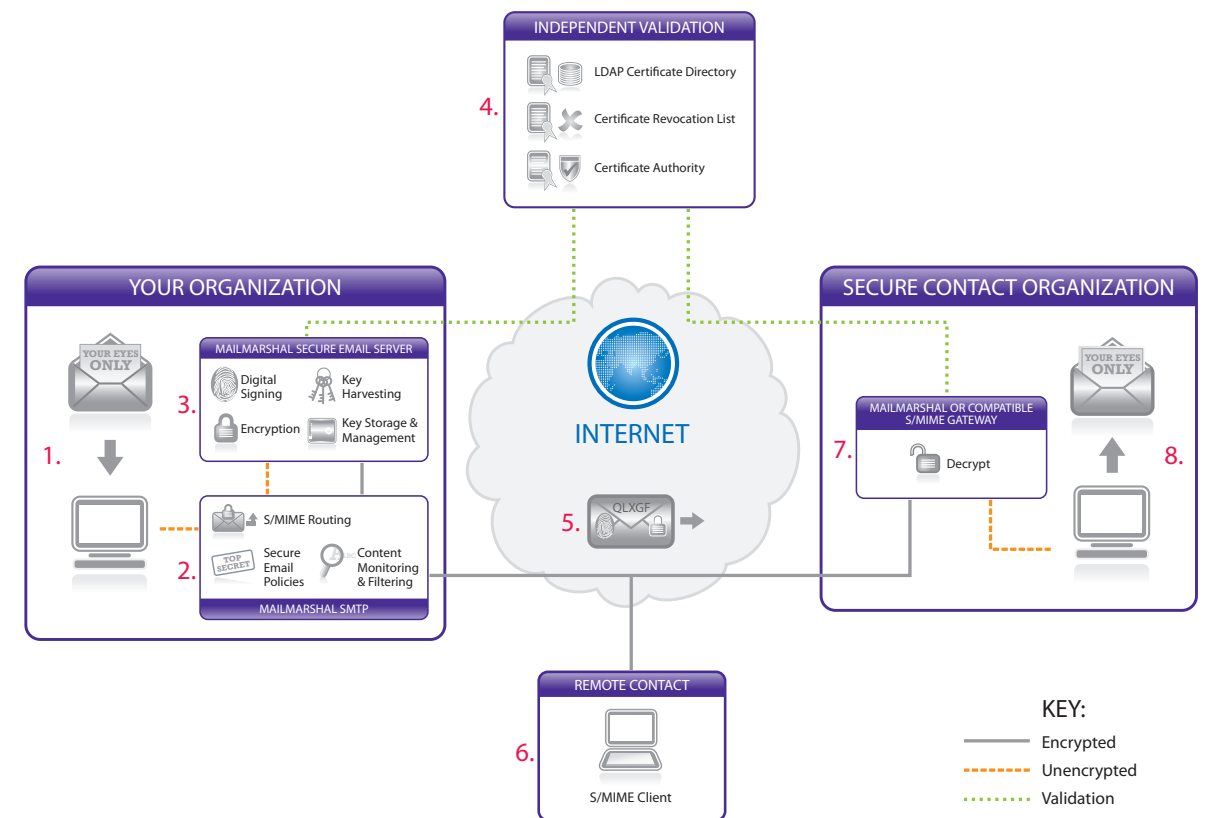|	
Signing algorithms	RSA with MD5 and SHA-1
Encryption levels	RC2 40, 64 and 128-Bit, DES CBC 56-Bit and DES EDE3 CBC (triple DES 168-Bit)
Key pairs	512, 1024, 2048, 4096-Bit (Windows 2000/XP High Encryption is required for options over 512-Bit)
Key transport	PKCS#12 (personal information exchange message syntax)
Other standards	RFC2311, RFC2312 and RFC1422 (X.509 v1, v3 S/MIME certificate compliance), PKCS#1 (RSA encryption standard), PKCS#2 (password based encryption standard), PKCS#7 (cryptographic message syntax standard) and Base 64 encoded PKCS#7 / X.509
Accreditation	Secure Electronic Environment (S.E.E.) New Zealand Government accredited

M86 MailMarshal Secure Email Server
Policy-based Email Encryption and Digital Signing for Data Leakage Prevention and Regulatory Compliance

M86 MailMarshal Secure Email Server is a secure email solution, ensuring that organizations can communicate effectively without exposing sensitive or private information. It provides enhanced Public Key Infrastructure with advanced functionality for key generation, certificate harvesting, automated maintenance and centralized authentication directories. M86 MailMarshal Secure Email Server automatically enforces security policies and leverages deep content inspection technology to achieve regulatory compliance and protect against data leakage.

KEY FEATURES

- Dedicated solution providing policy-based email encryption and digital signing
- Public Key Infrastructure (PKI) with S/MIME encryption standards up to Triple-DES (168-bit) strength cryptography
- Works with M86 MailMarshal SMTP, or other S/MIME gateways, to provide content monitoring and filtering of confidential messages, ensuring compliance with industry requirements and government legislation
- Secure certificate generation technology and comprehensive support for third-party Certificate Authorities
- Extensive certificate management including support for Certificate Revocation Lists, automated certificate harvesting, sorting and storage
- Centralized certificate updates through directory (LDAP) synchronization with established authentication servers
- Extensive reports and auditing for secure communications
- Cost effective and easy to deploy with almost zero ongoing manual administration

ABOUT M86 SECURITY

M86 Security is a global provider of Web and messaging security solutions and the industry's largest vendor of Web security appliances. The company delivers comprehensive protection to more than 21,000 customers and over 16 million users worldwide and has the expertise, product breadth and technology to protect organizations from both current and emerging threats. M86's appliance, software and cloud-based solutions leverage real-time threat data to proactively secure customers' networks from malware and spam; protect their sensitive information; and maintain employee productivity. The company is based in Orange, California with international headquarters in London and offices worldwide. For more information about M86 Security, please visit www.m86security.com.

TRY BEFORE YOU BUY
M86 Security offers free product trials and evaluations. Simply contact us or visit **www.m86security.com/downloads**

M86 SECURITY™

Corporate Headquarters
828 West Taft Avenue
Orange, CA 92865
United States

Phone: +1 (714) 282-6111
Fax: +1 (714) 282-6116

International Headquarters
Renaissance 2200
Basing View, Basingstoke
Hampshire RG21 4EQ
United Kingdom

Phone: +44 (0) 1256 848080
Fax: +44 (0) 1256 848060

Asia-Pacific
Millennium Centre, Bldg C, Level 1
600 Great South Road
Ellerslie, Auckland, 1051
New Zealand

Phone: +64 (0) 9 984 5700
Fax: +64 (0) 9 984 5720

Version 09/29/09

KEY BENEFITS

Security and Compliance

Enables confidential communication
Ensures the content of confidential emails and attachments remain private between you and your intended recipient. No other party can access the content of the message

Confirms email sender's identity and integrity of message content
Authenticates the identity of the email sender via Digital Signing and verifies that the message is genuine and has not been tampered with. Prevents email spoofing or forgeries where a third party can fake the address of the sender and impersonate them. Also ensures that a third party has not altered the content of a message, changing its meaning or critical details, before it has reached the recipient.

Ensures consistent application of security policies
Automatically manages encryption and decryption according to your organization's policy and compliance standards. As a centralized, server-based solution, no confidential message that needs to be encrypted can be accidentally or intentionally transmitted in an unencrypted format. This removes the potential for human error and ensures that policies are always adhered to.

Meets compliance requirements
Through integration with M86 Security's content monitoring and filtering solutions, M86 MailMarshal Secure Email Server can analyze encrypted message content to confirm that communications comply with regulatory practices and meet organizational policies.

Provides peace of mind
Offers optional levels of encryption strength up to Triple-DES 168-bit. This level of security ensures that it is nearly impossible for even the most determined of attackers to break your encryption.

Ease-of-Use and Automation

Allows centralized control of encrypted communication
As a server-based solution at the email gateway, M86 MailMarshal Secure Email Server provides a single point of control to manage encryption for your entire organization. This makes email encryption easier to deploy and maintain. It also reduces training requirements and ensures that all outgoing and incoming encrypted communications comply with organizational policies.

There is no requirement for any additional software for workstations or end user training. The entire process is automated and transparent for end users, requiring no effort on their part.

Self-maintaining with low Total Cost of Ownership
M86 MailMarshal Secure Email Server automatically searches for, harvests, sorts and stores relevant digital certificates for later use. Depending on who a specific email message is addressed to, M86 MailMarshal Secure Email Server will select and apply the relevant public key for the appropriate recipient.

Streamlines administration and automatically maintains secure email best practices
M86 MailMarshal Secure Email Server takes full advantage of information-rich certificates to provide automatic updates and notifications when certificates/keys are due to expire. This allows for keys to be set to automatically expire periodically without introducing undue administrative burden. M86 MailMarshal Secure Email Server can automatically retrieve and deploy updated/replacement certificates from centralized servers via Lightweight Directory Access Protocol (LDAP).

Via LDAP synchronization, M86 MailMarshal Secure Email Server is able to automatically update contact details and credentials with secure email partners.

Versatility and Integration

Compatible with other S/MIME gateway solutions
M86 MailMarshal Secure Email Server provides easy integration with other organizations. It can work with third party S/MIME gateways that are capable of policybased email routing.

Works with independent Certificate Authorities
M86 MailMarshal Secure Email Server complies with industry standards for certificate validation, allowing it to automatically communicate with major Certificate Authorities.

Easily operates with standard S/MIME clients such as Microsoft Outlook
M86 MailMarshal Secure Email Server provides gateway-to-gateway and gateway-to-desktop encryption delivery options, allowing you to securely communicate with organizations and individuals.

SMARTER, MORE ADVANCED PUBLIC INFRASTRUCTURE

Using email to communicate confidential information is not ideal. It is an open medium and vulnerable to interception and manipulation.

Public Key Infrastructure (PKI) provides a robust system for securing confidential data. It also provides a high degree of trust that verifies parties are who they claim to be and that messages arrive intact and unaltered.

The challenges with PKI in a business environment are scalability and ongoing management requirements. When multiple secure email partners are involved the complexities and costs of managing certificates and authentication have long been touted as major shortcomings which detract from the viability of PKI for secure enterprise email.

M86 MailMarshal Secure Email Server is specifically designed to address these challenges and offers a solution that is cost effective, simple to operate and can streamline any ongoing maintenance tasks.

IDEAL SOLUTION FOR SECURE BUSINESS COMMUNICATION

M86 MailMarshal Secure Email Server is ideally suited to environments where secure communications need to be established and maintained between groups of organizations with flexibility for changing membership and credentials.

This can apply to a range of scenarios, including:

- Between healthcare providers and insurance companies sharing confidential patient records and medical information
- Between manufacturing and construction contractors working on sensitive project plans, schedules, budgets and designs
- Between government agencies sharing private information or collaborating on government business
- Between legal service providers and corporate customers working on contracts, agreements and other confidential legal material
- Between organizations and external experts or consultants such as accountants, stock brokers or business analysts sharing privileged information

In these scenarios, a platform of trust needs to be established with organizations that must communicate, collaborate and share information securely. A workable solution needs to provide versatility and flexibility to enable other organizations or specialized contributors to easily join the secure network without undue costs.

M86 MailMarshal Secure Email Server is the perfect and proven solution for this requirement.

TECHNICAL OVERVIEW

Content Monitoring and Filtering

M86 MailMarshal Secure Email Server is designed to work with M86's email content security solution M86 MailMarshal SMTP and can also be configured to work with M86 MailMarshal for Exchange. Integration with M86 MailMarshal SMTP allows full content analysis of encrypted communications including text, attachments, anti-virus and anti-spyware scanning as well as pornographic image detection. This means M86 MailMarshal Secure Email Server can block threats in encrypted messages and protect against legal liability and inappropriate content.

Message Archiving

M86 MailMarshal Secure Email Server can classify and store encrypted messages along with relevant keys to ensure that messages can be decrypted later and audited for compliance purposes.

Policy-Based Security

When used with M86 MailMarshal SMTP (or M86 MailMarshal for Exchange), M86 MailMarshal Secure Email Server can use message cues to trigger policies for automated encryption and/or signing before delivery.

For example, M86 MailMarshal Secure Email Server can use the presence of a phrase such as "Private & Confidential" in any part of the message body, subject line or attachment(s) to trigger automatic encryption. M86 MailMarshal Secure Email Server can also link this condition with additional conditions such as the sender's rights to transmit outbound confidential material and the intended recipient's authorization to receive confidential messages.

M86 MailMarshal Secure Email Server will automatically select the appropriate public key needed to encrypt the message for the intended recipient. You can define encryption policies around additional requirements.

This can include minimum standards for cryptography strength and levels of trust for certificates such as reference checks through Certificate Authorities or Certificate Revocation Lists.

Certificate Management

M86 MailMarshal Secure Email Server automatically detects, harvests and catalogs digital certificates. All a new secure email contact needs to do is email you a digitally signed message and M86 MailMarshal will retrieve and store the attached certificate. You can also use trusted authentication servers or independent Certificate Authorities to validate certificate credentials.

M86 MailMarshal Secure Email Server makes full use of information-rich certificates to store data such as update locations, CRL locations, and expiry dates. Five days prior to expiry of a certificate M86 MailMarshal Secure Email Server will automatically retrieve a replacement certificate (if available) and notify network administrators via email.

Certificate Revocation List (CRL) support enables M86 MailMarshal Secure Email Server to check, if certificates have been revoked by their issuer and are therefore invalid or not to be trusted.