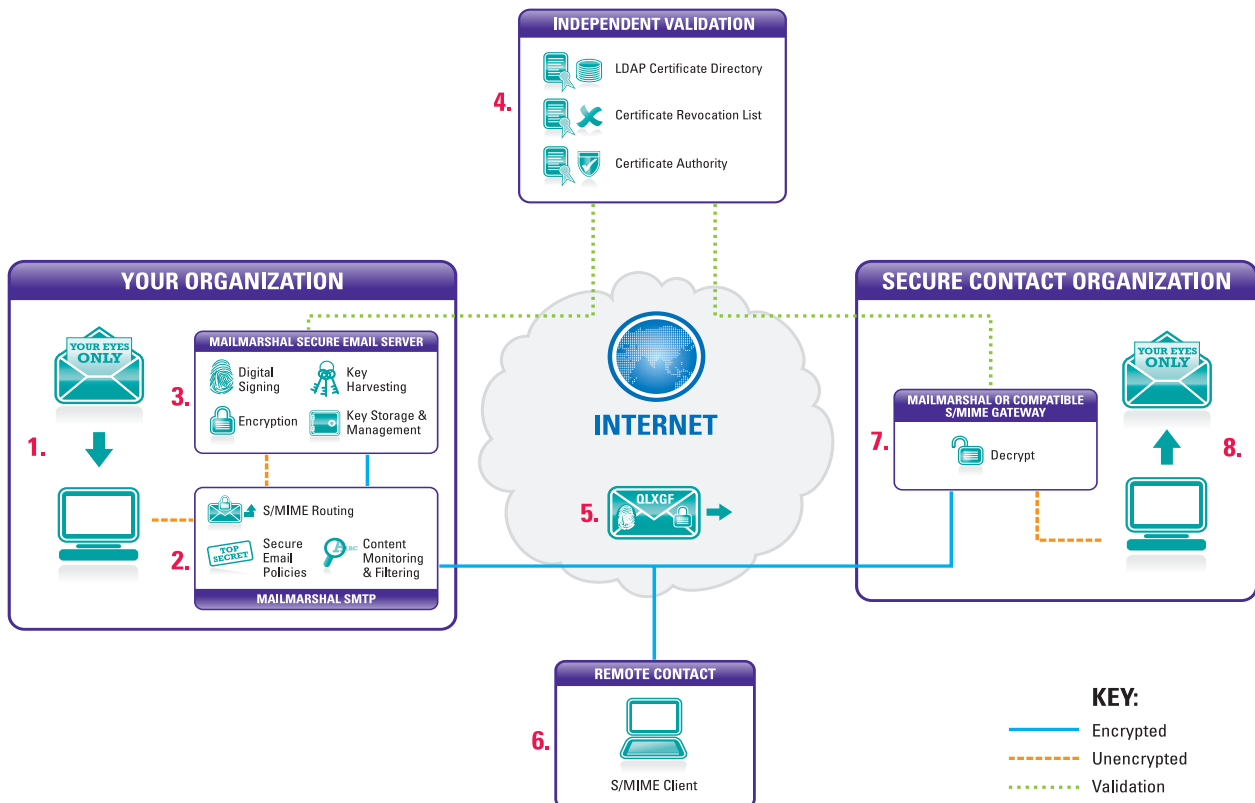


MailMarshal Secure Email Server

Policy-based email encryption and digital signing for data leakage prevention and regulatory compliance

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. MailMarshal Secure Email Server automatically enforces security policies and leverages deep content inspection technology to achieve regulatory compliance and protect against data leakage.



MailMarshal Secure Email Server is a flexible, powerful email encryption and digital signing solution. Once it is installed at the email gateway, it automatically manages encryption for all outgoing and incoming messages and can maintain security credentials for encryption contacts via centralized server updates.

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 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

MailMarshal Secure Email Server

Policy-based email encryption and digital signing for data leakage prevention and regulatory compliance

KEY BENEFITS

SECURITY & 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 Marshal's content monitoring and filtering solutions, 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 even the most determined attempts to break encryption will take enormous effort and resources.

EASE-OF-USE & AUTOMATION

Allows centralized control of encrypted communication As a server-based solution at the email gateway, 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 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, 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 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. MailMarshal Secure Email Server can automatically retrieve and deploy updated/replacement certificates from centralized servers via Lightweight Directory Access Protocol (LDAP).

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

VERSATILITY & INTEGRATION

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

Works with independent Certificate Authorities 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 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 KEY 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.

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.

MailMarshal Secure Email Server

Policy-based email encryption and digital signing for data leakage prevention and regulatory compliance

IDEAL SOLUTION FOR SECURE BUSINESS COMMUNICATION

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.

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

TECHNICAL OVERVIEW

Content Monitoring and Filtering

MailMarshal Secure Email Server is designed to work with Marshal's email content security solution MailMarshal SMTP and can also be configured to work with MailMarshal for Exchange. Integration with 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 MailMarshal Secure Email Server can block threats in encrypted messages and protect against legal liability and inappropriate content.

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

For example, 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. 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.

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 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 MailMarshal will retrieve and store the attached certificate. You can also use trusted authentication servers or independent Certificate Authorities to validate certificate credentials.

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 MailMarshal Secure Email Server will automatically retrieve a replacement certificate (if available) and notify network administrators via email.

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

MailMarshal Secure Email Server

Policy-based email encryption and digital signing for data leakage prevention and regulatory compliance

TRY BEFORE YOU BUY.

Marshal offers a free 30-day trial of MailMarshal Secure Email Server.

Please visit us at www.marshal.com and arrange a complimentary trial.

For best results we recommend working with one of our certified technical sales consultants to identify the ideal solution for your organization's secure email requirements.

SYSTEM REQUIREMENTS

Processor - Pentium 4 class processor

Memory - 512MB RAM or higher

Storage - 10GB HDD (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 – MailMarshal SMTP version 6.4.5. or later OR other compatible email gateway with S/MIME routing capabilities

SUPPORTED ENCRYPTION STANDARDS

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

CONTACT MARSHAL

Europe, Middle East & Africa

Marshal Limited,
Renaissance 2200,
Basing View,
Basingstoke,
Hampshire RG21 4EQ
United Kingdom

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

Email: emea.sales@marshal.com

Americas

Marshal, Inc.
5909 Peachtree-Dunwoody Rd
Suite 770
Atlanta
GA 30328
USA

Phone: +1 404-564-5800
Fax: +1 404-564-5801

Email: americas.sales@marshal.com

Asia-Pacific

Marshal Software (NZ) Ltd
Suite 1, Level 1, Building C
Millennium Centre
600 Great South Road
Greenlane, Auckland
New Zealand

Phone: +64 9 984 5700
Fax: +64 9 984 5720

Email: apac.sales@marshal.com

info@marshal.com | www.marshal.com

MARSHALTM
Secure. Protect. Comply.