Secure Your Emails in Any Platforms, Anytime, Anywhere

SecureAge

What is SecureAge SecureEmail?

SecureAge SecureEmail, one of the core components of SecureAge Security Suite, is the perfect solution to counteract imminent email threats. It ensures email's authenticity and privacy by signing and encrypting email transparently based on IETF S/MIME (RFC 3851) standard.

What Makes SecureAge SecureEmail Unique?

1. Policy Based Security Control

SecureAge SecureEmail's powerful policy based security control allows intuitive labeling of sensitive email information. It controls how each labeled email should be treated when transmitted, stored, forwarded and replied to. Email classification labels like "Confidential", "Secret" and "Protected" can be easily defined by using a software configuration tool. These labels can be added to email subject line for convenient viewing in email list view. They can even be added to email MIME header so that Mail Server (MTA) could apply additional policy control on such emails.

2. Seamless Integration with Most Email Applications

SecureAge SecureEmail works seamlessly with most email platforms like Lotus Notes and Microsoft Outlook. Organizations can readily deploy SecureAge SecureEmail without having to change their current email software or use a different email client. They can even incorporate their own secure email business logics by adding email security features like email security classification and secure email policy rules to their email communication.

3. Supports Digital Signature and Encryption with Unlimited Key Length

SecureAge SecureEmail protects all transmitted email messages and attachments by using unlimited key length RSA algorithms, 168-bit Triple-DES, and 256-bit AES encryption. For data to be transmitted in a fully secured environment, it is important for the digital signature and encryption key length to be large enough to resist any possible brute force attack.

4. Supports Unlimited Key History

SecureAge SecureEmail ensures that all archive emails can still be decrypted with every future renewal of encryption keys. It enables access to unlimited key history and automatically selects the correct key for users to decrypt any past email of their choice.

5. Provides Migration Tool to Re-encrypt Old Emails with New Encryption Key

SecureAge SecureEmail's powerful migration tool allows IT administrator to use the old key for a one time migration. After the migration, the emails in the email server and the archive folders will be encrypted with the new keys and the old key can be immediately discarded.

6. Supports S/MIME V2, V3 and V3.1 Email

SecureAge SecureEmail uses S/MIME (Secure/Multipurpose Internet Mail Extensions) standards to provide a consistent way to send and receive email messages and attachments securely. It also supports S/MIME v3.1 that comes with email compression capability. It significantly reduces the size of standard email messages and attachments by as much as 5 times and greatly accelerates the data encryption processing time.

7. Supports Email Header Integrity Protection

SecureAge SecureEmail securely signs and encrypts both email content and email header to ensure email integrity. It will first check and verify the integrity of the encrypted email header by matching it with the email headers located in the inbox mail folder view. It will then alert the recipient if any discrepancies are found.

8. Supports User Defined Encryption Algorithms

SecureAge SecureEmail supports user defined encryption algorithms. To further boost the security strength of their corporate email system, government regulators, military or organizations can choose to incorporate their proprietary encryption algorithms into SecureAge SecureEmail, with or without the standard encryption algorithms.

9. SecureAge SecureEmail Digital Rights Management (DRM)

SecureAge SecureEmail DRM is an extension of SecureAge SecureEmail. It allows email senders to stipulate additional email permissions and impose certain restrictions on the recipients when accessing the email. It can basically restrict the recipients from copying, saving, printing, screen capturing, replying and forwarding the email. Email senders can even define the email's expiry date to forbid the recipients from viewing the email contents once it expired and all the expired emails will be deleted permanently.

Key Features

1. Automatic Retrieval of Recipients' Digital Certificate

SecureAge SecureEmail will automatically perform a directory lookup of your recipients' certificates using a LDAP (Lightweight Directory Access Protocol) repository or Microsoft Active Directory. After locating your recipients' certificates, it will automatically import these certificates to your personal certificate store for future use.

2. Supports Certificate Revocation Checking

SecureAge SecureEmail's certificate revocation checking capability will automatically check the validity of the digital certificates every time they are used. The Certificate Revocation List (CRL) of each certificate is automatically updated to ensure their validity. If any of the certificates is found to be revoked, it will automatically retrieve the new certificate and replace the old version.

3. Supports Online Certificate Status Protocol (OCSP)

SecureAge SecureEmail's OCSP enables online certificate validity checking for timely revocation information. Digital certificates are considered as valid only after OCSP responder provides a positive response to the status request issued by SecureAge client.

4. Supports SecureAge Management Server

SecureAge SecureEmail supports SecureAge Management Server which allows enterprises to centrally control all SecureAge software deployment. It provides central policy control, audit log and key management for SecureAge SecureEmail.

5. Helps Achieve Regulatory Compliance

SecureAge SecureEmail is able to help your organization to fulfill regulatory compliances like California Security Breach Information Act (Senate Bill 1386), Sarbanes-Oxley Act of 2002 (SOX), Health Information Portability and Accountability Act of 1996 (HIPAA) and the Gramm-Leach-Bliley Act of 1999 (GLBA).

Need More Information?

General Enquiry: contactus@secureage.com
Technical Support: support@secureage.com
Public Relations / Marketing: pr@secureage.com

www.secureage.com
www.lockcube.com

Asia Pacific
SecureAge Technology Pte Ltd
20, Ayer Rajah Crescent,
#09-13, Technopreneur Centre,
Singapore 139964

Japan
SecureAge K.K.
Barbizon 18, 7F
5-18-18 Shirokanedai
Minato-ku, Tokyo 108-0071
Japan

North America
SecureAge Technology Inc
3 Twin Dolphin Drive Suite 150
Redwood City CA 94065
U.S.A.