# SecureAge

SecureWebmail

To stay ahead of competition, mobile employees need to get hold of the most updated business information and expedite critical business decision promptly. An instantaneous way of ensuring the timeliness of information exchange is using web-based email. Over the years, enterprise webmail has increasingly gained popularity among large enterprises due to its easy maintenance, support and upgrade. Unlike email client, it does not require frequent software fixes or patches or upgrades that can be very tedious and costly to maintain. Therefore more and more enterprises are gradually migrating from standard email client to webmail solution.
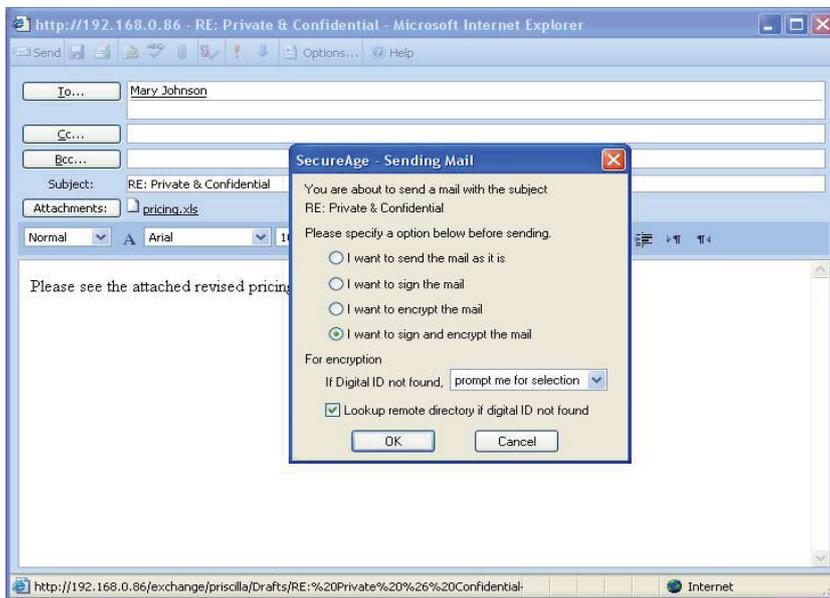
The trend of using webmail as an indispensable communication tool for organizations is apparently increasing. But, widespread treacherous cyber risks like unwanted tampering or interception has increased organizations' concern over webmail confidentiality. They are beginning to realize the importance of implementing a robust webmail security solution to counteract such perilous webmail threats.

In the past, standard solution can only protect S/MIME enabled email client. Some organizations, unable to find a solution to protect webmail system, are hesitant to migrate from standard email client to webmail solution. But this issue is no longer a concern with SecureAge SecureWebmail.

SecureAge SecureWebmail is an end-to-end webmail security solution that comes with state-of-the-art authentication, encryption and digital signature capabilities. It transparently signs and encrypts webmail based on S/MIME standard to ensure it is securely exchanged among all mainstream webmail applications.

Apart from SecureAge SecureWebmail, SecureAge client also comes with another core component, SecureAge SecureEmail. SecureAge client provides organizations with the flexibility of securing either the email or webmail system or both, depending on their needs. By deploying SecureAge client, they no longer need to purchase two separate solutions just to secure both email and webmail systems. Organizations that have already deployed SecureAge SecureEmail can easily extend SecureAge SecureWebmail security if they wish to migrate to webmail platform. This will help them to reduce their investment cost significantly.

Product Features

Seamless Integration With Most Email Applications

SecureAge SecureWebmail works seamlessly with most enterprise webmail system like Outlook Web Access, Domino Web Mail and Sun Messaging Servers. Optional support to public webmail system like Hotmail and Yahoo Mail are also available. This means that it can be readily deployed to your current enterprise webmail system without having to modify it. SecureAge SecureWebmail also provides additional secure email features apart from the standard S/MIME capability. It can help organizations to add email security features likeemail security classification and incorporate their own secure email business logics.

Support Digital Signature and Encryption with Unlimited Key Length

SecureAge SecureWebmail supports unlimited key length RSA algorithms, 168-bit Triple-DES, and 256-bit AES encryption to ensure that your transmitted webmail messages and attachments are fully secured and not tampered with. When strong algorithms and larger keys are used, attackers will need to spend more computing resources and longer time to decipher the encrypted data. Currently, Triple-DES, AES (Advanced Encryption Standard) and RSA encryption algorithms are considered to be strong enough to ward off any brute force attack.

Automatic Retrieval of Recipients' Digital Certificate

SecureAge SecureWebmail comes with the certificate and key management features that allow you to manage certificates easily and efficiently. When sending an encrypted webmail, it automatically lookup for your recipient's certificate via the LDAP (Lightweight Directory Access Protocol) repository or active directory.

Once found, it will automatically import the certificate to your personal certificate store. SecureAge SecureWebmail also provides the ability to expand your group emailing list. This is especially useful when you want to send encrypted email to a few recipients listed in a group email address. SecureAge SecureWebmail automatically traces the individual encryption key of every recipient and then encrypts the webmail using their respective keys. This ensures that only the recipients listed in the group email address are privy to the webmail content.

Support S/MIME V2, V3 and V3.1 Email Compression

SecureAge SecureWebmail supports S/MIME (Secure / Multipurpose Internet Mail Extensions) security for webmail access to enterprise email system based on Exchange, Lotus Domino and Sun Messaging Servers. S/MIME provides cryptographic security services to encrypt and decrypt webmail, thereby ensuring authentication, message integrity, non-repudiation and dat confidentiality. SecureAge SecureWebmail also supports the latest S/MIME v3.1 with email compression capability. With this compression feature, standard webmail message and attachment (like word document, excel worksheet and text file) can significantly reduced by as much as 70 percent. A greatly reduced message size will speed up the data processing time during the encryption stage and the network transmission in an environment with slower network bandwidth.

Support Unlimited Key History

SecureAge SecureWebmail enables access to unlimited key history and automatically selects the correct key for users to decrypt any past email of their choice. It resolves the problem faced by most organizations whereby users no longer able to decrypt past emails due to renewal of encryption keys. Therefore, with SecureAge SecureWebmail, you can now have a peace of mind without worrying about the inability to retrieve old mails

Support Certificate Revocation Checking

SecureAge SecureWebmail comes with a comprehensive CRL (Certificate Revocation List) checking and automatic updating capability. All the digital certificates are automatically checked for their validity. If any certificate is found to be revoked, it will automatically locate the newer certificate and replace the old certificate with the new one.

Support Online Certificate Status Protocol (OCSP)

SecureAge SecureWebmail also provides online certificate revocation validity checking via OCSP. It is an ideal option for organizations that require more timely revocation information. Digital certificates are considered as valid only after OCSP responder provides a positive response to the status request issued by OCSP client.

Support User Defined Encryption Algorithms

SecureAge SecureWebmail supports user defined encryption algorithms. To further boost the security strength of their enterprise webmail system, government regulators or organizations can choose to incorporate their own developed proprietary encryption algorithms into SecureAge SecureWebmail, together with or without the standard encryption algorithms.

SecureAge® SecureEmail

Apart from securing webmail, SecureAge client also provides SecureAge SecureEmail solution to transparently sign and encrypt email based on S/MIME standard. It works seamlessly with most email platforms like Lotus Notes, Microsoft Outlook, Sun Messaging Server, Outlook Express, Netscape Messenger and QualComm Eudora.

Support Smart Card and USB Token

SecureAge SecureWebmail supports smart card or USB token to enable the best PKI security with tamper resistance and two-factor protection. Digital certificates, when are used in conjunction with smart card and USB token, will provide the highest security in controlling access to sensitive email messages and attachments.

Help Achieve Regulatory Compliance

SecureAge SecureWebmail is able to help your organization to fulfill regulatory compliances like Sarbanes-Oxley Act of 2002 (SOX), Health Information Portability and Accountability Act of 1996 (HIPAA) and the Gramm-Leach-Bliley Act of 1999 (GLBA). It helps to meet the requirement under HIPAA and GLBA by encrypting webmail messages and attachments to protect the confidentiality of information, whether during transmission over the Internet or stored in the desktop / laptop / email server. It also helps your organization to comply to the legislations of SOX with its authentication and encryption capabilities.

Key Features

. Support PKCS #1, #5, #7, #8, #9, #10, #11, #12 standards.

. Support MD2, MD5 and SHA-1 hash functions.

. Support external PKI / CA for certificate based authentication and certificate validity checking.

. Provide full support for X.509 v3 and PKIX compliance extensions digital certificate format.

. Support key and certificate import / export via PKCS #12, DER and PEM formats.

. Support .pem, .der, .cer, .crt, .p12, .pfx, .p7m, .p7s and .p7z file formats.

. Support SecureAge® CA and many other public enterprise CAs.

. Interoperable with other commercial S/MIME compliance solutions.

. Support user account and certificate mapping.

. Support standard browser like Internet Explorer, Netscape and Firefox.

. COM APIs and DLL to provide integrated PKI support for external applications.