SECURE CONTENT APPLICATIONS

User-Level S/MIME Encryption

Overview

Public key encryption depends on consistent management of user keys and end-user compliance with encryption procedures whenever confidentiality is required. At the enterprise level, these requirements are difficult to meet consistently. Our User-Level S/MIME Encryption solution addresses both requirements by managing keys in Sentrion's LDAP key store and automatically applying user-level encryption actions through the Sentrion Message Processing Engine.

Audience

Government agencies, military and intelligence organizations, biotechnology firms, healthcare providers, financial services firms and any company that needs to maintain the confidentiality and verify the authenicity of email messages.

Key Features and Functionality Overview

A chain of trust is only as strong as its weakest link. In theory, the S/MIME public key protocol provides a very strong method for validating the authenticity and integrity of an email, verifying its sender, and encrypting its contents for the eyes of the intended recipient only.

The problem – and the reason S/MIME hasn't achieved wider adoption among companies that should be concerned about email security – is the two weak links. First, there's the issue of managing user keys, especially on the large scale required for an effective enterprise implementation. Second, everything depends on the ability and willingness of end users to take appropriate encryption actions on their own desktops, every time without fail. And if you've ever tried to get users to behave predictably, you've learned the true meaning of "weak link."

User-Level S/MIME Encryption removes the weak links from the chain of trust. It automatically encrypts and digitally signs outgoing email messages using the S/MIME standard, and it decrypts and verifies signatures on incoming messages. User keys are managed automatically in Sentrion's LDAP key store, eliminating the need for users to manage their own keys. There are no management hassles, and no need to use client-based mail agents to encrypt, sign, decrypt and verify messages – so messaging security never depends on users doing the right thing.

When an outgoing message requires confidentiality and authentication, User-Level S/MIME Encryption retrieves the appropriate sender and recipient keys from the key store in the LDAP directory, encrypts and signs the message, and routes it to its destination. When a message with encryption or a digital signature is received, the appropriate keys are retrieved for decryption and authentication, and the message is delivered to the recipient in clear text.

User-Level S/MIME Encryption:

- Lowers costs by eliminating end-user key distribution and training
- Ensures compliance with encryption and authentication policies
- Works transparently, without the need for web clients or plug-ins
- Interoperates with other email server and client implementations using the S/MIME Internet standard.

When the chain breaks, you lose control. Don't let that happen to your confidential assets, or to the privacy of your employees and clients. Eliminate the weak links and strengthen the chain of trust with User-Level S/MIME Encryption from Sendmail.