

SecureIT<sup>®</sup> gives you transparent and easy to use policy based S/MIME individual and domain signing and encryption of e-mail at the content security gateway.

#### SecureIT ensures that:

- **Message content remains confidential** during transmission over the public network
- **Recipients can be certain about the authenticity and integrity** of messages they receive
- **Control and management of the Public Key Infrastructure (PKI)** necessary for this process is maintained transparently at a single point

Encryption provides privacy for content as it passes across the public network. Digital signatures provide proof that a message is from who it appears to be from and that it has not been tampered with during transmission. But these processes can create problems like exposure to content threats, orphaned data that can't be decrypted, unauthorised transfer of confidential information, the complexity of managing and synchronising all the public and private keys necessary to run the process and the effort necessary to set up links.

SecureIT has two-way encryption/decryption & signing/signature verification to S/MIME standards at the gateway. This avoids the high cost, complexity, security pitfalls and reliance on end users associated with desktop solutions.

SecureIT requires only a single software installation and automates the process for establishing and maintaining links to other S/MIME gateways and individuals. This guarantees security policy is always applied consistently and makes the set up and operation of links transparent.

SecureIT can work stand-alone or in conjunction with popular policy-based content security engines. This helps to prevent damage from threats that might be hidden in the content of encrypted e-mail.

SecureIT has its own Certificate Authority software (licensed separately) that can be used to generate traditional RSA key pairs and Advanced Employee Certificates as used in Danish government S/MIME systems.

SecureIT provides encryption with a choice of: RC2 (40, 64 and 128-Bit), DES (56-Bit), Triple DES (168-Bit) and AES algorithms with X9.31 PRNG.

Clear and opaque signing using RSA with MD5, SHA-1 & SHA-2 are supported.

SecureIT supports X.509 v3 certificates with key lengths of 512, 1024, 2048 or 4096-Bit. These can be issued by any of the major Certificate Authorities, or self-signed certificates generated by SecureIT. Import private keys from PKCS#12 containers and storage in an encrypted vault. Import Public key from P7C, P7B, CER, PEM and PKCS#12 containers and LDAP directories. It has full support for Certificate Revocation Lists (CRL) and automatically changes the status of revoked certificates.

#### SecureIT permits:

- More than one active certificate per domain
- Separate certificates for signing and encryption
- Different signing and encryption algorithms for each link
- Multiple internal domains/users with their own certificates, proxy signing
- Automatic retrieval of replacements for expired public certificates
- Re-encryption of messages after content checking for secure delivery
- Management of individually encrypted messages through its Key Guardian system
- Production and verification of triple wrapped messages
- Intelligent handling of external List Server messages
- Annotation of message From: and Subject fields to show secure arrival
- S/MIME v3.1 concealment of To, From, Subject and other MIME headers
- Outbound subject line commands select policy & change sender address
- Use of keywords in the message body, attachments or subject line to trigger policy
- Collection and optional activation of certificates from inbound messages
- Retention of before and after encryption copies for archive purposes
- Detailed reporting of signature verification and decryption status.
- Messages failing policy to be annotated (message text prepended and appended) or attached to an informative message.
- Automatic retry when outbound certificate problems occur
- Automated interoperability and policy testing against a standard reference system
- Integration with customised messaging systems via remote procedure call API

For large dynamic secure communities policy rules are stored, updated and disseminated centrally. SecureIT automates link set up and maintenance, and automatically obtains and caches certificates via LDAP and CRLs via HTTP. For smaller static secure communities SecureIT provides local policy and simplified manual link set up and maintenance.

SecureIT supports S/MIME v3 capabilities, and automatically selects the most secure algorithms compatible with each remote S/MIME gateway.



WHAT SecureIT DOES

HOW SecureIT WORKS

WHERE TO GET SecureIT

#### Who to Contact

Scientific Software and Systems Limited  
Telephone +64 4 917-6670  
e-mail: info@sss.co.nz  
web: <http://www.secureit.co.nz>

#### Licensing

SecureIT is licensed on a per user basis.



SecureIT can also be used by ISPs, ASPs and in cloud based SAAS to provide S/MIME messaging services.

SecureIT is a product of:  
Scientific Software and Systems Limited  
New Zealand  
Telephone +64 4 917-6670  
e-mail: info@sss.co.nz  
web: <http://www.secureit.co.nz>

