

## Secure Messaging Using Outband Mode Authentication

### Abstract

**[0036]** The present invention provides a secure messaging system (100) using outband mode authentication. The secure messaging system includes a security module (130,130a) that is pluggable into a messaging application (120,120a). The security module (130,130a) has a protocol (132) for allowing a user to enter a passphrase (134) for use with a symmetric cryptographic algorithm (80). In another embodiment, the protocol (132) allows the passphrase (134) to be split into a predetermined number of sub-passphrases (134a,134b,etc.); the passphrase (134) or at least one sub-passphrase (134a,134b,etc.) is operable to be sent to a recipient through an out-of-band channel (160), which is separate from an I/O channel (150) for sending the secure message. Each mode of the out-of-band channel (160) enhances security of the message by increasing the difficulty of re-assembling the sub-passphrases; in addition, each out-of-band mode constitutes a form of authentication.

**[0037]** FIG. 1 for publication.