Secure Your Email Communication

S/MIME certificates prevent impersonation, data leaks, phishing, fraud and tampering while increasing customer trust in your communication.

What is S/MIME?

S/MIME or Secure/Multipurpose Internet Mail Extensions is the leading standard for email signing and encryption. It enables users to encrypt and decrypt messages to each other preventing unauthorized access while signing messages with a validated identity preventing impersonation.

S/MIME Provides:

- **Protection Against Phishing** through sender authentication, lowering the risk of divulging private information.
- **Elimination of Man-in-the-Middle Attacks** through email encryption, preventing unauthorized access and alteration of emails in transit.
- **Prevention of Spoofing Attacks** with S/MIME's digital signatures, ensuring email integrity and sender identity.
- **Enhanced Data Security** through encryption, protecting sensitive email content from unauthorized access even in the event of a data breach.

Use Cases:

- Protecting privileged and sensitive communications
- Preventing intellectual property and trade secrets from compromise
- Securing customer financial data and preventing fraudulent payment requests
- Safeguarding patient health information

How It Works

- Order an S/MIME certificate with an organization or individual identity
- Undergo our audited, secure identity validation process
- Use our portal to send certificates to end users and devices

Organizations can enter into a Pre-validation Agreement that allows an organization to assume responsibility for retaining and validating identity evidence of employees or contractors within a company or organization enabling easy bulk ordering with just one validation process.

Ready to secure your email communication?
Contact SSL.com for a consultation or quote at sales@ssl.com or call 877-775-7328.