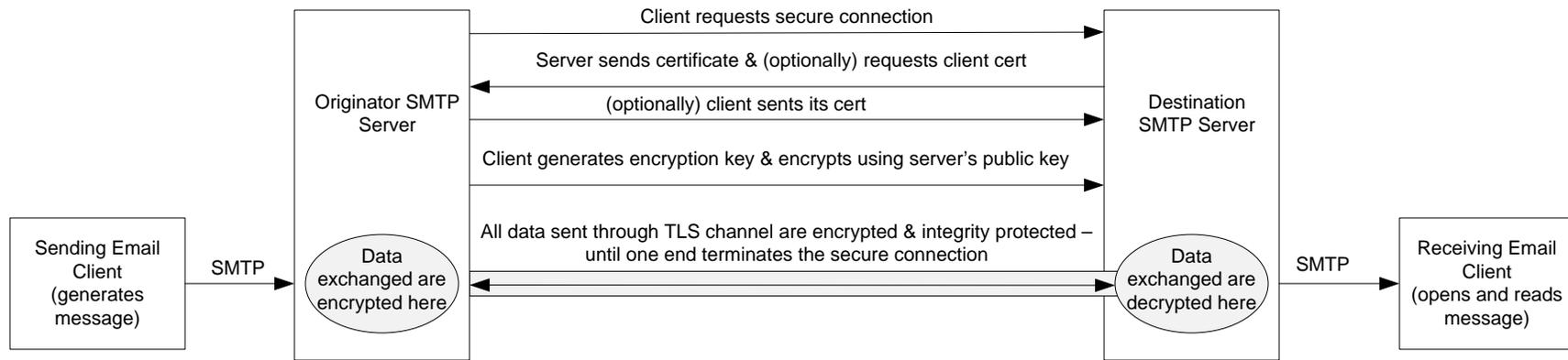
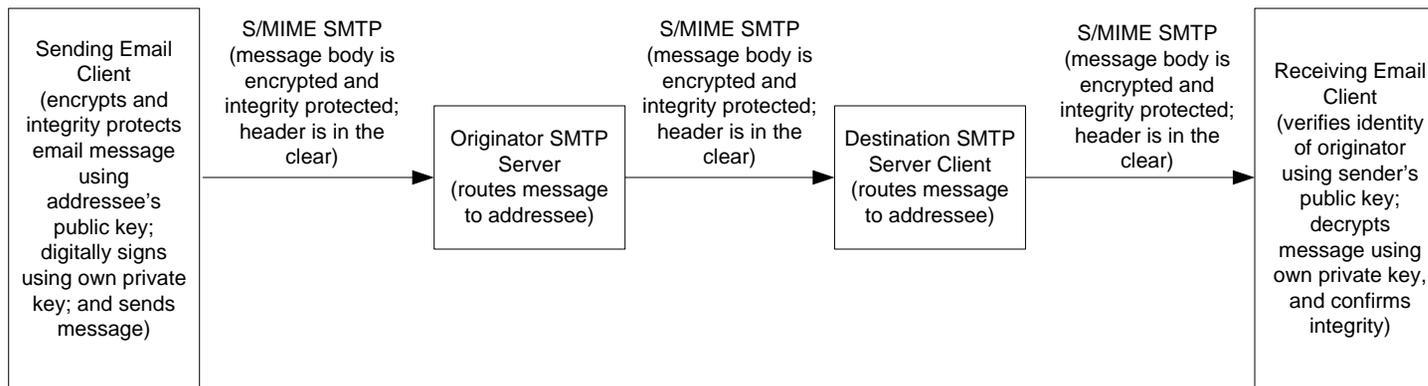


TLS with SMTP (without S/MIME)



NOTE: TLS authenticates the two ends of a connection, over which all data are encrypted between the two points. As illustrated here, the TLS channel is from the originating organization's SMTP server to the destination's SMTP server. Since Stage 1 meaningful use is organization-to-organization, that should be acceptable. It's possible to configure clients to use TLS to connect to the SMTP server as well. If this were done by both Originator and Destination organizations, we would have 3 TLS channels: 1) from sending email client to originator SMTP server, 2) from originator SMTP server to destination SMTP server; and 3) from Destination SMTP server to receiving email client.

SMTP with S/MIME



NOTE: S/MIME digitally signs the message and encrypts the message body using the recipient's public key. For stage 1 meaningful use, when the sender and recipient are "organizations" instead of individuals, this makes it quite similar to TLS with SMTP, except that the S/MIME message header (to/from, subject) are sent in the clear.

What I would like to see: S/MIME SMTP over TLS

