<< CP-1 >>

The uploaded file is not encrypted, as such can be easily intercepted and understood. After verifying SecStore's certificate, the client should request for SecStore’s RSA public key. The client then uses this public key to encrypt the file before sending it to SecStore. As only the SecStore knows the private key, intermediary routers and communication links will not be able to decrypt the data.

<< CP-2 >>

<< Helpful Stuff >>

<https://www.internetum.com/en/what-is-ssl-certificate-and-how-it-works/>