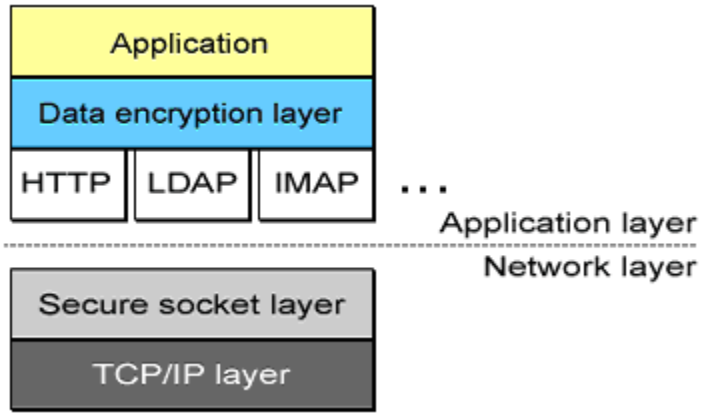
CryptoHeaven™
secure communications made easy

Transparent Data Encryption (TDE)

The biggest obstacles for people to use encryption technologies are additional burden and required level of expertise. The Transparent Data Encryption helps the user to focus on the communication content by working behind the scenes. When using software that incorporates Transparent Data Encryption, users need not think how to send information securely. Whether it is sending email, sharing documents, or chatting online, users do not have to perform additional steps; encryption is done for-the-recipient-eyes-only, seamlessly and transparently.



Data encryption layer runs above communication protocol layer and below application layer.

The data encryption layer runs above the application protocols and below the application itself to encrypt all data packets before they are passed down the communications stack and transferred over the Internet. The listed below client-server components provide vital data protection and enable**secured and encrypted central storage and messaging services**:

- **TDE client** transparently encrypts data with recipient's keys allowing the data to be viewed only by the designated recipient or designated groups. The encrypted data packets can be passed from client to server to client without possibility of decryption of the transmitted information by intruders or possibly compromised Internet devices / servers. Users need not trust the server integrity or the administrators for not reading their communication. All of the data encryption/decryption, integrity and authenticity checks are done on the client side. When transmissions arrive at the receiving client, they are guaranteed to be intact, un-intercepted and authentic.
- **TDE server** is typically a messenger and storage center, it need not possess any data encryption technology other than typically being SSL-enabled. All of the encrypted data packets which it receives directly from the client are either stored or passed along to another networked TDE server, or sent directly to the designated TDE client. The server acts as an encrypted packet delivery mechanism, or as a placeholder for the encrypted information packets forming an encrypted data storage center. This provides a "technological-bunker" for information.

Note the distinction between a secure data storage center where the word 'secure' usually refers to (a) physical security around the site/building, (b) firewalls preventing loose access to the servers, (c)

authentication mechanisms to ensure authorized access to information (stored in plain-text form). An encrypted data storage center is much more secure as it additionally protects information by storing it in an encrypted form. The necessary decryption keys to make the encrypted information legible are in the client's hands or optionally stored on the server encrypted with client's passphrase. The information is served to clients in its original encrypted form and it is the client's job to apply the decryption keys to make sense from the encrypted data.

Transparent Data Encryption is a high level technology. Transport Layer Security (TLS) securely transmits encrypted information between the sender and recipient without regard for integrity of internet servers and devices along the information path.

CryptoHeaven Secure Email uses Transparent Data Encryption on top of Transport Layer Security to provide total end-to-end security.

Next section: Client Accessible Encrypted Server Storage.

Read more about Transparent Data Encryption on Wikipedia.
Read more about Transparent Data Encryption on CryptoHeaven.