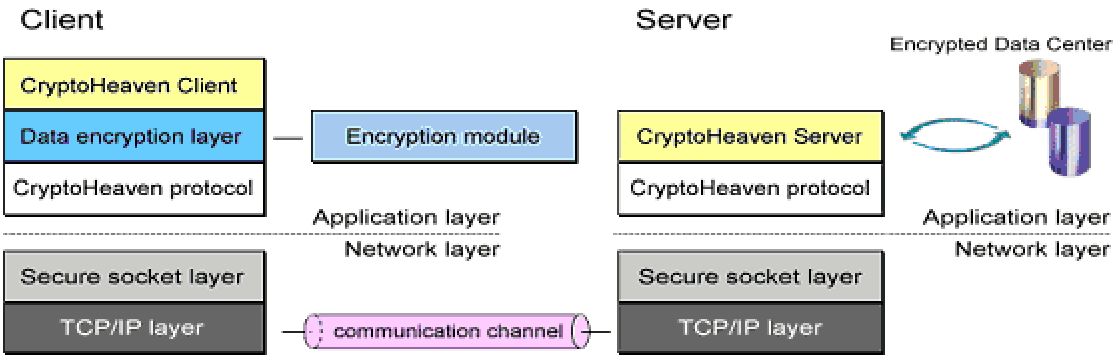
CryptoHeaven™
secure communications made easy

Client Accessible Encrypted Server Storage

By combining SSL and Transparent Data Encryption technologies into client-server type architecture we are able to create an encrypted data storage and messaging solution.



Simplified Client-Server architecture of an encrypted data heaven.

The CryptoHeaven client software passes data through the data encryption layer. This step essentially encrypts the data with recipient's public keys. Although there may be a varying hierarchy of symmetric keys involved, depending on the number of designated recipients and on the type of information being encrypted (email/chat/files/attachments/etc.), we will ignore them here for the purpose of simpler demonstration. With an application communication protocol the encrypted data is then formed into packets which flow down the client's network layer, across the communication channel, and up the network layer of the receiving server. The server recognizes the encrypted packets using the same application layer protocol that client used to format them. The server is not the end-receiver of the encrypted data, but rather a storage center or a messenger for other remote clients. The data encryption layer is not present on the server side as the server is not the final designated recipient of the data. Lacking decryption keys, server has no ability to read the contents of communications between sender and receiver although it is physically involved in storing or passing of encrypted information.

A high performance and scalable database system is used for storage of all data. This simplifies data management, improves performance, and easily accommodates system upgrades as well as provides robust backup capabilities. Scalability of the server application is ensured by a distributed architecture of servers connected in a mesh. For high capacity systems, connecting clients can be load balanced across all servers that are mutually connected in a common mesh. Mutually connected network of peer servers automatically ensures that all communication between clients flows uninterrupted.

Distributed server architecture makes CryptoHeaven a highly scalable solution and currently supports the following fully encrypted and secure services:

- Email
- Instant messaging and multi-user chat sessions
- Online file storage
- File sharing and document distribution
- Group shared file folders
- Group shared message boards

CryptoHeaven server network can run across heterogeneous platforms. Adding each additional server can be done without shutting down any part of the running network. Each new server that joins the mesh will automatically discover all nodes and make appropriate connections automatically. CryptoHeaven software features a pluggable encryption module for organizations to provide their own alternate cryptographic routines. Our in-house cryptographic module features 256-bit symmetric cipher Rijndael and 2048-4096 bit asymmetric RSA encryption. If required, a custom cipher suite with both a symmetric and asymmetric encryption capability can easily be used as a replacement.

CryptoHeaven Secure Email uses Encrypted Server Storage, Transparent Data Encryption, and Transport Layer Security to provide total end-to-end security.

Read more about Encryption on Wikipedia.
Read more about CryptoHeaven Security on CryptoHeaven.