Whispr - High Level Design

Braden Anderson, Austin Coelho, Nick Christensen

Processes

1. Registry Server
2. Client
3. Key Server
4. Message Server

Process Descriptions

1. The Registry Server is a tracker from which clients can request a list of active servers.

2. The Client process is the end user application implementing a user interface. The client will generate a private/public key pair, register its public key with the public key server, subscribe to a set of message groups, downloads a list of public keys for users it needs to send messages to, encrypt and decrypt messages, and relay messages through the message server.

3. The key server associates a unique username with a public key and assigns a user id to each user/key. The key server provides public keys to all authenticated users. The authentication step may be handled via username/password verification, or using the user's public key.

4. The message server is responsible for delivering encrypted messages to the intended recipients and managing rooms/channels. A copy of each message including the sender, recipient, group id, timestamp, and encrypted message body is stored in its database.

Feature Implementations

- End to end encryption is implemented by each user publishing a public key to the key server. The sending party uses the recipient's public key to encrypt the message. Only the holder of the private key can decrypt the message.

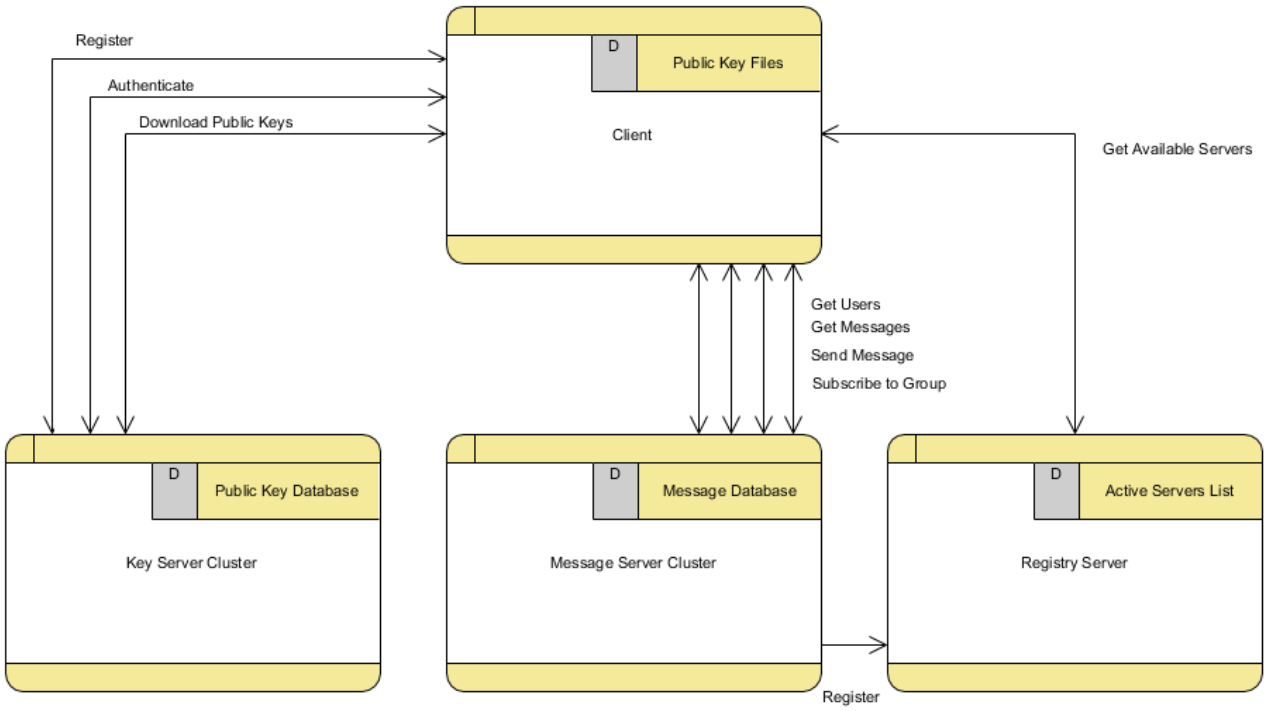
- User authentication occurs at the key server. Unauthorized users will not have access to the public key database so unauthenticated users can not send messages to authenticated users. Authentication may be done using either a username/password or using the previously published public key.

- Server fail-over is an optional feature where a primary server registers itself and any secondary servers with the server registry. The secondary servers will keep their databases in sync.

- Group message encryption will be implemented by re-encrypting and re-sending the same message to each of the individual recipients.

- Groups will be assigned a group id and will be handled by a designated message server.

- Groups can be kept private using a symmetric encryption key required to read individual encrypted messages.


Register
Authenticate
Download Public Keys
D
Public Key Files
Client
Get Available Servers
Get Users
Get Messages
Send Message
Subscribe to Group
D
Public Key Database
Key Server Cluster
D
Message Database
Message Server Cluster
D
Active Servers List
Registry Server
Register