Research

In order for the client to communicate with the server and be authenticated, a secure link must be used.

OpenSSL - version 1.0.2, January 22 2015. Open Source, written in C. previous versions have had vulnerabilities, most notably heartbleed.

Once the link is established, encrypted and authenticated messages will be passed between server and client.

The message will be encrypted, then HMAC function applied. This is the secure way to apply both encryption and authentication.

The HMAC function will use SHA-2. MD5 and SHA-1 WILL NOT BE USED.

In addition, a timestamp, direction bit, and client unique ID will be appended to the message. this will allow the server to authenticate the client while giving some protection against reflection, replay, and other attacks.