Biometric Authentication Documentation

Terms:

Biometric Reader Client - Client application that interfaces with Fingerprint Scanner. Takes in the Fingerprint image for authentication and the Blood Vessel image for confirming that the finger is alive. Uses the Byte Index Key generated by the Remote Server to produce an AuthKey.

Remote Server - Server application that opens SSL sockets to receive client communication. When it receives a communication request from a Client, it spawns off a thread and handles the authentication procedure. A Byte Index Key is generated using an algorithm to provide the client with a list of byte positions that will be used to verify that the Digital Image acquired by the Client matches a Server-Side Digital Image to a certain percentage. The algorithm used and the percentage are both adjustable.

Fingerprint Image - The actual Fingerprint Image acquired by the Fingerprint Scanner. The Fingerprint image held by the Client is deleted after the Digital Image is created.

Blood Vessel Image - The Blood Vessel Image is used to verify that the finger being scanned is a live finger. The Blood Vessel Image is deleted after verification.

Digital Image - A bitmap equivalent to the Fingerprint Image used for authentication. Content from the bitmap corresponding to the list of positions (BIK) are sent to the server to compare with the Server-Side Digital Image.

SSL - Secure Socket Layer authentication. Using public and private keys for both the Client and Server, communication between the two is made secure.

Byte Index Key (BIK) - A list of positions that will correspond to content from both the Client and Server Digital Images that will be compared for authentication. Multiple BIKs may be sent from the Server during the authentication process based upon desired criteria.

Authentication Key (AuthKey) - The content from the Client's Digital Image that is sent to the Server after the Client receives a BIK. The Server fundamentally produces its own Authentication Key when it receives one from the Client, using the Server-Side Digital Image and the generated BIK. The two Authentication Keys are compared by the server, and based on desired criteria, the Client can be either authenticated or denied.

ACK - An acknowledgement message sent to the Client from the Server, either confirming the Client's Fingerprint or denying it.

Process (Corresponding to the Authentication Flowchart):

1. ***Client:*** The Fingerprint Image is acquired from a scanner, along with a Blood Vessel Image. Blood Vessel Image is verified for liveness.
   Server: Settings are initialized, and an SSL Server Socket is opened for communication.

2. ***Client:*** A Digital Image (bitmap) is produced from the Fingerprint Image. The Blood Vessel Image and Fingerprint Image are both destroyed.
   Server: The Server waits to receive a connection from a client with the correct SSL Keys/Authentication information.

3. ***Client:*** Using SSL authentication, establish a connection with the Remote Server. Send a ready message to signal the beginning of the authentication process.
   Server: Accept SSL connection from Client. Receive a Ready Message indicating the beginning of the authentication process, and then spawn a thread to handle the process for the Client.

4. ***Server:*** Generate a Byte Index Key using the Server-Side Digital Image. This is a list of positions created through the use of a desired algorithm (e.g. one random position, 1000 random positions, specific positions, etc.). This BIK is sent to the client.
   Client: The Client received the BIK from the Remote Server.

5. ***Client:*** Generate Authentication Key using the BIK and the Digital Image of the Fingerprint. Positions from the Bitmap are selected corresponding to those specified in the BIK, and are gathered together.

6. ***Client:*** Send Authentication Key to the Remote Server.
   Server: Receive Authentication Key from the Client.

7. ***Server:*** Verify that the Authentication Key is authentic using the previously generated BIK and Server-Side stored Digital Image to produce a Server-Side Authentication Key. Compare this to the Authentication Key sent by the Client. If it meets certain requirements (e.g. 100% matching at the BIK positions, certain positions matching, certain percentage of positions matching, etc.), the Client can be authenticated.

8. ***Server:*** Based on desired conditions, the Client may need to provide additional authentication. The process returns to Step 4, possibly requesting a different set of content from the Client's Digital Image to further confirm that the client has a genuine image. If no more steps are needed, an ACK can be sent to the client.

9. ***Server:*** Send an ACK to the Client informing of approval or denial.
   Client: Receive the ACK from the Remote Server, further actions will either be approved or denied.