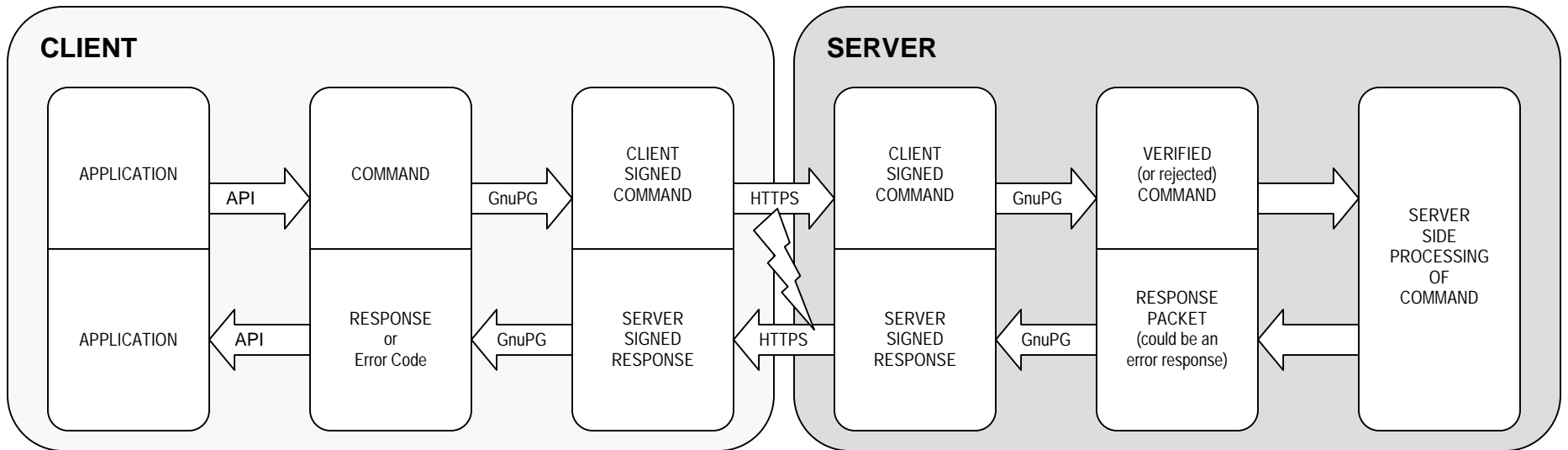


Example Use Case Diagram



Transaction Steps:

- The client builds and formats a command packet according to the protocol specification.
- The packet is digitally signed with the secret key of the SRS client
- The entire signed packet is sent to the SRS server via HTTPS.
- Upon receipt, the digital signature is checked. If the signature does not match the one on file for the client, an error return packet is generated. Otherwise, the command is processed and an appropriate return packet is constructed.
- The return packet is then signed by the SRS server's secret key and returned to the client via HTTPS.
- The client receives the packet and checks the digital signature to make sure the response actually came from the SRS server. If the signature does not match, an error is returned. Otherwise, the results are parsed out of the packet and returned to the client. In this case, we see that the command was successful and returned the name-value pairs.