**SEC Project 2 Report by Group 2 Alameda**

During this phase of the project we had to change the Client in order for it to use the Portuguese Citizen Card to authenticate the user.

When the user starts up the client, the CC needs to be inserted in the card reader. The client will then read the CC and extract from it the authentication certificate. It then checks if the server already has this certificate stored. If the server doesn’t have the certificate stored then it’s necessary to store it. The certificate is then sent to the server with another certificate present in the CC (certificate with the index 3 in the certificate list present in the card) in order for the client to receive the challenge. The server will verify the certificate it received with the second certificate and will then send a random array of bytes to user. The server will also store a time limit for which the challenge can be completed (one hour after the challenge is sent). The client will sign the random byte array with the private authentication key of the CC and send it back to the server in order for this to verify the signature using the public key present in the authorization certificate sent to the server. This allows to verify that the certificate was sent exclusively by the owner of the card and not by another person.

During this phase it was also modified in order for the Public Key Blocks to be signed using the private key of the authentication certificate present in the CC card. To sign the Public Key Blocks using this key it is necessary for the user to insert the authentication pin for the card which is a secret only known to the owner of the card. By utilizing this it is possible to verify that another person, even if it had access to the card of the user it would not be possible to write because it needed the pin code.

There was also another feature implemented in which the user could access all the public keys of the certificates present in the server. This allowed for an easier access to read other files.