Aadhar details verification. Ns assignment-5 -by Aaron agnel (2017010) and Bharath Kumar (2017035)

Scenario:
We have two subjects, client (C) and server (S). C wants to know whether the aadhar details of a certain person are fake or original which S knows. So C has to send the identification of the person (name/number) along with the details to be checked (in our case, the DOB), and then S has to send YES for correct details or NO for fake details.

Solution:

So for this, we maintain public/private key pairs for both parties and assume both of them know the public keys of one another (that is the CA is inherent). So we first share a hmac secret from the client to the server.

C->S E(PubC,E(PrivS,hmac))
S->C E(PubS,E(PrivC,"confirmation")

Once the hmac is established, C sends a message which contains the identifier, the DOB the nonce, timestamp, and the hash to S.

M={ADI,DOB,timestamp,nonce}
C->S E(PubC,M||E(PrivS,hash(M))

S then gets the message, verifies hash, and gets the message M. It searches its database and finds the user and then cross verifies the DOB and returns YES for correct DOB else NO.

M={"YES/NO",timestamp,nonce}
S->C E(PubC,M||E(PrivS,hash(M))

In all communications, we use mutual authentication and confidentiality by using pub,priv keys together for encryption.

Hmac secret sharing:

For this we maintain a public and private key pair for each individual. B then sends a request to A by first encrypting the request with his private key then he adds his identifier to the request and then he encrypts the entire message using A’s public key (the public is assumed to be known and verified). So now A decrypts this message using her private key first gets the identifier of B and then uses his public key to decrypt the request. The request then consists of the shared secret which B wants to use. If A agrees then it uses it else it sends a new secret to B. That is the return request is either a OK or a new secret for B. The return request is similarly encrypted first with A’s private key and then with B’s public key. After this step both A and B agree upon the hmac secret.

1) {{secret:xxx}|B_{priv} | B_{id}}|A_{pub}
2) {{secret:xxx}|A_{priv} | A_{id}}|B_{pub}