Needham Schroeder Authentication protocol

Needham and Schroeder protocol uses a secret key known to the sender and also to an authentication server.

Sender and Receiver share a secret key and use it for secure communication with the authentication server.

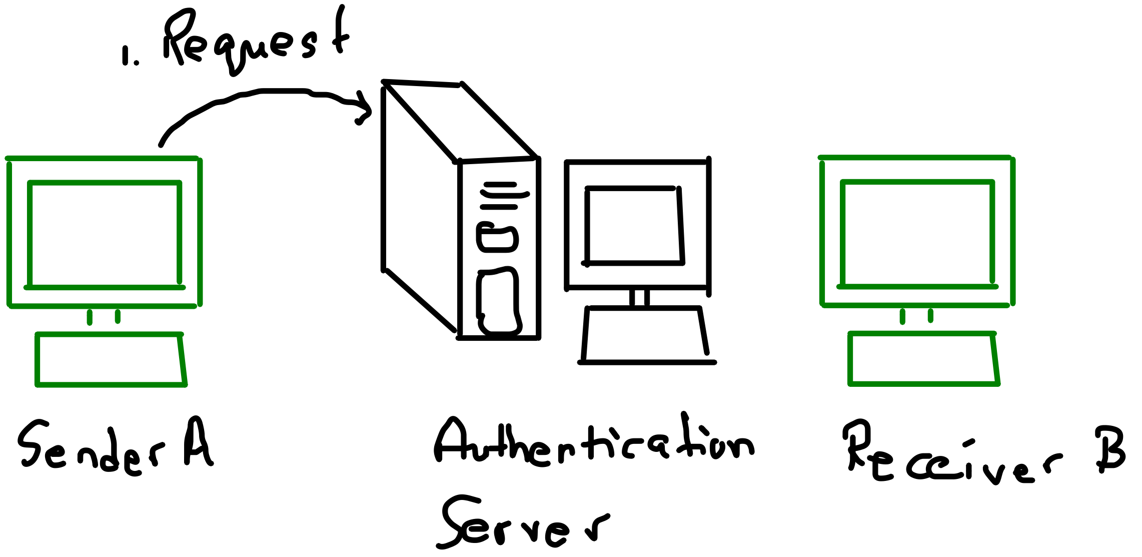
Step 1:

Sender A requests for a session key to the authentication server for communiation with Receiver B.

The message consists of A's Secret key Ka, A's Network Address Na, B's Network Address Nb and a Nonce.

The request sent by A to the authentication server which is in its encrypted form is :

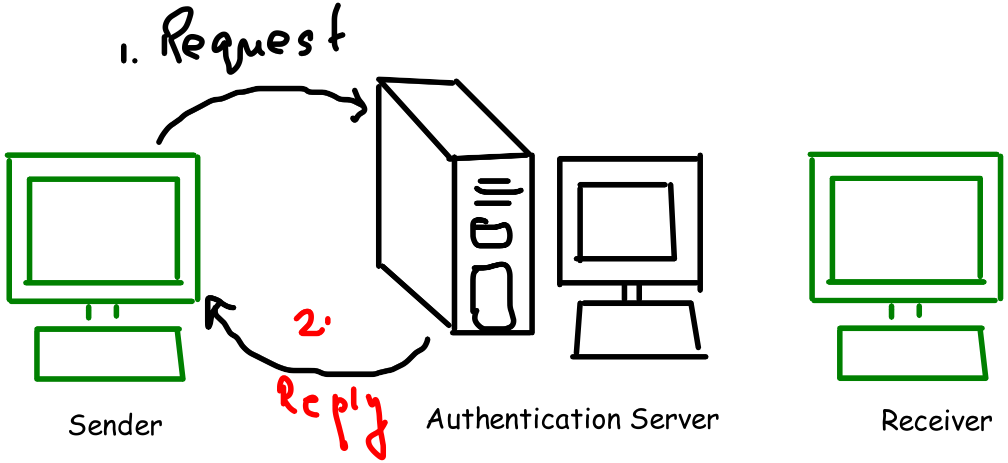
E(Ka,[Na,Nb,N])



Step 2:

Authentication Server returns a message, containing a newly generated key Kab, nonce N(same), ticket(Kab+Sender's Name) encrypted with B's secret key Kb, receiver's name and this whole message is encrypted with the sender's private key Ka to ensure that no one else can read it.

E(Kab, N, {A,Kab}Kb,B)Ka

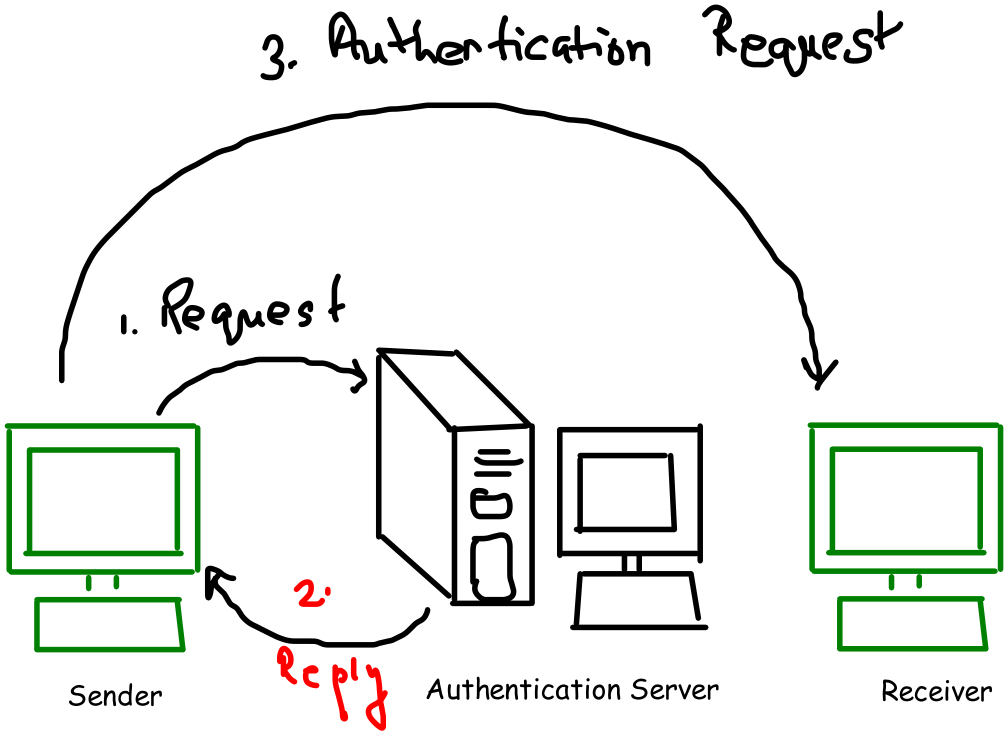


Step 3:

After receiving the reply from the Authentication Server, the sender decrypts the message and send the {A,Kab} to receiver B.

A sends the ticket to B which is not in encrypted format because it was previously enrypted by the Authentication server using B's secret key.

(A, Kab)Kb



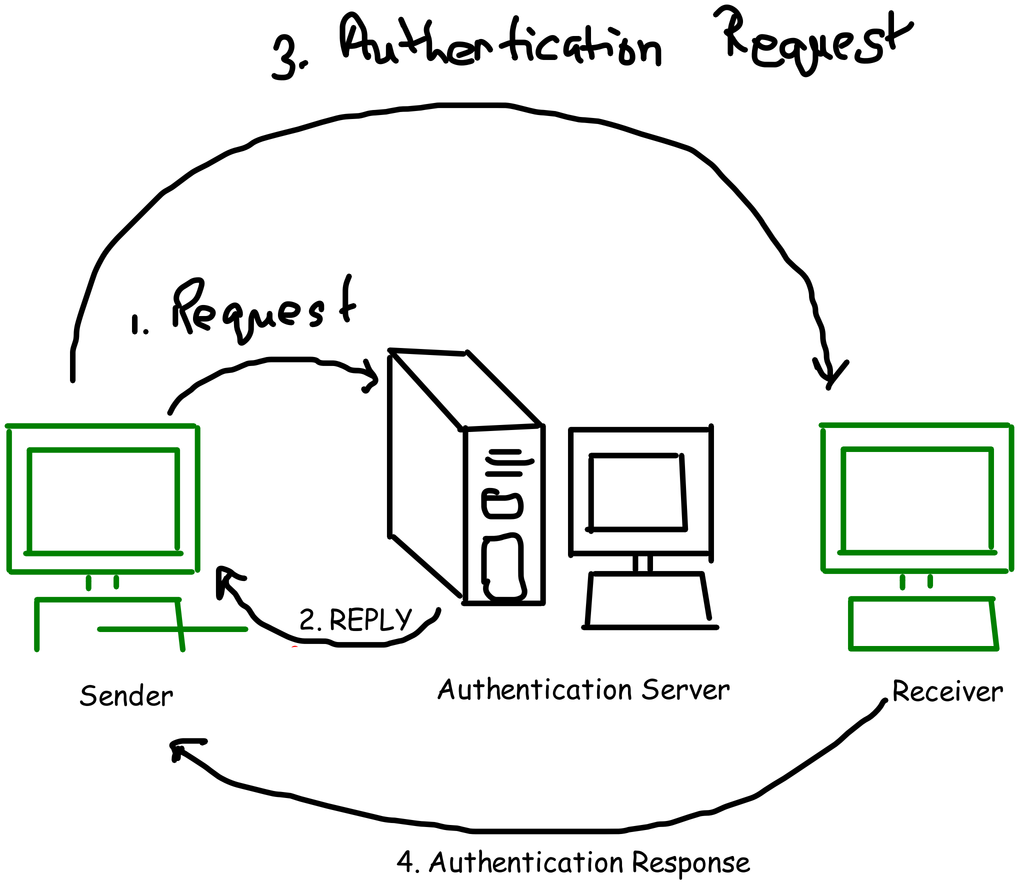
Step 4:

B decrypts the ticket received from A using the secret key Kb and compares the sender's identity.

B again encrypts the message using the shared secret key Kab and generates nonce N1 and sends it back to the receiver.

E(N1)Kab

In this step B got the session key (Kab) to securely communicate with A.

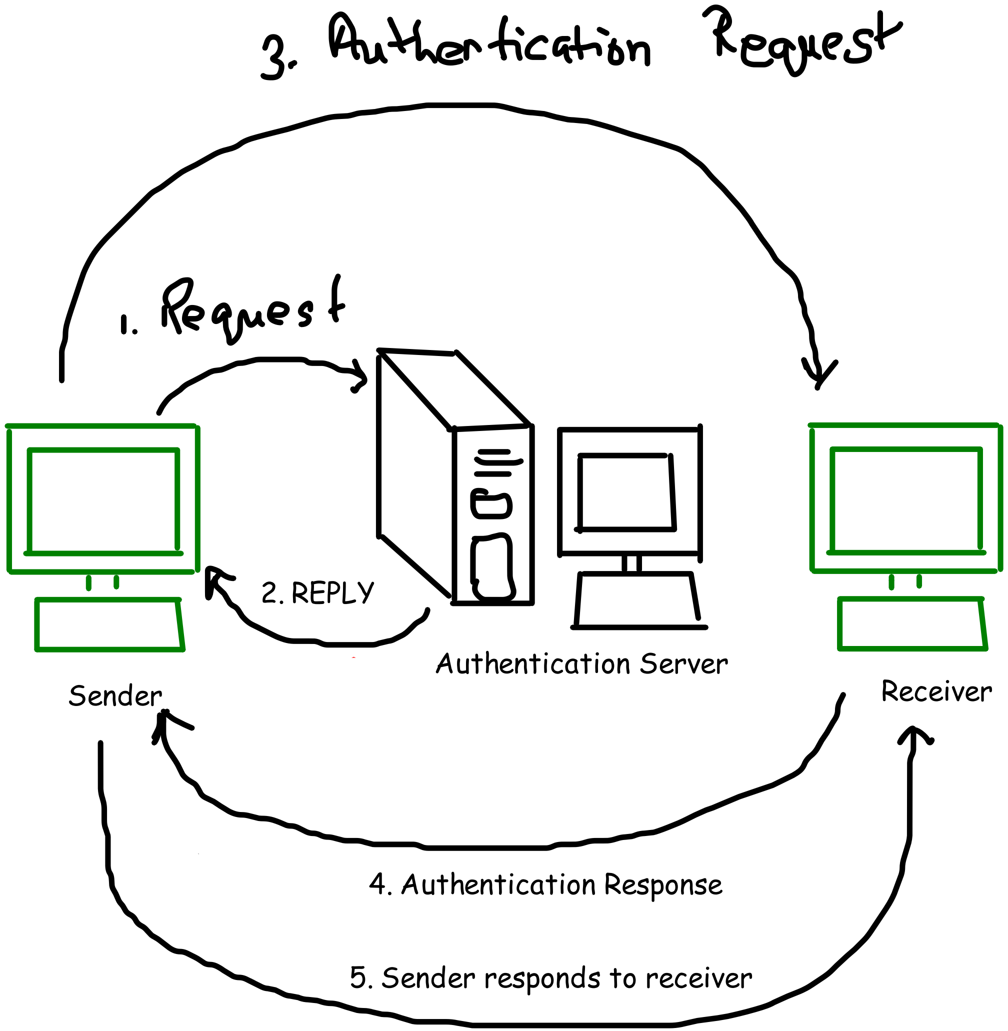


Step 5:

Sender decrypts the Nonce N1 using the shared secret key Kab . This proves th sender's identity.

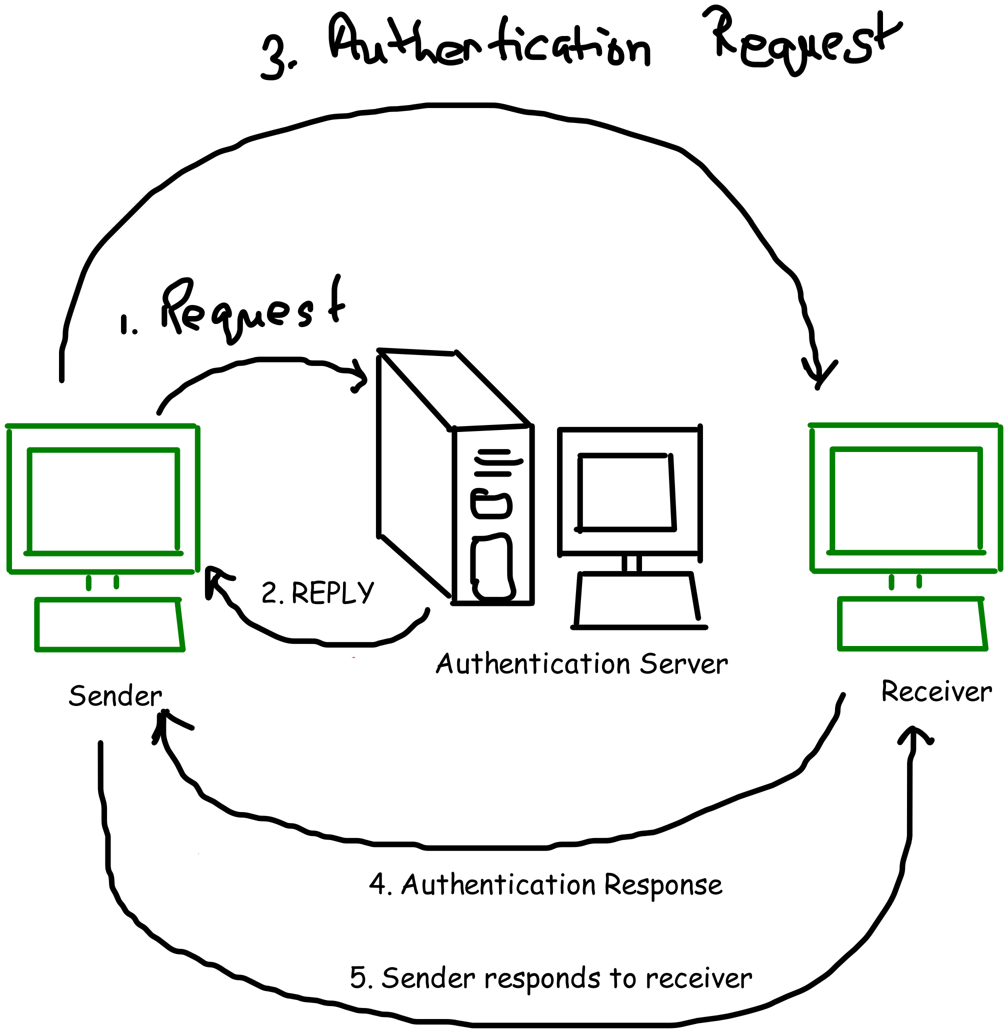
The sender sends response N1+1 encrypted using the shared secret key Kab.

E(N1+1)Kab


3. Authentication Request
1. Request
2. REPLY
Authentication Server
Sender
Receiver
4. Authentication Response
5. Sender responds to receiver

Step 6:

Now the sender A and receiver B can securely communicate with each other using the session key generated


3. Authentication Request
1. Request
2. REPLY
Authentication Server
Sender
Receiver
4. Authentication Response
5. Sender responds to receiver