

## Client

Message  $m$ : LOGIN; user, password

Signature:  $K_A^-(m)$

SYN,  $K_A^-(m)$

Authenticated

## Server

### APACHE

Login and  
sign  $m$



Apaches  
private key

$K_A^-$



Apaches  
public key

$K_A^+$

Verify signature  
 $K_A^+(K_A^-(m))$

### WebSocket Server