

## Client

Message  $m$ : LOGIN; user, password

Signature:  $K_A^-(m)$

SYN; user, password,  $K_A^-(m)$

Authenticated

## Server

### Apache

Login and sign  $m$

$K_A^-(m)$



Apaches private key

$K_A^-$



Apaches public key

$K_A^+$

Verify signature

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

### WebSocket Server