SMART RESTAURANT

FINAL PRESENTATION

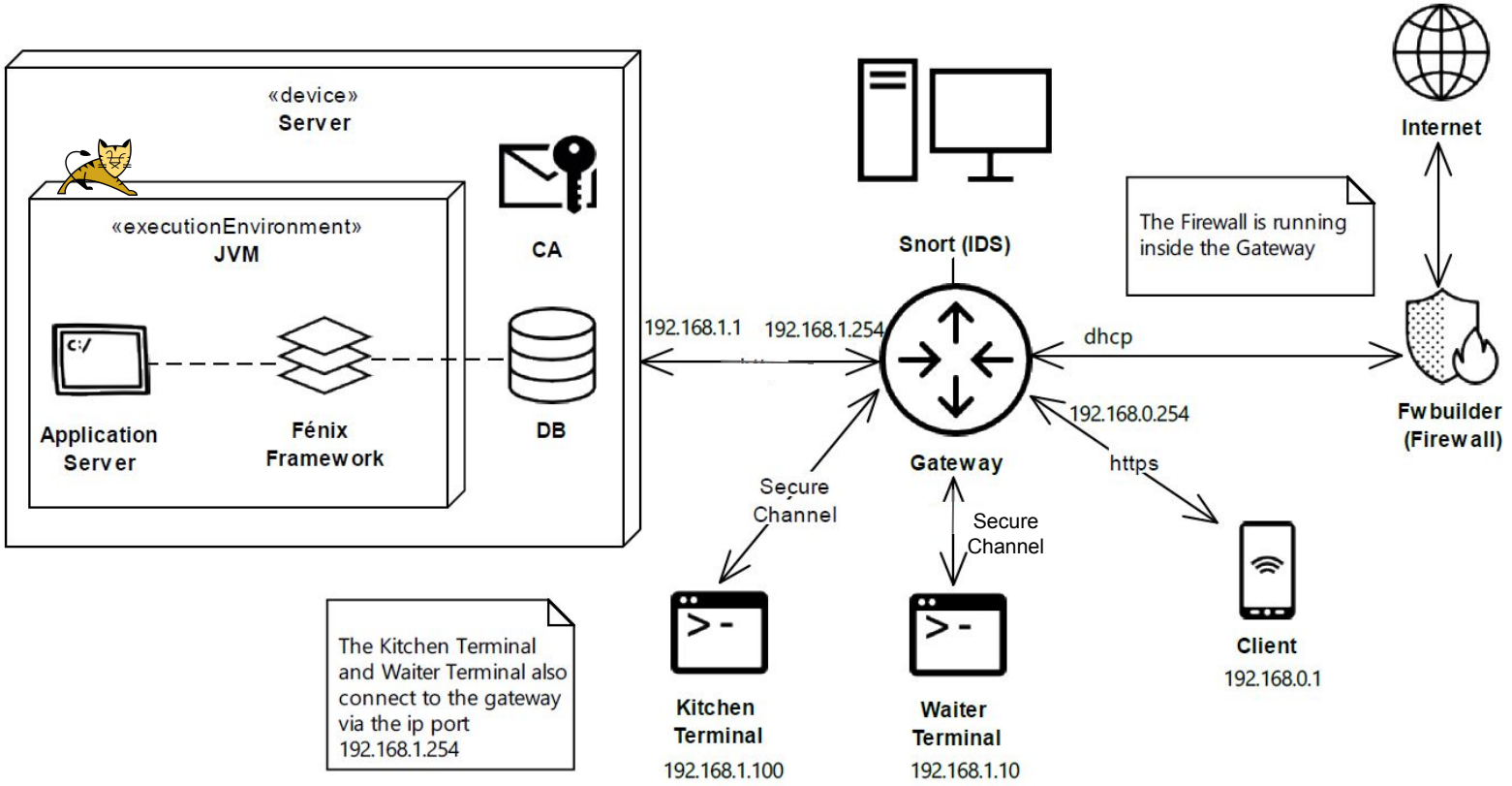
SEGURANÇA INFORMÁTICA EM REDES E SISTEMAS

Work By

Diogo Ferreira - 79018
Tiago Vicente - 79620
Francisco Santos - 79719
GROUP 12

SEGURANÇA INFORMÁTICA EM REDES E SISTEMAS

ARCHITECTURE



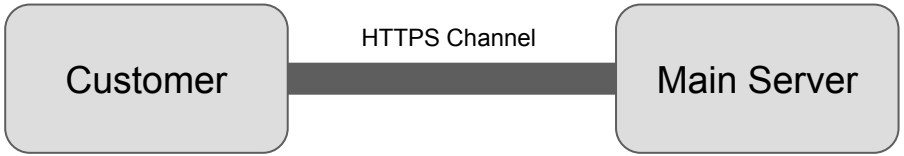
SECURITY MEASURES

- Two-Factor Authentication;
- Salt;
- HTTPS between Customer and Main Server;
- Handmade channel using ws-handlers between Main Server, Kitchen and Waiter;
- Firewall;
- IPS/IDS.

KEYS/CERTIFICATE DISTRIBUTION

- A shared key between the Main Server and the Kitchen is manually distributed;
- Another shared key between the Main Server and the Waiter is manually distributed;
- Certificates are distributed using a CA.

PROTOCOL

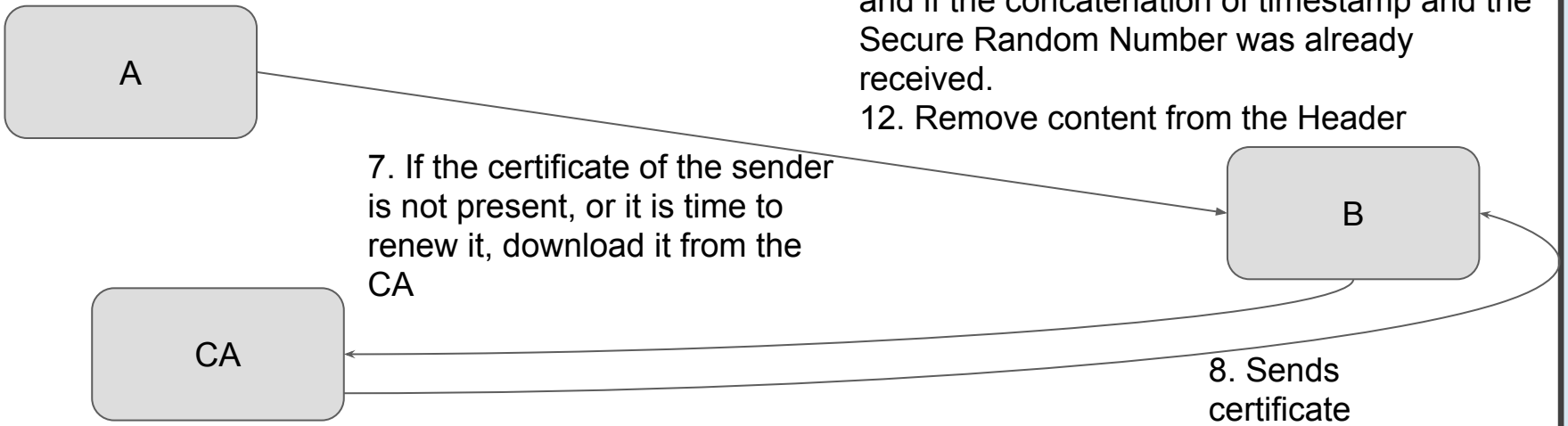


When the user login, the Main Server assigns to that session an 128 bit random unique token.

HANDMADE PROTOCOL

1. Insert Sender, Receiver, Timestamp and Secure Random Number to Header
2. Sign message using entity's private key
3. Add IV to Header
4. Cipher Message with AES 128

5. Get IV
6. Decipher
9. Check if I am the receiver and the sender
10. Verify Signature
11. Verify if Timestamp is within the interval and if the concatenation of timestamp and the Secure Random Number was already received.
12. Remove content from the Header



Youtube Link

YouTube Link