Smartphone as a Security Token

Segurança Informática em Redes e Sistemas
1st Semester 2020/2021

Group 27
João Soares - 89475 | João Dinis - 89485 | Tiago Fonseca - 89542

Project Motivation

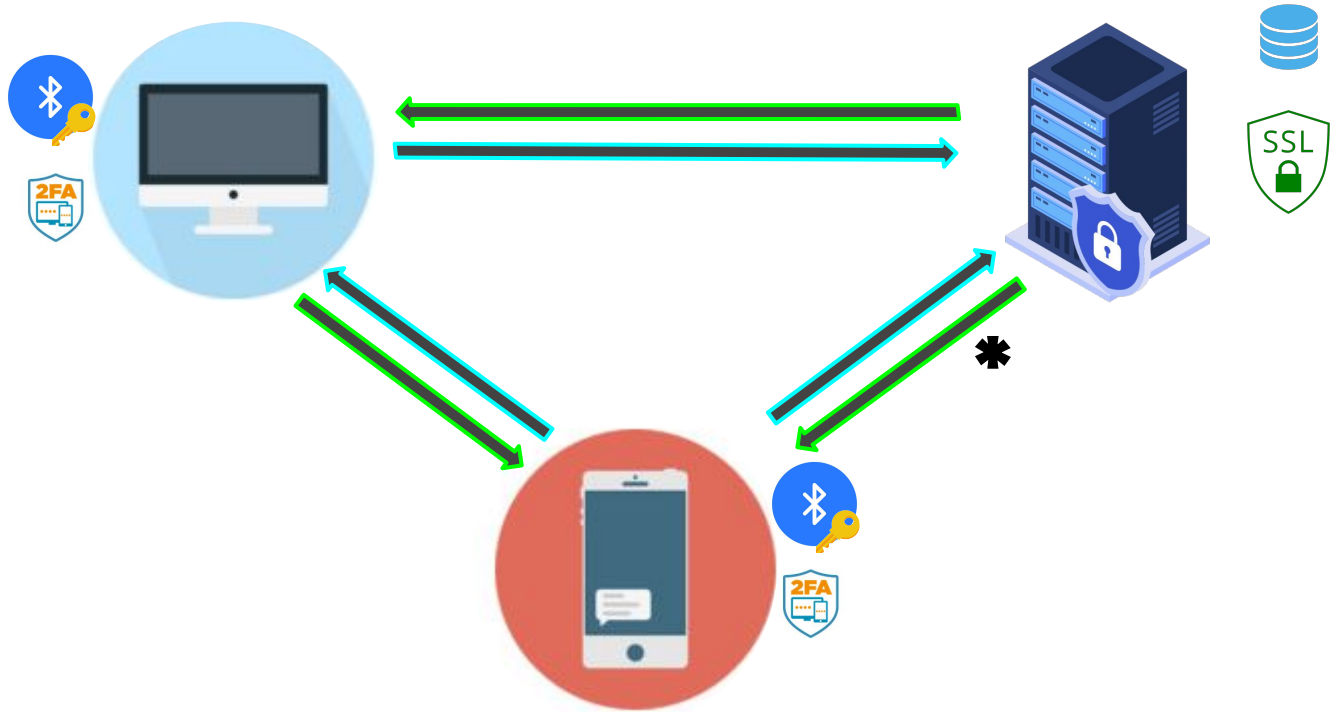
Main issue:

- ➔ Passwords are a single point of failure

To improve security, our bank application uses:

- ➔ Two-Factor Authentication *(Something we **have**/**know**/**are**)*
- ➔ Secure local connection *(Bluetooth)*

System Architecture



Key Distribution

Server

- Certificate signed by public domain trusted CA - *Let's Encrypt*
- Let's Encrypt Certificate is pre-installed in all clients by default

Desktop

- Key Pair is saved inside a protected KeyStore
- Public Key sent to the Mobile via QR Code

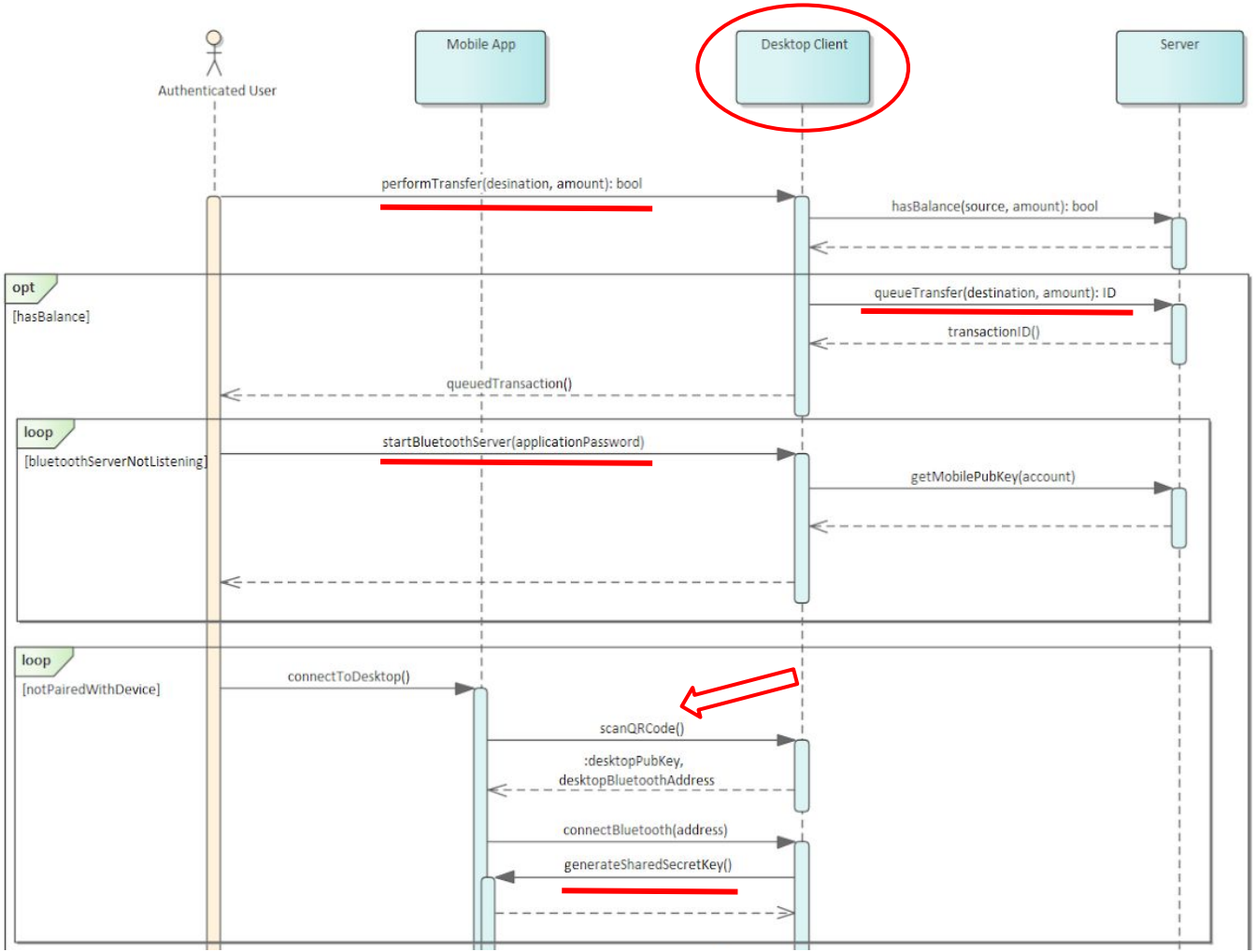
Mobile

- Key Pair is saved inside the AndroidKeyStore
- Public key stored on the Server during the initial setup

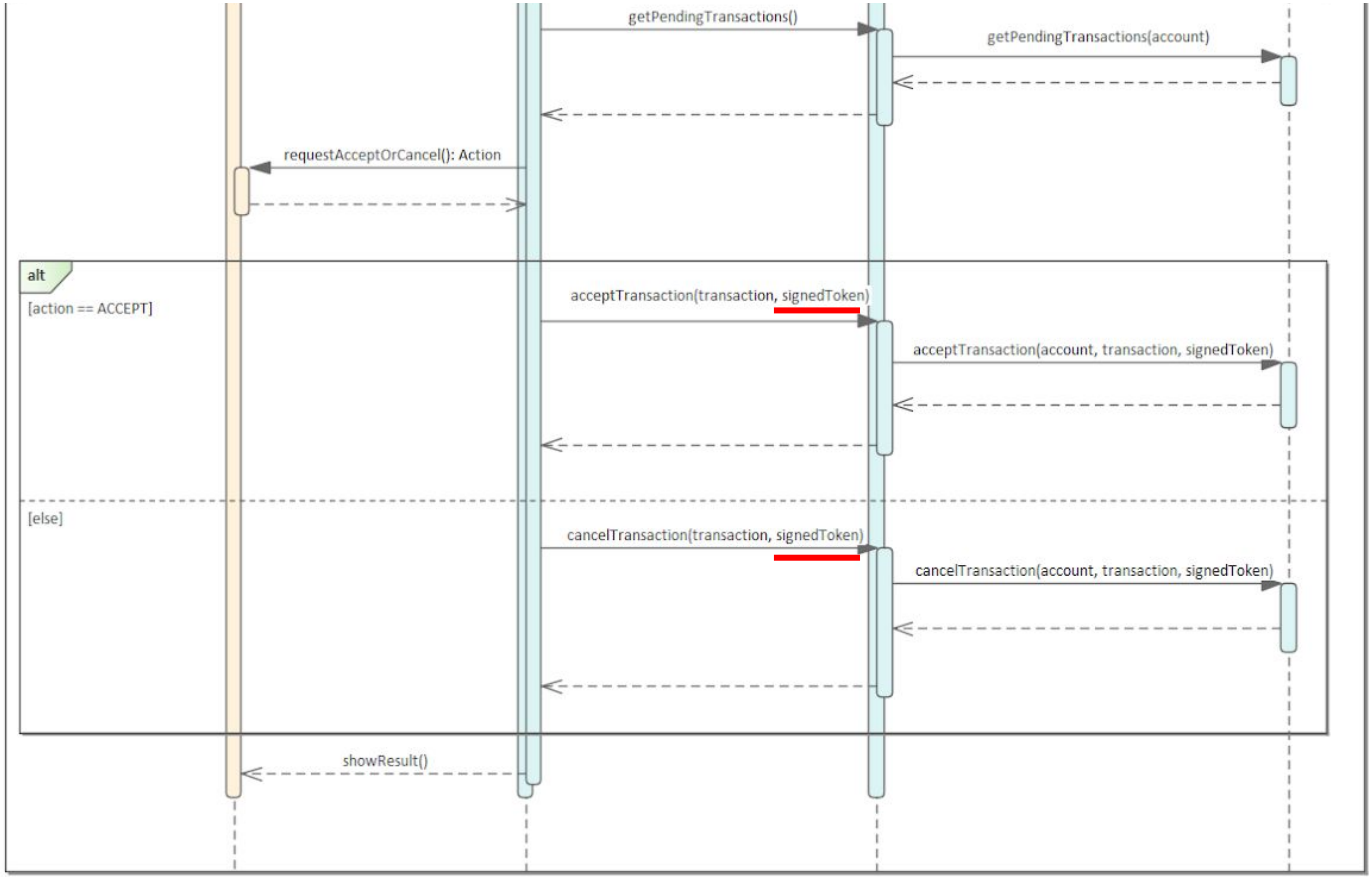
TOTP

- Generated on the Server and sent via QR Code
- Ciphered before storing

Bluetooth Secure Protocol



Bluetooth Secure Protocol



Live Demo