Login Scenario (Authentication)

MOBILE

MIDDLEWARE

BACKEND

Verify OTP ➤

Verify OTP ➤

1. Verify OTP and send response

OTP Verified

Authorization Bearer Token

Bearer eyJhbGciOiJIUzI1NiIsInR5cCI6IkpXVCJ9.eyJzdWIiOiIxMjM0NTY3ODkwIiwibmFtZSI6IkpbmUgRG9lIiwiaWF0IjoxNTE2MjM5MDIyfQ.SflKxwRJSMeKKF2QT4fwpMeJf36POk6yJV_adQssw5c

Claims: 775461117

After successful verification

1. Creates JWT Token
2. Adds phone # as claims data
3. Subsequent requests Token's MSISDN # will be verified with payload MSISDN

All requests after verify OTP

1. Middleware checks Token msisdn # vs Payload msisdn
2. Mismatch - req rejects
3. if matches - proceeds to BE

{
    "serviceType": "GETALLCUSTOMERWALLETSREQ",
    "externalReference": "1694549092",
    "msisdn": "77546115O",
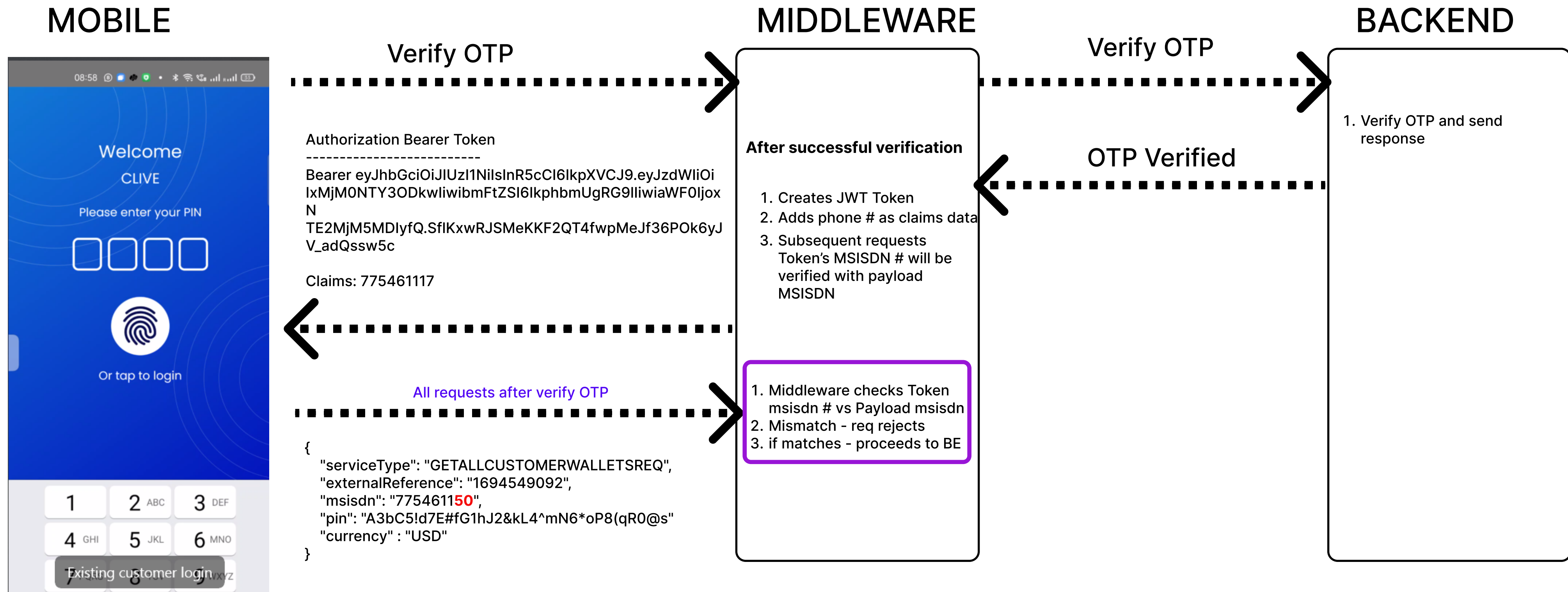   "pin": "A3bC5!d7E#fG1hJ2&kL4^mN6*oP8(qR0@s"
    "currency" : "USD"
}

Please Note: This token will be part of Authorization Header for every request after Login & Registration and validated in middleware. This will have Access Token & Refresh token.