STAR Payment

-by(WIN_TRIBE) Amarendra P,Shashank N,Kumaresan K

STAR : Secure Token Authorized Remote Payment

Problem statement : Improving payment experiences

Summary: Idea is to make the payment easy even in spotty network or in offline mode. Make it available to anyone having basic mobile or smart phone.

" User doesn't require internet or network coverage"

Core idea is to make use of "TOTP"(time based one time password). It is similar to RSA token which is using a built-in clock and the card's factory-encoded random key known as the "seed". The seed is different for each token, and is loaded into the corresponding RSA SecurID server

It may be soft-token if customer mobile is smart-phone or hard-token given to customer

Generating Secure offline payment token :

Using the below fields and encrypted by the private key either will generate Ultrasonic Sound or sent an sms to GRAB centeralised number.

encrypt(MERCHANT_ID + AMOUNT + TOTP + USER_PIN)

Paytment token will be JWT token having above fields as payload encrypted using user secert key.

if both parties (customer,Merchant) don't have internet :
-> If User has smart Phone through APP he can enter above details and sent SMS
-> If User has feature phone directly he can sent SMS to GRAB number

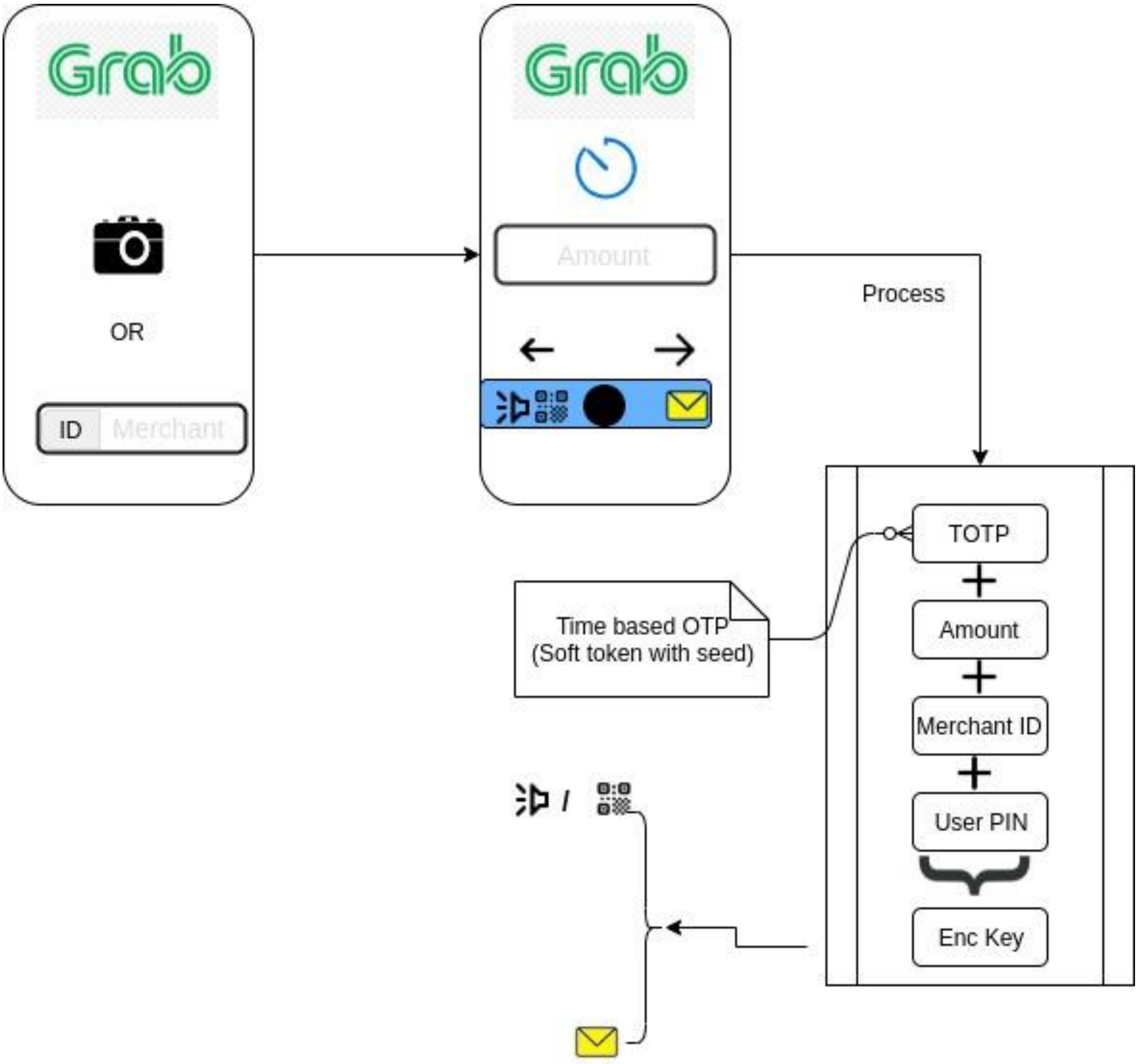
If merchant has internet and user has smart-phone without internet by giving the above details and can make Ultrasonic sound from APP.

Technologies Used

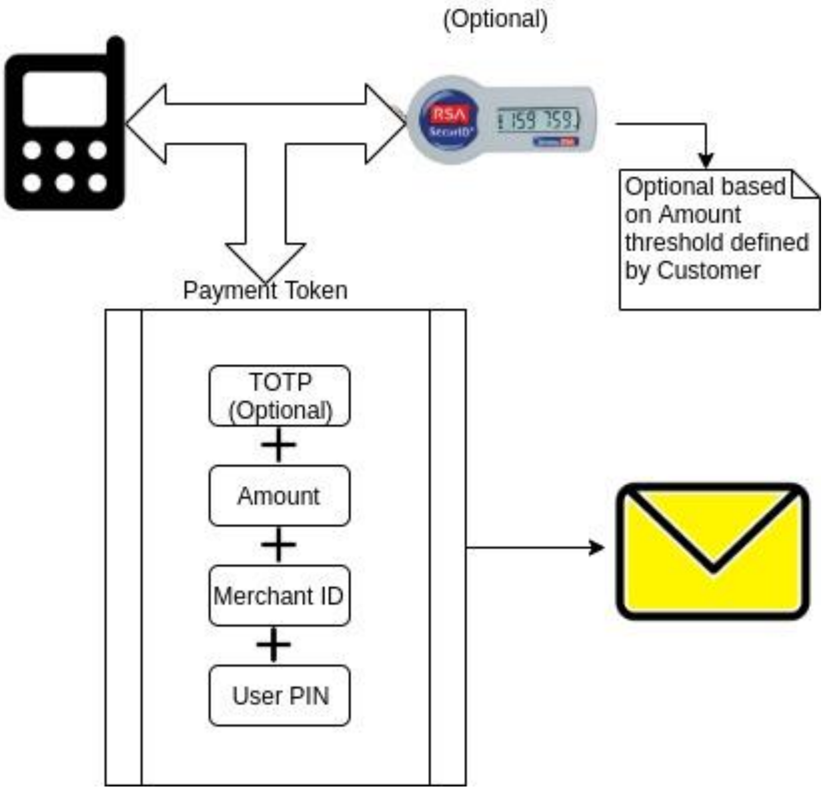
1. UI Hybrid (Ionic)
2. Spring JWT
3. Mongo DB
4. Twilio SMS service
5. Java TOTP lib
6. Redis

Interaction Diagrams

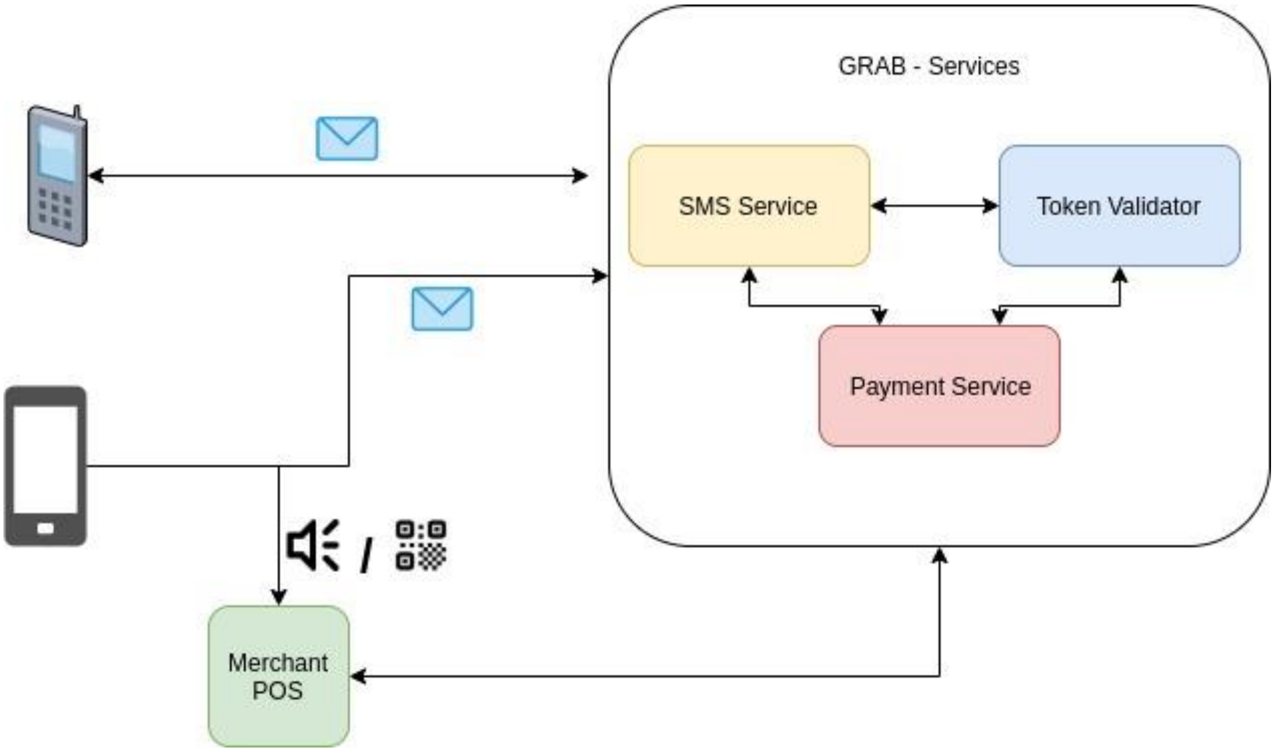
Smart Phone Flow



Basic Phone with Hard-token flow



Componenets



Feasibility:

1. To avoid replay atttacks, payment token will be invalidated once it s used.
2. Since User PIN we are including in token, so even user lost the mobile we can avoid unauthorised transactions
3. Since we are supporting totp based soft and hard tokens we can enable secure transaction experience to all the users
4. Since we are using jwt token Merchant can’t modify amount or any other details and also man in the middle attack is not possible