**CheckRelianceAPI**

* Authentication using JWT(json web token):

**Authentication:**

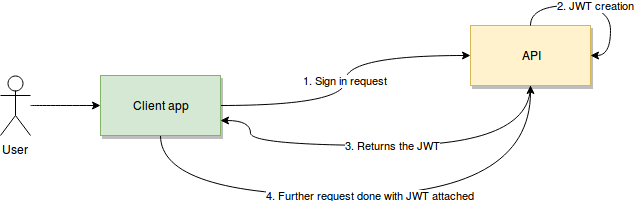
Every request must pass the authentication parameters along with the uriTemplate as given in following example:

http://checkrelianceAPI.glotechasp.com/WS/mobileApp.svc/verificationrequest?apiLogin=xP9JV25sf8 &transactionKey=UEx5qgYycrBZ &sv=xxxx&tId=xxxx&uid=xxxx

*Authentication Parameters:*

* apiLogin
* transactionKey
* sv (softwareVersion)
* tid (Terminal Id)
* uid (UserId)

WORKFLOW:



**Case 1:** API checks the parameters in the every request URL. If parameters are not find API return the JSON response with status code 401.

Sample Output JSON:

{

    "status": "Failed",

    "message": "Authentication parameters are missing!"

}

**Case 2:** If parameters exits API validate the values of parameters. If parameters are not valid API return the JSON response with status code 401.

Sample Output JSON:

{

    "status": "Failed",

    "message": "Authentication parameters are Invalid!"

}

**Case 3:** If authentication parameters are valid. API generate and return the JWT Token in JSON format with status code 200.

Sample Output JSON:

{

    "token": "eyJhbGciOiJIUzI1NiIsInR5cCI6IkpXVCJ9.eyJleHAiOjE3MDQ5ODExMTcsImlzcyI6InlvdXRDb21wYW55SXNzdWVyLmNvbSIsImF1ZCI6InlvdXRDb21wYW55SXNzdWVyLmNvbSJ9.3VEA-noteZxdlSZOQuNSnIGATROkxMeXMQVYDJDo2sM"

}

Now the client has to request with valid parameters along with the JWT Token return by the API.

**Case 4:** Now if the request URL has valid parameters but invalid token. API returns with status code 401.

{

    "status": "Failed",

    "message": "Token is Invalid!"

}

**Case 5:** If the parameters and token are valid in the request URL then the authentication is Successful.