

OIDC Client/  
Authentication Pipeline

OIDC Connect

Auth/Challenge Flows

User keys in their  
userID/email

Look up for PK of the  
user

Call Authsignal  
Initialization Auth End  
point

Initialization  
Auth

POST  
/init-auth

Return with one time  
use token

Initiate OIDC flow

Append token via the URL Parameter  
Authorization end point  
GET /oidc/auth

Redirect

Authsignal Rules  
Engine

Decision

IF CHALLENGE\_REQUIRED  
The user will be redirected  
to Authsignal's hosted  
auth/challenge flows

User completes Auth  
challenge

IF ALLOW

Authsignal Rules  
Engine

If user has successfully  
completed or failed  
Redirect to /callback

Redirect to OIDC  
call back redirect\_uri  
with auth\_code

Callback

Fetch access token  
using auth\_code  
POST /oidc/token

Return Access Token

Determine  
Authentication State

Access Token Returned

Inspect Access token  
action\_state claim

Decision

If  
BLOCKED  
CHALLENGE\_FAILED

Terminate

if  
ALLOW  
CHALLENGE\_SUCCEEDED  
and userID matches current session

Proceed with  
completion of  
Authentication/Or  
Business Logic

