EHR needs to provide Ocean the following:

- iss URL
- client id
- EHR Authz Server URL

- **iss**: Base URL for FHIR Server
- FHIR Resource URL (Access Token)

EHR App Launcher | Ocean SMART APP | EHR Authz Server | EHR FHIR Server

Set Patient Context & Launch Ocean App

1 GET REQUEST https://ocean.cognisantmd.com/sso/smart/auth?
siteNum=**[OceanSiteNum]**&
iss=**https://[Base URL for FHIR Server]**&
launch=**[ID for this specific launch]**&
action=**[Portal, viewMap, or sendMessage etc.]**

2 Validate issuer in allow-list or throw error

Smart Launch Failed
The issuer of the token is not one of the Ocean's trusted issuers. Please contact support to resolve this.

3 GET REQUEST **https://[EHR Authz Server authorize endpoint]**?
client_id=**[EHR Launch Server randomly assigned ID]**&
response_type=code&
aud=**https://[EHR FHIR Server URL]**&
launch=**[ID for this specific launch]**&
redirect_uri=**[Ocean's redirect URL, e.g. https://ocean.cognisantmd.com/smart/auth]**&
scope=launch patient/*.* openid profile &
state=**[128 bit guid]**

4 Authz Server verify request based on **client_id** & **launch**

5 GET RESPONSE **[https://Ocean's redirect URL]**?
code=**[Authorization Code]**&
state=[128 bit guid]

7 POST REQUEST https://[EHR Authz Server]/token
{
"redirect_uri" : **[https://Ocean's redirect URL]**
"grant_type" : authorization_code
"client_id" : **[EHR Launch Server randomly assigned ID]**
"code" : **[Authorization Code]**
}

8 Get Patient context (**Patient ID**) from EMR

9 POST RESPONSE:
{
"access_token" : "[**Access Token**]",
"token_type" : "bearer",
"expires_in" : "3600",
"scope" : "**patient/Patient.read**",
"patient" : "[**Patient ID**]",
"id_token": "**[User ID token]**",
"oceanSharedEncryptionKey": **[oceanSharedEncryptionKey to decrypt Ocean Patient Data in Bases64]**
}

id_token JWT:
{
"jti":"[JWT ID]",
"iat":[Issue At ID],
"exp":[Expiration Time],
"aud":"[Audience ID]",
"sub":"[Subject ID]]",
"iss":"https://[Base URL for FHIR Server]",
"given_name":"GIVEN_NAME",
"family_name":"FAMILY_NAME",
"profile":"[FHIR profile URL]",
"auth_time":[Auth Time],
"at_hash":"[**Access Token Hash Value**]"
}

10 GET REQUEST **https://[Base URL for FHIR Server]/.well-known/openid-configuration**

11 GET RESPONSE:
{
"issuer": "https://[Base URL for FHIR Server]",
"authorization_endpoint": "https://[EHR Authz Server]/authorize",
"token_endpoint": "https://[EHR Authz Server]/token",
"jwks_uri": "**https://[EHR Authz Server]/jwks**",
"capabilities": [
"launch-ehr",
"client-public"
]
}

12 GET REQUEST **https://[EHR Authz Server]/jwks** to validate identity token

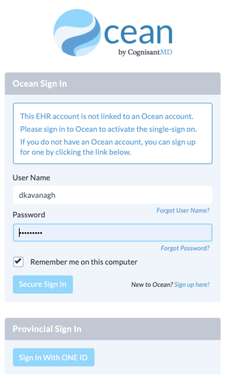
13 GET RESPONSE (Sample):
{
"keys": [
{
"use": "sig",
"kty": "RSA",
"kid": "public:c424b67b-fe28-45d7-b015-f79da50b5b21",
"alg": "RS256",
"n": "sttddbg-_yjXzcFpbMJB1flFam.r9smM",
"e": "AQAB"
}
]
}

14 1) Validate Identity Token with [**at_hash**] and **jwks json response**

2) Link EHR user to Ocean

If the user has not yet linked their EHR account to Ocean, a sign-in prompt is shown.

Once the account is linked (and from then on in future launches), the single sign-on is automatic.

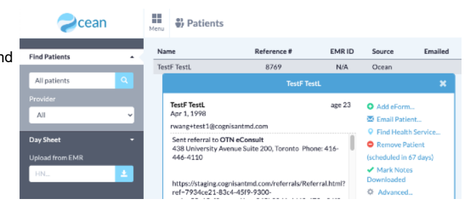


15 If patient is in context:
GET REQUEST **https://[EHR FHIR Server URL]/patient/[Patient ID]** with **[Access Token]**

16 GET RESPONSE (from FHIR Patient.read):
{
"resourceType": "Patient",
"id": "e26f645b-3eda-42a6-9348-2a058a3b5900",
"meta": {
}...
}

17 GET RESPONSE:
1) Patient is encrypted and saved in Ocean

2) Redirect based on requested action:
Ocean Patient Portal or Ocean Health Map



OR