Oauth Issue Summary

Long story short

According to documentation at http://docs.smarthealthit.org/authorization/ , the oauth flow works as expected on app-server (fhir-starter).

The problems appears on growth-chart app.
The "authorize" request include the launch identifier and the app is correctly authorized.
Despite this, when the access token is requested, the response doesn't contains the "patient" parameter.
Because of that the growth-chart app cannot retrieves the patient data from api-server, therefore throws an error.

It is unknown the reason why the "patient" parameter is not defined.

Below there's a complete dump of the communication between applications.
It start from the first "authorize" app-server request and finish wih the "acces-token" response to the growth-chart app.

App server

1st authorize request

GET /openid-connect-server/authorize HTTP/1.1
Host: ec2-35-162-90-131.us-west-2.compute.amazonaws.com:8080
Referer: http://ec2-35-164-199-202.us-west-2.compute.amazonaws.com:8080/fhir-starter/

Query Parameters:
client_id : fhir_starter
response_type : code
scope : smart/orchestrate_launch user/*.*
redirect_uri : http://ec2-35-164-199-202.us-west-2.compute.amazonaws.com:8080/fhir-starter/
state : 4228bab2-0bb2-72ef-78a7-a02dfea2a24b
aud : http://ec2-35-164-199-202.us-west-2.compute.amazonaws.com:8080/api-server

1st authorize response

HTTP/1.1 302 Found
Location: http://ec2-35-162-90-131.us-west-2.compute.amazonaws.com:8080/openid-connect-server/login

After login...

2nd authorize request

POST /openid-connect-server/authorize HTTP/1.1
Host: ec2-35-162-90-131.us-west-2.compute.amazonaws.com:8080
Referer: http://ec2-35-162-90-131.us-west-2.compute.amazonaws.com:8080/openid-connect-server/authorize?client_id=fhir_starter&response_type=code&scope=smart%2Forchestrate_launch%20

user%2F*.*&redirect_uri=http%3A%2F%2Fec2-35-164-199-202.us-west-2.compute.amazonaws.com%3A8080%2Ffhir-starter%2F&state=4228bab2-0bb2-72ef-78a7-a02dfea2a24b&aud=http%3A%2F%2Fec2-35-164-199-202.us-west-2.compute.amazonaws.com%3A8080%2Fapi-server
Cookie: JSESSIONID=FE8A0DBFBC00E79056ECEAC3E65A6B5B
Content-Type:application/x-www-form-urlencoded

Form data:
scope_smart/orchestrate_launch : smart/orchestrate_launch
scope_user/*.* : user/*.*
remember : until-revoked
user_oauth_approval : true
authorize : Authorize

2nd authorize response

HTTP/1.1 302 Found
Location: http://ec2-35-164-199-202.us-west-2.compute.amazonaws.com:8080/fhir-starter/?code=9qlmHS&state=4228bab2-0bb2-72ef-78a7-a02dfea2a24b

Query Parameters:
code : 9qlmHS
state : 4228bab2-0bb2-72ef-78a7-a02dfea2a24b

After redirect...

Token request

POST /openid-connect-server/token HTTP/1.1
Host: ec2-35-162-90-131.us-west-2.compute.amazonaws.com:8080
Accept: application/json, text/javascript, */*; q=0.01
Content-Type: application/x-www-form-urlencoded; charset=UTF-8
Referer: http://ec2-35-164-199-202.us-west-2.compute.amazonaws.com:8080/fhir-starter/

Form Data:
code : 9qlmHS
grant_type : authorization_code
redirect_uri : http://ec2-35-164-199-202.us-west-2.compute.amazonaws.com:8080/fhir-starter/
client_id : fhir_starter

Token response

HTTP/1.1 200 OK
Content-Type: application/json;charset=UTF-8

Body:
access_token : eyJhbGciOiJSUzI1NiJ9.eyJleHAiOjE0ODM0ODU5OTIsImF1ZCI6W...
expires_in : 3599
scope : "user/*.* smart/orchestrate_launch"

token_type : "Bearer"

Patient select request

GET /api-server/Patient/613876 HTTP/1.1
Host: ec2-35-164-199-202.us-west-2.compute.amazonaws.com:8080
Accept: application/json
X-Requested-With: XMLHttpRequest
Authorization: Bearer eyJhbGciOiJSUzI1NiJ9.eyJleHAiOjE0ODM0ODU5OTIsImF1ZCI6W…
Content-Type: application/json
Referer: http://ec2-35-164-199-202.us-west-2.compute.amazonaws.com:8080/fhir-starter/

Patient select response

HTTP/1.1 200 OK
Content-Type: application/json+fhir;charset=utf-8

Body:
<patient resource>

Select app and launch

GET /growth-chart/launch.html HTTP/1.1
Host: ec2-35-164-199-202.us-west-2.compute.amazonaws.com:8080
Referer: http://ec2-35-164-199-202.us-west-2.compute.amazonaws.com:8080/fhir-starter/launch.html?Tkvpd9Dka4Rstut11CWkcqW2BiePh3w1

Query Parameters:
iss : http://ec2-35-164-199-202.us-west-2.compute.amazonaws.com:8080/api-server
launch : 29

Growth Chart App

Authorize request

GET /openid-connect-server/authorize HTTP/1.1
Host: ec2-35-162-90-131.us-west-2.compute.amazonaws.com:8080
Referer: http://ec2-35-164-199-202.us-west-2.compute.amazonaws.com:8080/growth-chart/launch.html?iss=http%3A%2F%2Fec2-35-164-199-202.us-west-2.compute.amazonaws.com%3A8080%2Fapi-server&launch=29
Cookie: JSESSIONID=00C8CB1023B233E2D548A0C2F3607936

Query Parameters:
client_id : growth_chart
response_type : code
scope : patient/*.read launch
redirect_uri : http://ec2-35-164-199-202.us-west-2.compute.amazonaws.com:8080/growth-chart/
state : 27f414e8-b4aa-af7f-4b90-1d5b99f5ddc0
aud : http://ec2-35-164-199-202.us-west-2.compute.amazonaws.com:8080/api-server

launch : 29

Authorize response

HTTP/1.1 200 OK

Token request

POST /openid-connect-server/token HTTP/1.1
Host: ec2-35-162-90-131.us-west-2.compute.amazonaws.com:8080
Accept: application/json, text/javascript, */*; q=0.01
Referer: http://ec2-35-164-199-202.us-west-2.compute.amazonaws.com:8080/growth-chart/

code : 2rEPgS
grant_type : authorization_code
redirect_uri : http://ec2-35-164-199-202.us-west-2.compute.amazonaws.com:8080/growth-chart/
client_id : growth_chart

Token response

HTTP/1.1 200 OK

Body:
access_token : eyJhbGciOiJSUzI1NiJ9.eyJleHAiOjE0ODM1NzI0NjQsImF1ZCI6WyJncm...
expires_in : 3599
scope : launch patient/*.read
token_type : Bearer