# Memorandum

**Date**: 14 September 2020

**Subject**: CARIN Discussion on AWS Cognito Limitations for SMART on FHIR

**To**: Ryan Howells (Leavitt Partners)

**From:** Ryan Harrison (Amida), Elijah George (Amida)

**CC**: Sashi Ravipati (CNSI), Krishnamoorthi "BK" Brahmadesam (CNSI)

**Actions**: None

**Attachments:** None

## Cognito limitations for SMART on FHIR

CNSI and Amida attempted to configure AWS Cognito as a SMART on FHIR [1] compliant FHIR Auth Server (**Table 1**).

| Cognito Limitation | Standalone launch | EHR launch | Refresh | access_token.aud |
|---|---|---|---|---|
| **Cannot create scope without identifier (<identifier>/<scope>)** | | X<br>scope:<br>- launch | X<br>scope:<br>- offline_access<br>- online_access | |
| **Cannot modify /token response body** | X<br>scope:<br>- launch/patient | | | |
| **Cannot modify \`access_token\`** | | | | X |
| **Cannot access \`oauth2/authorize\` query parameters** | | X<br>query-param:<br>- launch | | X<br>query-param:<br>- aud |

***Table 1 – Summary of AWS Cognito limitations by SMART on FHIR requirement.*** *'X' indicates that the SMART on FHIR requirement (column header) is blocked by a (putative) Cognito limitation.*

## SMART on FHIR Capability support with Cognito

The Cognito limitations preclude supporting swaths of the SMART on FHIR specification. In **Table 2**, we summarize whether a SMART on FHIR Capability is allowed by Cognito.

| Capability | Description | Patient access CapabilitySet | Allowed by Cognito |
|---|---|---|---|
| launch-ehr | support for SMART's EHR Launch mode | | N[1] |
| launch-standalone | support for SMART's Standalone Launch mode | Y | Partial[2] |
| client-public | support for SMART's public client profile (no client authentication) | Y | Y |
| client-confidential-symmetric | support for SMART's confidential client profile | Y | Y |
| sso-openid-connect | support for SMART's OpenID Connect profile | | Y |
| context-banner<br>context-style<br>context-ehr-patient<br>context-ehr-encounter<br>context-standalone-encounter | Launch context | | N[3] |
| context-standalone-patient | support for patient-level launch context | Y | N |
| permission-offline | support for refresh tokens (requested by offline_access scope) | | Partial[4] |
| permission-patient | support for patient-level scopes (e.g. patient/Observation.read) | Y | N |
| permission-user | support for user-level scopes (e.g. user/Appointment.read) | | N |

***Table 2 – SMART on FHIR conformance summary.*** *Conformance definitions*.

[1] Cognito does not support i) `scope: launch` and ii) `query parameter: launch`

[2] Cognito does not support the SMART on FHIR required query parameter `aud`.

[3] Cognito does not support modifying the `/token` response body. This limitation impacts all launch context support.

[4] Cognito does not allow the creation of "bare" scopes for `scope: online_access` and `scope: offline_access`. However, each FHIR app client can be configured to allow refresh tokens. Unless a Cognito global logout is triggered, which invalidates all tokens, the FHIR app client will be able to use the `refresh_token`. In other words, where a FHIR app client is allowed `refresh_tokens` by Cognito (not configurable as a scope), there will be the same behavior as `Capability: permission-offline`.