FAST: Scalable Registration, Authentication, and Authorization for FHIR Ecosystem Participants

June 8, 2021
Project Page

- [https://confluence.hl7.org/display/SEC/FAST\%3A+Scalable+Registration\%2C+Authentication\%2C+and+Authorization+for+FHIR+Ecosystem+Participants](https://confluence.hl7.org/display/SEC/FAST%3A+Scalable+Registration%2C+Authentication%2C+and+Authorization+for+FHIR+Ecosystem+Participants)
Welcome New Participants

None this week
Timeline Progress

• HL7 FHIR Virtual Connectathon May 2021 completed!
  • Track page: [https://confluence.hl7.org/display/FHIR/2021-05+Cross+Organization+Application+Access](https://confluence.hl7.org/display/FHIR/2021-05+Cross+Organization+Application+Access)
  • 20 participants over the course of 3 days
  • Report-out available on HL7 connectathon 27 page

• FHIR IG proposal was approved by FMG last week

• NIB final deadline July 4 – plan to submit soon
  • HL7 still working on May ballot items
  • IG now listed at [HL7 Active Projects page (Security)](https://www.hl7.org/activeprojects), NIB not yet created

• Ballot for STU1 September 2021
FHIR Connectathon 27 - May 2021

• Track page: https://confluence.hl7.org/display/FHIR/2021-05+Cross+Organization+Application+Access

• Scenario 1: Trusted Dynamic Registration & JWT-Based Authentication (Consumer Facing)

• Scenario 2: Trusted Dynamic Registration & JWT-Based Authentication (B2B)

• Scenario 3: Tiered OAuth - Authentication using third party Identity Provider (IdP) via OpenID Connect (OIDC)

• Additional bonus scenarios detailed on track page
Porting UDAP IGs to FHIR IG template

• Source documents
  • https://www.udap.org/udap-ig-consumer-facing-health-apps.html
  • https://www.udap.org/udap-ig-b2b-health-apps.html

• Porting to FHIR IG builder requirements nearly complete
  • Draft local IG build reviewed with workgroup today

• Awaiting official github repo
  • Expected URL: http://build.fhir.org/ig/FHIR/udap-security/index.html
B2B Authorization Extension Object

- The following were reviewed in previous meetings:
  - Carequality “FHIR-Based Exchange IG v1.0” (12/1/20)
  - Commonwell “FHIR Client Dynamic Registration and Authorization” Draft v0.3 (4/26/21)
  - IHE’s IUA profile (incomplete UDAP compatibility, but extension object is constructed in UDAP format)

- Implementation examples were also reviewed for structural commonalities and differences (see 5/11/21 meeting slides)
Authorization Metadata – WG comments/recommendations (1 of 2)

• Certificate is used to determine the originating network for the request
  • This information does not need to be duplicated in the Authorization Extension Object

• Support for the following minimum authorization metadata elements is recommended for all participants:
  1. Purpose of Use – code or Coding? Multiple code systems in common use? system\code vs JSON Object
     • Code from value set defined by jurisdiction or trust community
     • Many codes in use today are carried over from old NHIN authorization framework documents (are these still maintained?) – is this the ‘de facto’ standard?
  2. Requesting Person Name (when applicable) – string, human readable, local convention
  3. Requesting Person Identifier (when applicable) – NPI appropriate for US Realm, what if no NPI?
     • Keep generic as “Requesting Person Identifier”? appropriate identifier for jurisdiction, e.g. NPI in USA
     • WG discussion 5/11 -- Realm: initial draft is US Realm, so we can use US specific concepts; later may consider making more generic for international use  \( \rightarrow \) e.g. replace NPI with “identifier”
     • General concept – jurisdiction or trust community should determine naming/code systems or value sets
  4. Requesting Person Role (when applicable) – similar issue, e.g. NUCC in USA
Authorization Metadata – WG comments/recommendations (2 of 2)

• Support for the following minimum authorization metadata elements is recommended for all participants (continued):

  5. Requesting Organization (human readable) - string
  6. Requesting Organization Identifier – uri most common, OIDs used in the wild, could be breaking change to use NPI. Prev WG comments:
     • should be a globally unique ID
     • should this be resolvable by the data holder from whom the request is made? Yes
     • i.e. requester only includes references that are resolvable by data holder
  7. Consent policy identifier(s) – again may have network or jurisdiction specific requirements
     • Array of URIs?
  8. Consent document location(s) – FHIR URI? Other URI?
     • Array of literal references? Consent and/or DocumentReference; must be resolvable?
Initial IG draft content based on 5/11/21 WG discussion for B2B Authorization Extension Object

• version
• subject_name – human readable name of subject (i.e. the human requester), if applicable, following local convention
• subject_id – unique identifier for subject (US Realm: use NPI)
• subject_role – code for role (US Realm: use NUCC)
• organization_name – human readable name of organization
• organization_id – unique identifier for subject (community/realm defined)
  • constrain to a URI, seek comment on constraining further
• purpose_of_use – code for purpose of use of requested data
  • community/realm defined; mapping legacy NHIN AF codes?
• consent_policy – array of URI identifying consent policy in force
• consent_reference – array of absolute FHIR resource URLs (DocumentReference|Consent)
Purpose of use codes

• CommonWell and Carequality currently using codes from NHIN Authorization Framework (2010)
  • http://hl7.org/fhir/R4/codesystem-nhin-purposeofuse.html
• Codes in use and possible mapping to HL7 POU codes (thanks to Jason)

  TREATMENT - TREAT
  OPERATION - HOPERAT
  REQUEST - PATRQT
  PUBLICHEALTH - PUBHLTH
  PAYMENT - HPAYMT
  COVERAGE - COVERAGE
  RESEARCH - HRESCH, there are more specific in HL7
Feedback from health information networks

• Assess willingness/readiness to change from NHIN codes to HL7 POU codes for networks participating in this workgroup
  • Dave Pyke will discuss this week with Carequality
  • Jason Vogt will discuss internally with CommonWell

• Options
  • Leave as HL7 POU required
  • Change to HL7 POU preferred
  • Change to remove specific value set; value set of allowed codes defined by trust community rather than constrained by it.
Updating/Deleting registration

• CQ (IG):
  • Update: Resubmit signed registration request with same identifying URI and new information
  • Delete: Resubmit signed registration request with same identifying URI and empty grant_types

• CW draft (hybrid IG/RFC7952):
  • Update: submit PUT request to special endpoint with same identifying URI
  • Delete: submit DELETE to special endpoint using a long lived bearer token provided at registration time

• IHE:
  • Not defined?