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

May 11, 2021

Welcome New Participants

- Jason Vogt, MEDITECH and CommonWell
- Richard Braman, Fly.Health
- Paul Wilder, CommonWell
- Jeff Hellman, SSA
- Aaron Seib, Onyx

Project Scope

- From PSS:

“The aim of this project is to expand upon the existing work by UDAP.org within the HL7 consensus process to produce a more complete set of implementation guides targeted at implementers of both client and server systems using FHIR for data exchange, standardizing how implementers integrate the UDAP profiles identified by the FAST Security Tiger Team into existing OAuth 2.0 and OpenID Connect workflows.”

Timeline Progress

- HL7 FHIR Virtual Connectathon May 2021
  - Track page: https://confluence.hl7.org/display/FHIR/2021-05+Cross+Organization+Application+Access
  - Registration closed Friday 4/30/21, but you still try to sign up late!
  - Email lcmaas@emrdirect.com to be listed as a track participant
  - Orientation recording available on Track Page
- FHIR IG proposal due by June 20
  - Dana is drafting – FMG is the only HL7 group to review this
  - Plan for submission this week
- NIB final deadline July 4 – plan to submit soon
  - waiting on HL7 to complete May ballot items
- Ballot for STU1 September 2021

FHIR Connectathon 27 – May 2021

- Track page: https://confluence.hl7.org/display/FHIR/2021-05+Cross+Organization+Application+Access
- Zulip stream: https://chat.fhir.org/#narrow/stream/179207-connectathon-mgmt/topic/Cross.20Organization.20Application.20Access

- 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

Existing UDAP IG's

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

- TODO: port to FHIR IG template
  - http://build.fhir.org/ig/FHIR/ig-guidance/index.html
  - https://github.com/HL7/ig-template-fhir
  - Will receive URL after IG approval completed

Comparison with Carequality UDAP framework (as discussed last meeting)

- Carequality FHIR IG (Version 1.0, December 1, 2020)
  - Aligns with Draft IGs
  - Algs: RS256 (SHALL), ES256 (SHOULD), ES384 + RS384 (MAY)
    - Note: draft IGs do not include RS384
  - Community Certifications: Basic App Certification (self-assertion)
  - Community Authorization Extension Objects: carequality, carequality_user
  - Community Authorization Extension Error Objects: carequality

B2B Authorization Extension Object

- Carequality “FHIR-Based Exchange IG v1.0” (12/1/20)
- Commonwell – internal documentation; updated documentation currently being drafted.
- IHE’s IUA profile (incomplete UDAP compatibility, but extension object is constructed in UDAP format)

Authorization Metadata – FAST Security TT 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 → 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 – FAST Security TT 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?

Implementation Examples

- "carequality": {
  "version": "1",
  "organization_id": "https://directory.carequality.org/Organization/2.16.840.1.113883.19.347473",
  "organization": "ABC Hospital",
  "subject_id": "Dr. Mary Johnson",
  "purpose_of_use": "TREATMENT",
  "acp": ["urn:oid:2.16.840.1.113883.3.7204.1.1.1.1.5"],
  "acp_reference": ["https://implementer1.example.com/fhir/R4/DocumentReference/consent-12345"]
  }

- "cw": {
  "role": "112247003",
  "subject-id": "Geoffrey Geiger",
  "organization": "St. Barnabas Hospital",
  "organization-id": "2.16.840.1.113883.4", ← organization supplied
  "purposeofuse": "TREATMENT",
  "npi": "1770589525"
  }

- NOTE: updated CommonWell examples will be available soon

Implementation Examples (cont)

- "ihe_iua" : {
  "subject_name": "Dr. John Smith",
  "subject_organization": "Central Hospital",
  "subject_organization_id": "urn:oid:1.2.3.4",
  "other_value": "..."
  }

  - subject_role (optional): Coded value indicating the user's role. If present, the value shall be formatted as FHIR Coding data type.
  - purpose_of_use (optional): Purpose of use for the request. If a coded value is used, the value shall be formatted as FHIR Coding data type.
  - home_community_id (optional): Home community identifier where the request originated. Its value should be an OID in URN notation.
  - national_provider_identifier (optional): A unique identifier issued to health care providers by their national authority.
  - person_id (optional): Patient identifier, Citizen identifier, or other similar public identifier.