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

April 27, 2021

Welcome

- James Norberg – Humana
- Steve Sullivan - Carequality
- Bill Mehegan – Carequality
- Patrick Haren – Cigna/Evernorth
- Tone Sutherland – OneRecord

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

- TSC: project approved 4/19/21
- HL7 FHIR Connectathon May 2021
  - Track page: https://confluence.hl7.org/display/FHIR/2021-05+Cross+Organization+Application+Access
  - Registration closes Friday 4/30/21
  - Email lcmaas@emrdirect.com to be listed as a track participant
- FHIR IG proposal due by June 20
  - Dana is drafting – FMG is the only HL7 group to review this
  - Status?
- NIB final deadline July 4 – plan to submit by end of April?
- 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
  - Two tabs instead of Two IGs: Consumer-Facing & B2B
    - Substantial overlap
    - Very different use cases

Comparison with Carequality UDAP framework

- 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
- IHE’s IUA profile (incomplete UDAP compatibility, but extension object is constructed in UDAP format)

Authorization Metadata – FAST Security TT recommendations

- Support for the following minimum authorization metadata elements is recommended for all participants:
  - Purpose of Use
  - Requesting Person Name (when applicable)
  - Requesting Person NPI (when applicable)
  - Requesting Person Role (when applicable)
  - Requesting Organization (human readable)
  - Requesting Organization Identifier
    - WG: globally unique ID
    - WG: should this be resolvable by the data holder from whom the request is made?
      - i.e. requester only includes references that are resolvable by data holder
  - Consent policy identifier(s)
  - Consent document location(s)

Other fields that may be useful identified by this WG

- Home community ID

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",
  "purposeofuse": "TREATMENT",
  "npi": "1770589525"
  }

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.