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

May 25, 2021
Welcome New Participants

Senthil – CommonWell
Andrei Zudin – Health Gorilla
Timeline Progress

• HL7 FHIR Virtual Connectathon May 2021 completed!
  • Track page: 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 due by June 20
  • Sec WG to review tomorrow, then FMG
  • Plan for submission to FMG following Sec WG approval

• NIB final deadline July 4 – plan to submit soon
  • HL7 still working on May ballot items

• Ballot for STU1 September 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)
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

- [https://www.udap.org/udap-ig-consumer-facing-health-apps.html](https://www.udap.org/udap-ig-consumer-facing-health-apps.html)
- [https://www.udap.org/udap-ig-b2b-health-apps.html](https://www.udap.org/udap-ig-b2b-health-apps.html)

- Will receive URL after IG approval received from FMG
  - Luis to create UDAP github repo pending official repo
    - Profile for CapabilityStatement rest service
  - [http://build.fhir.org/ig/FHIR/ig-guidance/index.html](http://build.fhir.org/ig/FHIR/ig-guidance/index.html)
  - [https://github.com/HL7/ig-template-fhir](https://github.com/HL7/ig-template-fhir)
B2B Authorization Extension Object

• 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)
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"],
}

• “commonwell” : {
  "version": "1",
  "subject_role": "112247003",
  "subject-id": "Geoffrey Geiger",
  "organization": "St. Barnabas Hospital",
  "organization_id": "2.16.840.1.113883.4",
  "purpose_of_use": "TREATMENT",
  "urn:oasis:names:tc:xspa:2.0:subject: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.
<table>
<thead>
<tr>
<th>Identifier</th>
<th>Type</th>
<th>Valid Values</th>
</tr>
</thead>
<tbody>
<tr>
<td>urn:oasis:names:tc:xacml:1.0:subject:subject-id</td>
<td>String</td>
<td>Is the name of the user as required by Health Insurance Portability and Accountability Act (HIPAA) Privacy Disclosure Accounting. The name will be typed as a string and in plain text.</td>
</tr>
<tr>
<td>urn:oasis:names:tc:xpsa:1.0:subject:organization</td>
<td>String</td>
<td>Organization the requestor belongs to as required by Health Insurance Portability and Accountability Act (HIPAA) Privacy Disclosure Accounting.</td>
</tr>
<tr>
<td>urn:oasis:names:tc:xpsa:1.0:subject:organization-id</td>
<td>anyURI</td>
<td>Unique identifier of the consuming organization and/or facility</td>
</tr>
<tr>
<td>urn:oasis:names:tc:xpsa:1.0:subject:hl7:permission</td>
<td>String</td>
<td>Refer to [HL7-PERM] and its OID representation.</td>
</tr>
<tr>
<td>urn:oasis:names:tc:xspa:1.0:subject:purposeofuse</td>
<td>String</td>
<td>TREATMENT, PAYMENT, OPERATIONS, EMERGENCY, SYSADMIN, MARKETING, RESEARCH, REQUEST, PUBLICHEALTH</td>
</tr>
<tr>
<td>urn:oasis:names:tc:xacml:1.0:resource:resource-id</td>
<td>String</td>
<td>Unique identifier of the resource defined by and controlled by the servicing organization. In healthcare this is the patient unique identifier.</td>
</tr>
<tr>
<td>urn:oasis:names:tc:xspa:1.0:resource:hl7:type</td>
<td>String</td>
<td>For minimum interoperability set of objects and supporting actions refer to [HL7-PERM] and their OID representations.</td>
</tr>
<tr>
<td>urn:oasis:names:tc:xpsa:1.0:environment:locality</td>
<td>String</td>
<td>Unique identifier of the servicing organization.</td>
</tr>
</tbody>
</table>

Table 2 from http://docs.oasis-open.org/security/xspa/v1.0/saml-xspa-1.0.html
Seeking consensus on minimal fields 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)
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?