2022-05 FAST Security & Identity

- **Short Description**
  - This track tests scalable ecosystem Security trust models and Identity requirements used by FAST, Carequality, CARIN, and others. Focus is on security and privacy, including client app registration, authentication and authorization for cross-organization query, endpoint validation, interoperable identity and patient matching (Scenario 6 on patient matching is the focus of this track for the May Testing Event; see also Scenarios 3 & 5).

- **Long Description**
  - Generate discussion about how to recognize certain classes of users, clients, or servers, reducing friction in ecosystem use of FHIR and working to develop best practices
  - Build on successes of previous work in Montreal at this track, in Atlanta, and at the May and September 2020, January, May, and July 2021, and January & February 2022 virtual connectathons.

  **Track Preparation:** Please see the following three videos for a detailed introduction to the identity topics in this track (including some information about Security topics in the 3rd video, though Security is not a focus of the February testing). Note that the Agenda for this event is immediately below, as the agenda in the videos is out of date.

  1- Identity Scenario Consumer & B2B Workflows Overview from September 2021 Connectathon
  2- Identity Scenario Update/Readiness Discussion/Q&A from September 2021 Connectathon
  3- Final Identity Scenario Pre-connectathon Overview including both Identity & Security focused scenarios from September 2021 Connectathon

- **Agenda**
  - **Day 1**
    - Welcome & Intros
      - Welcome, general introductions & overview of Reference Implementation status
  - Technical Breakout Session
    - Patient Profiling to Express Demographics for Improved Matching
  - Technical Breakout Session
    - Reference Implementation Overview Presentation
  - General Testing
  - **Day 2**
    - Welcome
      - Welcome, Day 2 Kick-off, Recap of Day 1 and Q&A,
      - Securing FAST Directory Access,
      - Feedback on Best Practice Identity Verification and Digital Identity Requirement,
      - Continued Discussion of Best Practice Match Guidance
  - General Testing
    - Patient use cases/patient engagement with guest speakers from OneRecord
<table>
<thead>
<tr>
<th><strong>Type</strong></th>
<th>Test a FHIR-associated specification</th>
</tr>
</thead>
</table>
| **Submitting Work Group/Project/Affiliate/Implementer Group** | Security Workgroup, Patient Administration Workgroup  
FHIR at Scale Taskforce (FAST): Identity Tiger Team  
FHIR at Scale Taskforce (FAST): Security Tiger Team |
| **Track Lead(s)** | Julie Maas, Jeff Brown |
| **Track Lead Email(s)** | julie@emrdirect.com, jeffbrown@mitre.org |
| **Related Tracks** | This track is not FHIR version specific. |
| **FHIR Version** | This track is not FHIR version specific. |
| **Specification(s) this track uses** | Implementation Guides:  
Security for Scalable Registration, Authentication, and Authorization v1.0.0 (continuous build version, not yet published)  
Interoperable Digital Identity and Patient Matching  
UDAP Information:  
UDAP Implementation Guide for Registration and Authorization of Business-to-Business Health Apps  
UDAP Implementation Guide for Registration and Authorization of Consumer Facing Health Apps  
- UDAP Dynamic Client Registration (DCR) - for clients that use authorization code or client credentials grants  
- UDAP JWT-Based Client Authentication  
- UDAP Tiered OAuth for relying on another OAuth server  
- UDAP Server Metadata for endpoint validation  
Related Implementation Guides:  
- Carequality FHIR Implementation Guide  
- CARIN Consumer Directed Payer Data Exchange (CARIN IG for Blue Button®) - Registration Authentication and Authorization  
- Da Vinci Health Record Exchange (HRex)  
- ONC FAST Identity Tiger Team Proposed Solutions and related PSS  
- ONC FAST Security Tiger Team Proposed Solutions and related PSS |
| **Artifacts of focus** | Google Slides for Additional Background & Notes |
| **Expected participants** | 4medica  
EMR Direct  
Evernorth  
MITRE  
OneRecord  
Add your name here! |
| **Zulip stream** | FAST Security Stream (Scenarios 1-4)  
FAST Identity Stream (Scenarios 5, 6, and match-related aspects of 3)  
*NOTE: These are both relatively new streams for connectathons & related IG work, that we'll use moving forward.* |
**Track Kick Off Call**

### Track Details

**System roles**

UDAP-enabled client, UDAP-enabled server, UDAP-enabled identity provider

This public “UDAP Implementers” Google sheet is continuously available and contains a tab for UDAP adoption “Beyond Sandbox Use” too; please add your own information there to encourage cross-testing!

Please find the tab specific to this connectathon.

UDAP-enabled clients are capable of trusted dynamic registration and JWT-based authentication and optionally Tiered OAuth and Server Metadata.

UDAP-enabled servers are capable of trusted dynamic registration and JWT-based authentication and optionally Tiered OAuth and Server Metadata.

UDAP-enabled identity providers are capable of the IdP side of Tiered OAuth, including other client and server components as above.

**Prerequisites**

Scenarios 1-4 leverage trusted digital certificates; in addition to scenario-specific preconditions, participants will also want to:

- Obtain a certificate from UDAP.org or share your certificate’s trust anchor in the UDAP Implementers Google sheet
- Configure trust with the EMR Direct Test CA and other participants’ anchors

**Scenarios**

1. **Trusted Dynamic Registration & JWT-Based Authentication (Consumer Facing)**

   This scenario tests the ONC FHIR at Scale Taskforce (FAST) Security solution for user-facing apps

   Precondition: User has user-level credentials for FHIR server and client’s UDAP certificate is trusted

   Action: Client app registers, user authenticates, and client app requests FHIR data

   Success Criteria: Client app successfully registers, user successfully authenticates, and client app obtains FHIR data. Client should validate server metadata per UDAP Server Metadata profile.

   Bonus point: Client and server use Tiered OAuth to authenticate user with trusted OpenID account from a third party instead of credential provisioning native to FHIR server

   Bonus point: Include (on server side) and validate (within clients) signed endpoints

   Bonus point: Multi Factor Authentication

2. **Trusted Dynamic Registration & JWT-Based Authentication (B2B)**

   This scenario tests the ONC FHIR at Scale Taskforce (FAST) Security solution for business-to-business apps

   Precondition: Client’s UDAP certificate is trusted

   Action: Client app registers, authenticates, and requests FHIR data

   Success Criteria: Client app successfully registers, authenticates, and obtains FHIR data leveraging a trusted certificate. Client should validate server metadata per UDAP Server Metadata profile.

   Bonus point: Client and server use Tiered OAuth to authenticate user

   Bonus point: Authenticated Client performs a $match request and server responds to the request

   Bonus point: Include the Carequality FHIR IG Authorization Extension Object in your requests (clients) and process these objects (servers)

   Bonus point: Include (on server side) and validate (within clients) signed endpoints

   Bonus point: Multi Factor Authentication

3. **Authentication using third party Identity Provider (IdP) via OpenID Connect (OIDC)**

   This scenario tests additional elements specific to ONC FAST Identity solution #3, Networked Identity Management

   Action:
Client app initiates **UDAP Tiered OAuth** connection to OAuth server's authorization endpoint, identifying user's preferred OIDC IdP (rather than the native OAuth server)
- OAuth server redirects user to IdP authorization endpoint (server acts as client of IdP)
- User authenticates and authorizes access to identity information
- OAuth server exchanges authorization code from IdP for token and id_token, optionally retrieves additional info from IdP's userinfo endpoint
- OAuth server determines authority of user based on available identity information, pre-registration of the ID, or other out of band interaction with the end user
- Authenticated user authorizes client app to access **FHIR resources**
- Client exchanges authorization code from OAuth server for token, and access FHIR resources

**Preconditions:**
- OAuth server (securing FHIR resources) and client app support UDAP Tiered OAuth
- Client is registered with OAuth server for authorization_code flow
- OAuth server (data holder) is registered with IdP for authorization_code flow

**Success Criteria:**
- Client app can access FHIR resources

**Bonus points:**
- OAuth server registers dynamically with IdP using UDAP DCR
- Client app registers dynamically with OAuth server using UDAP DCR
- IdP uses Multi Factor Authentication

4. **Validation of FHIR endpoint managing organization in multi-tenant environment**

This scenario tests additional aspects of the ONC FAST Security and Identity solutions

**Action:**
- Client app validates trust with server endpoint before proceeding to OAuth sign in page per **UDAP Server Metadata** profile.
- Server validates trust with client app
- Flow continues, using information from previous step (happy path: user authenticates and authorizes client app to access FHIR resources)/TBD

**Precondition:**
- FHIR endpoint certificate advertisement, demonstrating control of key

**Success Criteria:**
- Client app can access FHIR resources (happy path)

**Bonus point:** Include and validate signed endpoints

5. **Patient matching using OpenID Connect account**

This scenario tests additional aspects of the ONC FAST Security solution and is also related to ONC FAST Identity solution #3, Networked Identity Management

For example, could store as identifier with:
- `Identifier.system = Issuer Identifier URI`
- `Identifier.value = Subject Identifier assigned by Issuer`

**e.g.**
Action:

Search on OpenID subject identifier
e.g. GET [base]/Patient?identifier=https://as.example.com/issuer1|1234567

Precondition:
The data holder confirmed the binding of an OIDC subject identifier to the person named in a Patient (or equivalently to a Practitioner, Person, or RelatedPerson) resource using a suitable registration process before adding the identifier.

Success Criteria:
Client app can access FHIR resources for the correct patient linked to the OIDC subject identifier.

Bonus point: Use OpenID Connect user profile information to match on patient

6. Best practice probabilistic patient matching (DRAFT; feedback requested)

This scenario is a starting point for prototyping and discussion of higher-assurance matching events involving the use of workflow-specific attributes with some data verification or an interoperable identifier, stronger identity assurance and opportunity to involve the subject (patient) for consent and/or notification. Key questions for further discussion as the Interoperable Digital Identity and Patient Matching Capabilities IG IG is written include:

- Minimum required demographics for various use cases
- Digital Identity requirements for building interoperable identifiers
- Best practices for representing verified attributes and identifiers in FHIR, recognizing that verification events occur at a point in time and may exist among self-asserted or otherwise non-validated data in health records
- Best practices for managing identity (to include verified attributes and identifiers) in the broader context of a Patient and how that relates to encounter-level identity

Preconditions:
FHIR Match Server and Match Client app support the FHIR patient $match operation with additional profiling as defined here and in the IG

Alternative approach 1: FHIR server and client app accept an alternative OIDC IdP and server obtains attributes for matching from user profile

Alternative approach 2: FHIR server and client app support UDAP JWT-Based Client Authentication and matching attributes are exchanged through assertion object

*More specifics on each of these workflows will be added in the next few days to provide more steps to guide implementers; please ask any specific questions on Zulip

Success Criteria:
Matching patient ID is returned by FHIR server

Bonus point: Demonstrate use of "weighted" information patient profiles (Level 0 and/or Level 1) for input to $match operation
B2B Workflow

Step 1: Match Client makes a $match request to responder Match Server:

```json
POST [base]/Patient/$match

[required headers]
{
    "resourceType": "Parameters",
    "id": "example",
    "parameter": [  
        {  
            "name": "resource",
            "resource": {  
                "resourceType": "Patient",
                "name": [  
                    {  
                        "family": [  
                            "Newman"
                        ],
                        "given": [  
                            "Alice"
                        ]
                    ]
                },  
                "gender": "female",
                "birthDate": "1970-05-01"
            },  
            "telecom": [  
                {  
                    "system": "phone",
                    "value": "5557771234",
                    "use": "mobile"
                }
            ]
        },  
        {  
            "name": "count",
            "valueInteger": "10"
        },  
        {  
            "name": "onlyCertainMatches",
            "valueBoolean": false
        }
    ]
}
```


Step 2: Match Server returns match result; in this B2B case a certain match is not required so the server returns multiple matches, at most 10 in this example, with various match confidence values:

```
HTTP/1.1 200 OK
[required headers]
{
  "resourceType": "Bundle",
  "id": "26414249-18b3-45de-b10e-dca039172b",
  "meta": {
    "lastUpdated": "2021-08-10T03:28:49Z"
  },
  "type": "searchset",
  "total": 2,
  "entry": [{
    "fullUrl": "http://server/path/Patient/example",
    "resource": {
      "resourceType": "Patient",
      "id": "example",
      ... snip ...
    },
    "search": {
      "extension": [{
        "url": "http://hl7.org/fhir/StructureDefinition/match-grade",
        "valueCode": "certain"
      }],
      "mode": "match",
      "score": 0.9
    }
  },
  "fullUrl": "http://server/path/Patient/292",
  "resource": {
    "resourceType": "Patient",
    "id": "292",
    ... snip ...
  },
  "search": {
    "extension": [{
      "url": "http://hl7.org/fhir/StructureDefinition/match-grade",
      "valueCode": "possible"
    }],
    "mode": "match",
    "score": 0.9
  }
}]
```

B2C Workflow

**Required attributes:** all known patient demographic attributes, however responders are not required to return a result unless match confidence is certain

Step 1: Match Client makes a $match request to responder Match Server:

```
POST [base]/Patient/$match
[required headers]
{
  "resourceType": "Parameters",
  "id": "example",
  "parameter": [
    {"name": "resource",
     "resource": {
      "resourceType": "Patient",
      "name": [
        {
          "family": [
            "Newman"
          ],
          "given": [
            "Alice"
          ]
        }
      }
    }
  ]
}
```
Step 2: Match Server returns match result; in this case a certain match IS required, so the server returns at most one result
B2C Vaccination encounter matching

This is a similar use case for consideration in a future scenario. Trust of signed vaccination encounter data including associated demographics can be validated and the demographic elements used in matching. Today, attributes available for matching in vaccination credentials are: name, DOB, and identity assurance level (the latter informs what confidence is in the attributes per this SHC value set). The VCI standard includes identity assurance level as a required meta security tag on an immunization and the expression of a level indicates confidence in asserted attributes. The Interoperable Digital Identity and Patient Matching IG welcomes input on additional ways demographic element verification can be expressed, that could be helpful to match responders.

Security and Privacy Considerations:

Aspects of this track focus on security and privacy. OAuth (client credentials, authorization code, and dynamic client registration), OpenID Connect, UDAP profiles, and PKI are usually in scope. One exception to this is Scenario 6, where both B2B and B2C workflows are intended to leverage B2B security in a production setting, may be easiest to test with unsecured servers.