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

Luis Maas, MD, PhD
May 28, 2021
The ONC FHIR at Scale Taskforce’s Security Tiger Team was formed in late 2018 to investigate scalability issues for FHIR and identify potential solutions. The Tiger Team identified the Unified Data Access Profiles (UDAP) for Dynamic client registration, client authentication, client authorization, and Tiered OAuth as building blocks to be used by implementers to address the issues above and enhance the overall scalability of the FHIR ecosystem.

Current 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.”
Implementation Guide Topics (from PSS)

- integration of existing public key infrastructure mechanisms with registration, authentication, and authorization processes to establish robust trust networks with reusable credentials to identify actors

- trusted dynamic client registration

- client app submissions of self-assertions, third party certifications, or other endorsements to servers, and vice-versa

- client app assertions of additional information for a given session so that resource holders can more finely scope access tokens, including information related to consent or purpose of use

- increase security and assurance in identity of all actors by using asymmetric cryptographic methods for authentication, including specific protocols to support network-wide revocation of credentials

- dynamic federation of user credentials to facilitate reuse of credentials and single sign-on
UDAP IGs: the starting point for first FHIR IG

- [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)

- Porting of these IGs to the standard FHIR IG format is in progress
  - Will be hosted in udap-tools github pending assignment of HL7 github repo

- These are being assembled into one FHIR IG due to significant overlap
  - numerous common requirements, especially around general JWT requirements, discovery and dynamic registration
  - separate sections focusing on differences for the two use cases, especially around authorization and authentication
HL7 Calendar

• HL7 FHIR Virtual Connectathon May 2021
  • 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
  • pending approval by FMG
  • on FMG agenda June 2

• NIB by July 4

• Ballot for STU1 September 2021
What is UDAP?

**UDAP JWT-Based Client Authentication**: Increase security by using asymmetric cryptography to authenticate client applications

**UDAP Trusted Dynamic Client Registration**: Identify and dynamically register trusted client applications, streamlining app management

**UDAP Tiered OAuth**: Reusable identities via scalable, dynamic, cross organizational user authentication

**UDAP JWT-Based Authorization Assertions**: Extensible JWT-based client authorization grants and

**UDAP Certifications & Endorsements**: Other Trusted Informational Assertions

Trademark Notice: UDAP and the ecosystem gears design are trademarks of UDAP.org and are used with the permission of UDAP.org.
Swimlane Overview

Trusted Dynamic Client Registration & Token Request

Participant’s Client App

UDAP Dynamic Client Registration request (signed with client’s certificate-backed key)

- Client submits:
  - Client name
  - Redirect URIs?
  - Token Endpoint Auth Method
  - Grant type client credentials

Authorization and/or Authentication JWT using client_id (signed with same key)
- e.g. UDAP JWT-Based Client Authentication

Access Token

Registration Endpoint

Policy Engine <rules>

Registration Response

Policy Engine <rules>

Authz & Token Endpoints
UDAP Trusted Dynamic Client Registration

• An automated registration API
  • replace (and standardize) manual developer registration processes

• Trusted app operator identities
  • reusable credentials
UDAP Certifications and Endorsements

- Integral part of UDAP Trusted DCR
- Apps can include additional information automatically
- Self-asserted or validated by third party (e.g. EHNAC)
  - e.g. privacy and security assessments, patient disclosures
- Increased confidence for actions beyond read-only access
UDAP JWT-Based Client Authentication

• Increased security over shared secrets
  • e.g. RSA, Elliptic Curve
• Simplified Key Management
  • Public Key Infrastructure
• Increased confidence for actions beyond read-only access
Token Request – authorization code flow

**Implementer’s Client App**

- Token Request
- Implementer's Client App

**User’s Browser**

- User's Browser
- GET https://{redirect}?code={auth_code}&state=123

**Authorization Endpoint**

- Authorization Endpoint
- App sends user to authz endpoint
- GET https://{authz}?response_type=code &client_id={client}&state=123&scope=s1+s2 &aud={fhirBase}&redirect_uri={redirect}
- Server redirects user to app
- 302 Found
- Location: https://{redirect}?code={auth_code}&state=123

**Token Endpoint**

- Token Endpoint
- Server returns access token for use with FHIR endpoint
- POST https://{token}
  - grant_type=authorization_code&code={auth_code}
  - &client_assertion_type=urn:ietf:params:oauth:client-assertion-type:jwt-bearer&client_assertion={JWT_goes_here}&udap=1

**Authz Engine**

- Validates audience, client ID, and redirect URI
- Interacts with user
- Authenticates user
- Obtains user authorization so app can use requested scopes

**Policy Engine**

- Validate JWT & certificate chain
- Validate auth code
- Optional purpose assertion

---

Art credit: adapted from ONC FAST communications collateral
OAuth Sign In Page with Trusted DCR

Dynamic **Client** Registration (DCR) provides additional details when used in a Trusted model through digital certificates:

- App Discovery & Validation, Reusable Client Vetting
- Automated registration details (not validated)
- Additional details from trusted digital certificate
Token Request – client credentials flow

Implementer’s
Client App

User’s
Browser

Authorization Endpoint

Token Endpoint

App sends user to authz endpoint
GET https://{authz}?response_type=code&client_id={client}&state=123&scope=s1+s2&aud={fhirBase}&redirect_uri={redirect}

Server redirects user to app
302 Found
Location: https://{redirect}?code={auth_code}&state=123

Client constructs authentication JWT and requests token using JWT per UDAP JWT-Based Client Authentication

Server returns access token for use with FHIR endpoint
200 OK
{"access_token": "random_UUID_or_other_token_issued_by_AS", "token_type": "Bearer", "expires_in": 3600 }
UDAP Tiered OAuth with Trusted Dynamic Registration

Requestor Actor
Client App

User’s Browser

Responder Actor
Authorization Endpoint

Responder Actor
OIDC Endpoints

3a
App sends User to authorization endpoint

3b
Server redirects User back to App

App receives code

Responders use OpenID Connect to authenticate User

Authentication Response

Authenticate/Authorize (CC2)

Role/Context Identification (CC9)

Art credit: adapted from ONC FAST communications collateral
UDAP Tiered OAuth with Trusted Dynamic Registration

Requestor Actor

Client App

User’s Browser

App sends User to authorization endpoint
"idp": "https://myidp.com/"

1

Responder Actor

Authorization Endpoint

Responder gets metadata and validates trust

2

Registration Response (including client_id)

Responder dynamically registers with OIDC IdP if not previously registered;

3

User interacts with IdP to complete Authentication

4

IdP provides ID token to responder

5

Responders redirects user agent if additional interactions with user are required;

6

Responder provides ID token to responder

7

Server redirects User Back to App (success or failure)

Art credit: adapted from ONC FAST communications collateral
Thank you!

lcmaas@emrdirect.com