UDAP Technical Overview
Adding scalability and security to API transactions with trusted certificates

September, 2022
UDAP High Level Overview

• Client app obtains digital certificate; some attributes may be validated by CA
• Interactions with registration & token endpoints are then automated

Client certificate

Transaction Request

• Each participant can be reliably identified, including servers, identity services, and issuers of other claims

Response

• Data Holders and other relying parties can dynamically discover participant attributes & use to inform policy decisions (registration request, token request, authorization)
UDAP Trusted API Ecosystem

Trademark Notice: UDAP, the UDAP green lock and the UDAP ecosystem gears designs are trademarks of UDAP.org and are used with the permission of UDAP.org.
OAuth Sign In Page with UDAP Trusted Dynamic Client Registration

- Digital certificates enable:
  - OAuth server indicates verified app details
    - Client app details from trusted issuers
    - Client uses certificate for registration & authentication
  - Clients validates UDAP Server Metadata
    - Proceed to ABC Hospital System’s server?
  - Identity Provider trust, for reusable identity, or to validate other claims
    - Vaccination status, identity attributes, etc.
UDAP 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 URL?
  - 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

Authz & Token Endpoints

- Policy Engine <rules>

Art credit: adapted from ONC FAST communications collateral
Frictionless Cross-Organization Matching with Digital Identity-Overview (Identity IG)

**Requestor**

1. Prerequisite: **Subject uses a credential such as a patient portal account** (or other trusted OpenID Connect account) with ability to allow Responder to obtain verified demographic info from user profile.

2. Authorization Request with profile information about **Subject**.

3. **Networked Identity Management via Subject’s Own OpenID Credential and Authorization Code Flow with UDAP Tiered OAuth**


**Responder**

- Uses metadata to match locally.
- If Subject of Requestor’s query cannot be resolved, Responder may contact Subject or Issuer for additional information e.g. out of band resolution.

Prerequisite:
- **Subject uses a credential such as a patient portal account** (or other trusted OpenID Connect account) with ability to allow Responder to obtain verified demographic info from user profile.

Art credit: Adopted from ONC FAST materials.
Frictionless Cross-Organization Matching with Digital Identity-Deep Dive (Identity IG)

Not pictured but also part of this transaction:
- Requestor->Responder UDAP DCR
- Requestor->Responder UDAP JWT-Based Client Authentication (B2C)

Art credit: Adopted from ONC FAST materials.
Implementing the UDAP Trusted Ecosystem

**UDAP JWT-Based Client Authentication:**
Uses asymmetric cryptography to authenticate client apps

**UDAP Server Metadata:**
Endpoint validation for added confidence

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

**UDAP JWT-Based Authorization Assertions:**
Extensible JWT-based client authorization grants, identity & other claims incidental to a token request

**UDAP Certifications & Endorsements:**
Trusted informational assertions

**UDAP Tiered OAuth:**
Reusable identities via scalable, dynamic, cross organizational user authentication
Glide path
UDAP Ecosystem Benefits

• **Scalability**
  » Frictionless app onboarding & life cycle management; automated discovery
  » Reusable credentials for apps, servers, & users

• **Security**
  » Trusted apps and servers are identified through digital certificates, eliminating 1) app impersonation due to a compromised secret, 2) server impersonation leading to compromised user’s or app’s credentials or compromised PII or PHI, and 3) data provenance and credential trust issues
  » Exchange health data directly between trusted endpoints & trust the source of assertions made, e.g. Purpose of Use, HIPAA Authorization, verified Identity Attributes

  - Identity information is exchanged directly from IdP to FHIR server using Tiered OAuth
  - Verifiable directory information and endpoint identity
HL7 Interoperable Digital Identity and Patient Matching Implementation Guide – user profile

```json
{
  "iss": "https://generalhospital.example.com/as",
  "sub": "328473298643",
  "identifier": "123e4567-e89b-12d3-a456-426614e174000a",
  "name": "http://udap.org/code/auth/aal2",
  "ac": "http://udap.org/code/10/1a12",
  "name": "Jane Doe",
  "given_name": "Jane",
  "family_name": "Doe",
  "birthdate": "1979-01-01",
  "address": {
    "street_address": "1234 Hollywood Blvd.",
    "locality": "Los Angeles",
    "region": "CA",
    "postal_code": "90210",
    "country": "US"
  },
  "email": "janedoe@example.com",
  "picture": "https://generalhospital.example.com/fhir/Patient?identifier=https://generalhospital.example.com/issuer1|123e4567-e89b-12d3-a456-426614e174000a"
}
```