OAuth2 and OpenID Connect
A 5 Minute Introduction
ALAN VIARS
OAuth2 is a Framework for Delegated Access

- Delegated access is achieved in an “access_token”.
- The access_token is used to access to online resources. This includes machine readable APIs such as FHIR resources.
- There are several possible “flows” to get an access_token.
- The “authorization_code” flow is the most vanilla and arguably inherently more secure than the “implicit” flow.
- The “authorization_code” flow requires the client can keep a secret, but the “implicit” flow does not.
- Implicit flow will work for client applications that live in a web browser. (e.g. JavaScript)
- “Scopes” are OAuth2 concept. Scopes are labels used to tag some limited access.
OAuth2 – What it Isn’t

• OAuth2, the standard itself, is NOT a single-sign-on solution. (It is often used in single-sign-on and easily conflated with single-sign-on.)
• OAuth2 does not specify how to get user details, but user details is an almost ubiquitous requirement.
• Instagram Example: Request User Profile Information: https://api.instagram.com/v1/users/self/?access_token=ACCESS-TOKEN
GET /users/self

https://api.instagram.com/v1/users/self/?access_token=ACCESS-TOKEN

```
{
  "data": {
    "id": "1574083",
    "username": "snoopdogg",
    "full_name": "Snoop Dogg",
    "profile_picture": "http://distillery.s3.amazonaws.com/profiles/profile_1574083_75sq_1295469061.jpg",
    "bio": "This is my bio",
    "website": "http://snoopdogg.com",
    "is_business": false,
    "counts": {
      "media": 1320,
      "follows": 420,
      "followed_by": 3410
    }
  }
}
```
User Detail APIs are Often Custom

- Facebook, Instagram, LinkedIn,.... Everyone is doing it a little bit differently.
- OpenID Connect defines a standard for user profile information.
- OpenID Connect defines a service discovery standard, which may include the user information endpoint.
- The service discovery endpoint is a JSON document at this URL:
  - /.well-known/openid-configuration
Open ID Connect Discovery Example

```
{
  "grant_types_supported": [
    "authorization_code",
    "implicit",
    "refresh_token"
  ],
  "token_endpoint_auth_methods_supported": [
    "client_secret_basic",
    "client_secret_post"
  ],
  "issuer": "https://alpha.verifymyidentity.com",
  "userinfo_endpoint": "https://alpha.verifymyidentity.com/o/userinfo",
  "authorization_endpoint": "https://alpha.verifymyidentity.com/o/authorize",
  "token_endpoint": "https://alpha.verifymyidentity.com/o/token",
  "revocation_endpoint": "https://alpha.verifymyidentity.com/o/revoke_token",
  "response_types_supported": [
    "code",
    "token",
    "id_token",
    "id_token token",
    "code token",
    "code id_token",
    "code token id_token",
    "none"
  ],
  "scopes_supported": [
    "openid"
  ]
}```
OpenID Connect User Profile Response

```json
{
    "sub": "304685313797962",
    "family_name": "VIARS",
    "given_name": "ALAN",
    "email": "aviars@videntity.com",
    "email_verified": false,
    "birthdate": "1919-01-01",
    "gender": "male",
    "name": "ALAN VIARS",
    "nickname": "silverfox",
    "phone_number": "+13046853137",
    "phone_verified": true
}
```
Open ID Connect (OIDC): What is It?

• Open ID Connect (OIDC) is OAuth2. OIDC sits on top of OAuth2.
• Open ID Connect is a standard for Single-Sign-on
• Defines discovery and user info endpoints as discussed earlier.
• Open ID Connect is a modern replacement for SAML.
  • SOAP/XML is dead. Long live REST/JSON.
• Instead of, or in addition to, the “access_token”, OpenID Connect returns an “id_token”. This token is in a very specific format called JWT, which is like digitally signed JSON (i.e. machine readable) document.
• The payload of an identity “id_token” looks a lot like the user profile response shown earlier.
The Identity Token “id_token”

• The validity of the id_token is established by verifying the signature by using the public key.
• The URL for the public key is found in the discovery documents found at:
  • /.well-known/openid-configuration

• The “id_token” can have a ton of information such as a list of addresses.
• Using “Profiles” even more information can be standardized including:
  • Identifiers / document IDs (e.g. a driver’s license number or a Medicaid number)
  • Identity Assurance Information
• Relevant Profiles:
  • Open ID Connect for Identity Assurance: https://openid.net/specs/openid-connect-4-identity-assurance.html
  • Open ID Connect International Government Assurance Profile: https://openid.net/wg/igov/
  • HEART Profiles - https://openid.net/wg/heart/
OAuth2 Now Has a Discovery Spec

https://tools.ietf.org/html/rfc8414 says the URL shall be:
- ./well-known/oauth-authorization-server
"verified_person_data": {
  "verification": {
    "trust_framework": "us_nist_800_63_3",
    "method": "TRUSTED-REFEREE-VOUCH",
    "ial": "2",
    "date": "2019-05-22",
    "claims": {
      "given_name": "ALAN",
      "family_name": "VIARS",
      "birthdate": "2000-01-01",
      "gender": "male"
    }
  }
}
Thanks for Listening

- Alan Viars, President Videntity aviars@Videntity.com | +1 304-685-3137
- Links to open source code can be found on http://transparenthealth.org
Trusted Dynamic Client Registration
Tools to increase scalability and confidence in the HL7 FHIR® ecosystem

LUIS MAAS, MD, PHD | CTO, EMR DIRECT
LCMAAS@EMRDIRECT.COM, 858 367 0770
@EMRDIRECT, @UDAPTOOLS
Trusted Dynamic Client Registration

• About EMR Direct
  • Health IT software vendor providing Direct Messaging, HL7 FHIR, Identity Management, & Certificate Authority services to 150+ EMRs & other apps
  • UDAP –series of profiles adding scalability & confidence in the HL7 FHIR® ecosystem
• Want to reuse any app vetting performed in context of one EMR Vendor, rather than silo that approval to the context of 1 vendor
• Would like to reuse patient and provider credentials rather than create new ones for each health system
  • Similar problem: keeping track of patient and provider identity across systems
  • Magnified by: emergent increased identity and authentication standards (NPRM)
OAuth Sign In Page with Anonymous Client Registration

- API for app registration without manual user interaction—“headless”
- Purpose: scale registration & discovery of verified attributes about client apps, servers, users, +assertions such as purpose, policies & agreements
- Uses digital signatures for authenticity & integrity
- Manage the same app over time
Oauth Sign In Page with Trusted Client Registration

Dynamic Client Registration (DCR) provides additional details in Trusted model:
- User Authorization: Pre registered or Discoverable Identity;
- Client may access Health Data & Consents

Trusted FHIR Server:
- Discovery, Validation, Provenance

User Authorization:
- Pre registered or Discoverable Identity;
- Client may access Health Data & Consents

ABC Hospital System

Authorize access to health data by HealthToGo (using UDAP Trusted DCR)*

By clicking Authorize, you agree to the ABC Hospital System Terms of Use and Privacy Policy, and request that ABC Hospital System share with HealthToGo (using UDAP Trusted DCR) the following health information accessible using your credentials:

- Personal information, such as name, birthdate, gender, and other demographics
- Observations, such as lab results, vital signs, imaging, and social history
- Conditions, such as medical problems, diagnoses, and health concerns
- Documents, such as summaries of care and discharge summaries
- Records relating to medications, allergies, immunizations, surgeries or other procedures, implanted devices, care plans, care teams, and goals
- Any other categories of health information or other data, including categories that become accessible in the future

Username: 
Password: 

Afterwards, you’ll be automatically redirected back to HealthToGo (using UDAP Trusted DCR).

Contact ABC Hospital System directly regarding credentials, or with other questions about application access APIs.

About the app you are using to access this data:

HealthToGo SANDBOX

HealthToGo (using UDAP Trusted DCR) completed an automated dynamic client registration process to identify itself and provided the following website during the registration process:
http://www.emrdirect.com/

This app also presented the following trusted information:
- Developer Organization: EMR Direct
- Privacy Policy: http://www.interopengine.com/privacy.html
- Terms of Use: http://www.interopengine.com/open-api-terms.html

You assume all responsibility and liability for any apps you authorize. Apps vary in their data use policies and may not be subject to the same privacy and security laws that healthcare providers are, refer to the app developer’s privacy policy before proceeding.

powered by Interoperability Engine™
Terms of Use | Privacy Policy
©2019 EMR Direct
Ecosystem Components Adding Federated Identities

UDAP Client Authorization JWTs

UDAP Dynamic Client Registration

UDAP Server Validation

Trusted 3rd Party OAuth Servers:
Leverage Reusable Identities Issued by Others through Tiered OAuth

User Authorization
Pre registered or Discoverable Identity;
Client may access Health Data & Consent

Dynamic Client Registration (DCR)
& Trusted DCR; App Discovery & Validation,Reusable Client Vetting

Trusted FHIR Server:
Discovery, Validation, Provenance
CARIN – Kantara: Why?

NOREEN WHYSSEL, COO, DECISION FISH
IDEF REGISTRY, KANTARA INITIATIVE EDUCATIONAL FOUNDATION
NWHYSSEL@GMAIL.COM

COLIN WALLIS, EXECUTIVE DIRECTOR
COLIN@KANTARAINITIATIVE.ORG
TWITTER: @KANTARACOLIN @KANTARANEWS
CARIN – Kantara; complementary partners in Healthcare

- ‘Commons’ ethics & societal purpose. No/Low barriers to participation. Passionate about giving back control of identity & personal data. Consent Receipt and User Managed Access specs
- Mission: the global consortium improving trustworthy use of identity and personal data through innovation, standardization and good practice
- Business model: Revenue from Membership, Sponsorship, R&D and Trust Framework Operations program management invested in specification development & publishing platform, and contributions to ISO OECD Internet Technical Advisory Committee
- The only industry consortium to have both identity and personal data agency scoped within its mission - to nurture, develop, operate
- Global thought-leaders; Organizations & Individuals & Government

Our Leadership

Our Liaisons (examples)
CARIN’s interest in Kantara’s Award-Winning, Trend-Setting, Compliance-Assisting Innovations


- **Kantara Consent Receipt** - the world’s first digital receipt specification for personal data containing the conditions upon which the consent is given – giving agency over personal data to individuals. Annexed into Draft International Standard ISO/IEC 29184 Online privacy notices and consent.

- **Kantara Trust Framework** - the world’s first to offer 3rd party accredited assessment, approval & grant of trust mark to solution & service providers for NIST SP 800-63-3 per TEFCA. IDESG’s IDEF self-attesting scheme added Aug 2018.
Example Deployments of Kantara’s Specifications

The UMA specification gives individuals a unified control point for authorising who & what can access their digital assets at their desired grain.

The Consent Receipt Specification define the requirements for a record of authority by a PII Principal to a PII Controller for processing of the Principal’s PII.

Customer Commons/Kantara Intent Casting UX and Human Readable terms

Gluu

more..
The ID Ecosystem Framework’s Registry (IDEF-R)

- IDESG was funded by NIST (2011-2018) to fulfil the NSTIC’s vision
- The ID Ecosystem Framework defines requirements for Privacy, Security, Interoperability and Usability of an ID service
- The IDEF itself and the IDEF-R are now part of the recently established Kantara Education Foundation (a 501 c3)
- The Framework includes a scoping statement, baseline requirements and a functional model to be used by stakeholders
- Registered entities self-attest and are scored on level of framework implementation; threshold score earns a Trustmark
- CARIN interested in leveraging the self-attesting IDEF-R for its own Code of Conduct and other conformance items

http://idefregistry.org  nwhysel@gmail.com
The IDEF and Patient Choice in Health Care Identity

Health Profile for Digital Ecosystem
Focus on medical records locator and access to data by the patient

Allow developers and UX teams to determine if their systems are compliant with the framework.

Distributed Attribute Use Case
At registration with a new provider, patient creates initial EHR

Patient may use their own ID or one from a Trusted 3rd Party

Provide good assurance that a patient's data records are as accurate as possible and relate to the real live person requesting services.

Prototype Sandbox
Example use case – Emergency contacts + Current Rx and Adverse-meds

Provide good assurance that patient’s contact data is kept as private as possible consistent with emergency access