UDAP WORKFLOWS: A DEVELOPER TOOLKIT

Expanding FHIR ecosystem security and scalability

Luis Maas, MD, PhD
1/14/2021
INTRODUCTION TO UDAP
Purpose

• Utilize existing FHIR infrastructure & security workflows as a starting point

• Enhance security & confidence in exchange
  – Validate the organization behind the client application, FHIR datasource, or identity server
  – Validate claims from transaction participants

• Reduce cost of scaling as number of clients & servers increases
Workflow Overview

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

Query

- Each participant can be reliably identified

Response

- Data Holder can dynamically discover participant attributes & use in/help to inform policy decisions (registration request, token request)
Use Cases

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

Trademark Notice: UDAP and the ecosystem gears design are trademarks of UDAP.org and are used with the permission of UDAP.org.
Glide path
GENERAL BACKGROUND FOR UDAP IMPLEMENTERS
Working with Cryptographic Software

Resources:

• The Specs: RFC 5280, RFC 7515-7519

• Common JWT signing and validation libraries
  – RS256 cryptographic algorithm
  – Several public lists of available libraries:
    JWT.io: https://jwt.io/
    OpenID: https://openid.net/developers/jwt/
Additional Deployment Considerations

• Obtain digital certificate from a CA/RA
• Add keystore management to your security policy & risk analysis
• Trust store management & policy
  – the “Internet PKI” is not enough
Trusted Registration

• Essential to scaling the registration process
• Registration parameters
• Assembling as a signed JWT
  – Header, Payload, Signature
• Certifications & Endorsements
  – Self Assertions vs. Third Party Certifications

• UDAP Links: Dynamic Client Registration, Certifications & Endorsements
Authorization and Authentication

• Sign JWT with trusted certificate in token request
• Hint patient’s own identity service to invoke Tiered OAuth in authorization request
• Authorization assertions

• UDAP Links: [JWT-Based Authentication](https://www.hl7.org/fhir/), [Tiered OAuth](https://www.hl7.org/fhir/), [Client Authorization Grants](https://www.hl7.org/fhir/)

© 2019 Health Level Seven® International. Licensed under Creative Commons Attribution 4.0 International HL7, Health Level Seven, FHIR and the FHIR flame logo are registered trademarks of Health Level Seven International. Reg. U.S. TM Office.
Enabling Identity Provider Discovery

• Server validation before redirecting to AS
  – Use conventional X.509 chain building techniques and path validation
  – Implement & manage trust policy logic

• For either a tightly coupled AS or 3rd party IdP

• UDAP Links: Server Metadata
Certificate-Backed Registration

• Dynamically trust new clients that meet a common bar
  – Validate digital signatures on submitted JWTs
  – Use conventional X.509 chain building techniques and path validation to validate trust chains
  – Implement & manage trust policy logic
  – Issue client_id only if a valid, trusted request is submitted
  – Maintain client registration details in audit trail
Certificate-Backed Authentication

• Add trust validation step to Authn policy logic
  – Receive a signed JWT with every token request
  – Certificate details match previously-registered client
  – Trust policy enablement, as at registration

• Process additional assertions made by client
  – Purpose of use, consent, user identity

• Delegate to a trusted IdP for User Authentication via Tiered OAuth
Identity Providers

• Generally the same requirements as data holders
• The data holders act as clients to the IdP servers
• IdPs interact directly with the End User but not with the User’s Client App.
More at:
• UDAP.org
• UDAP-discuss Google Group
• udap-tools GitHub