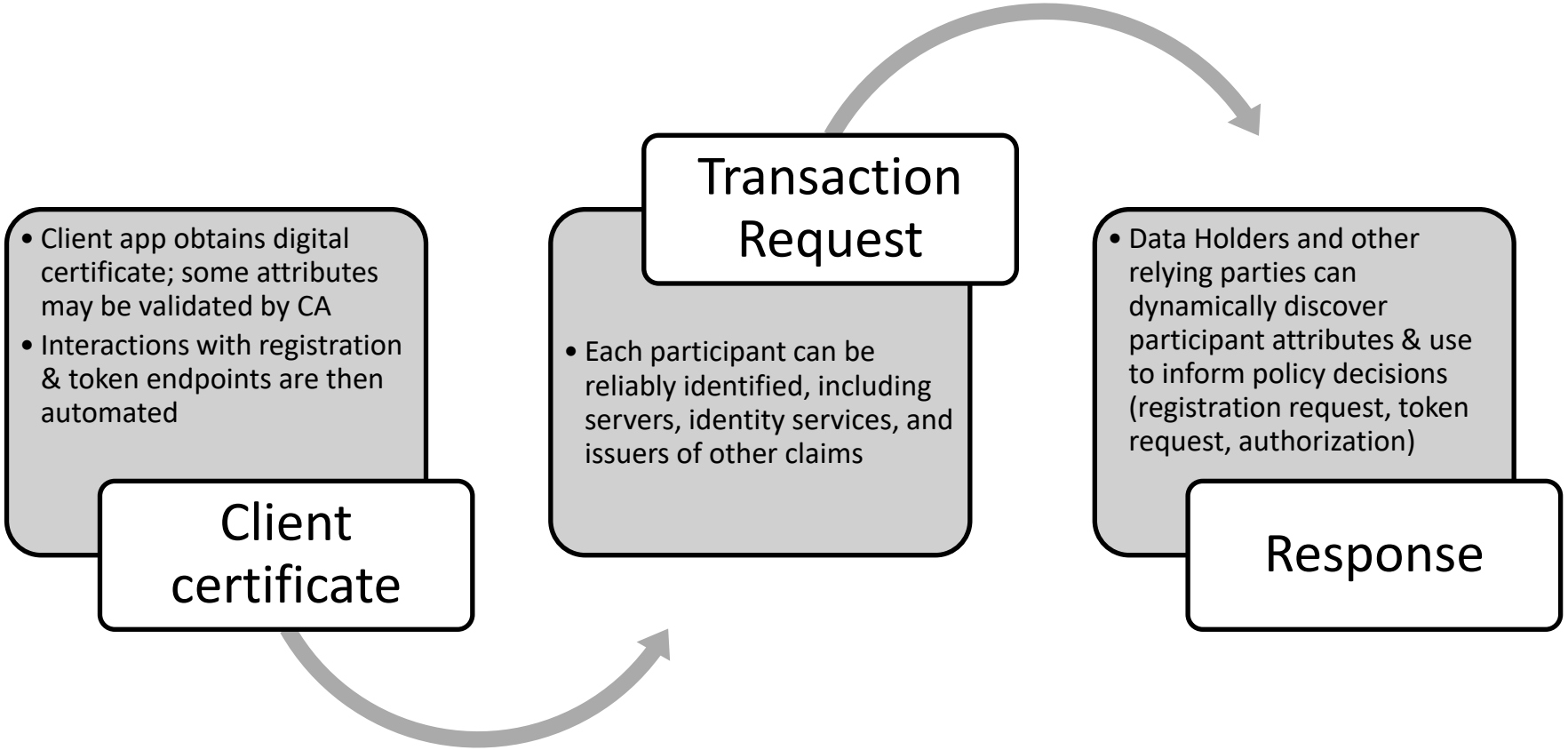
UDAP Technical Overview

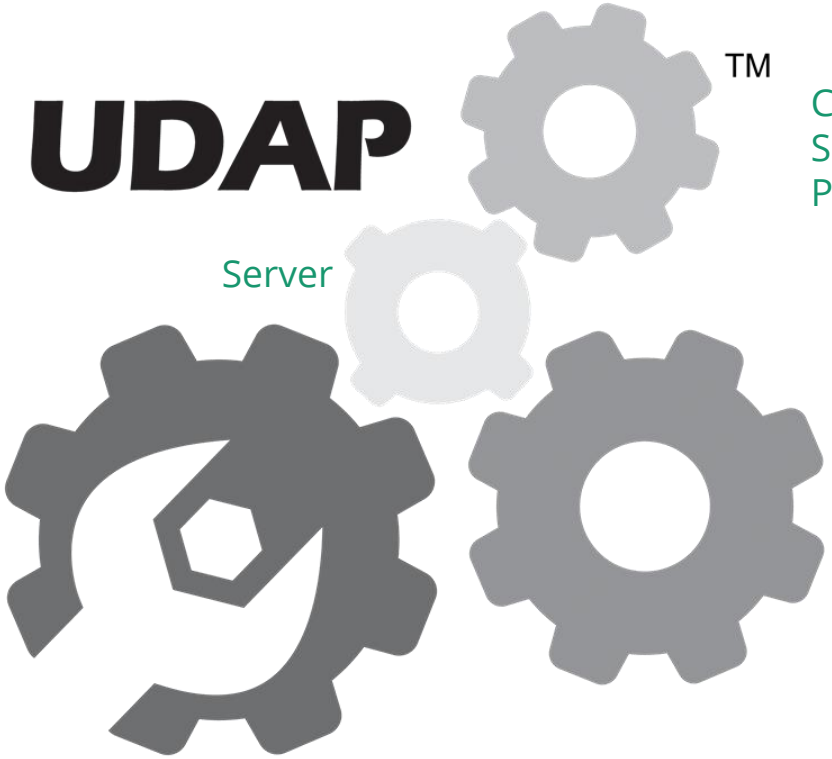
Adding scalability and security to API transactions with trusted certificates

September, 2022

UDAP High Level Overview

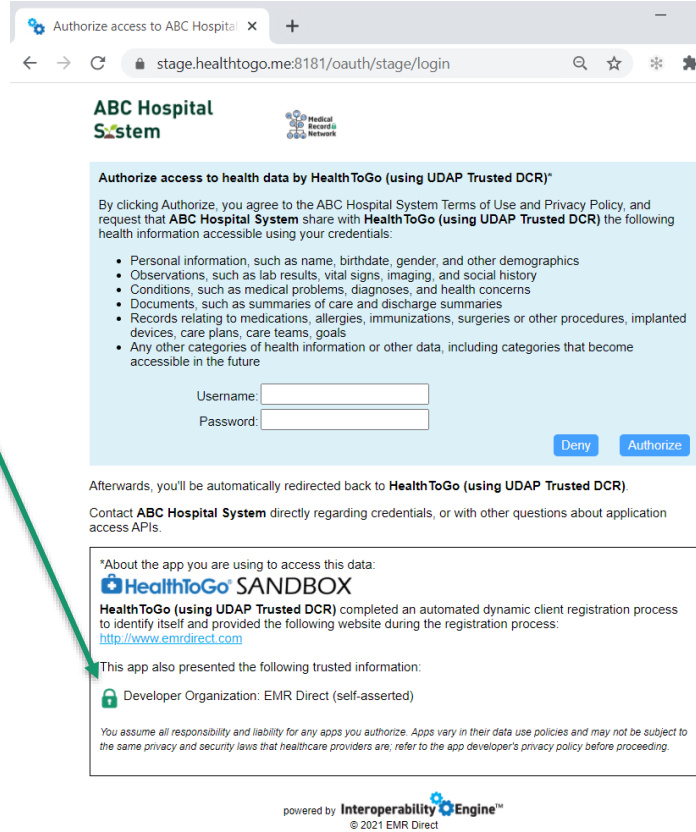


UDAP Trusted API Ecosystem

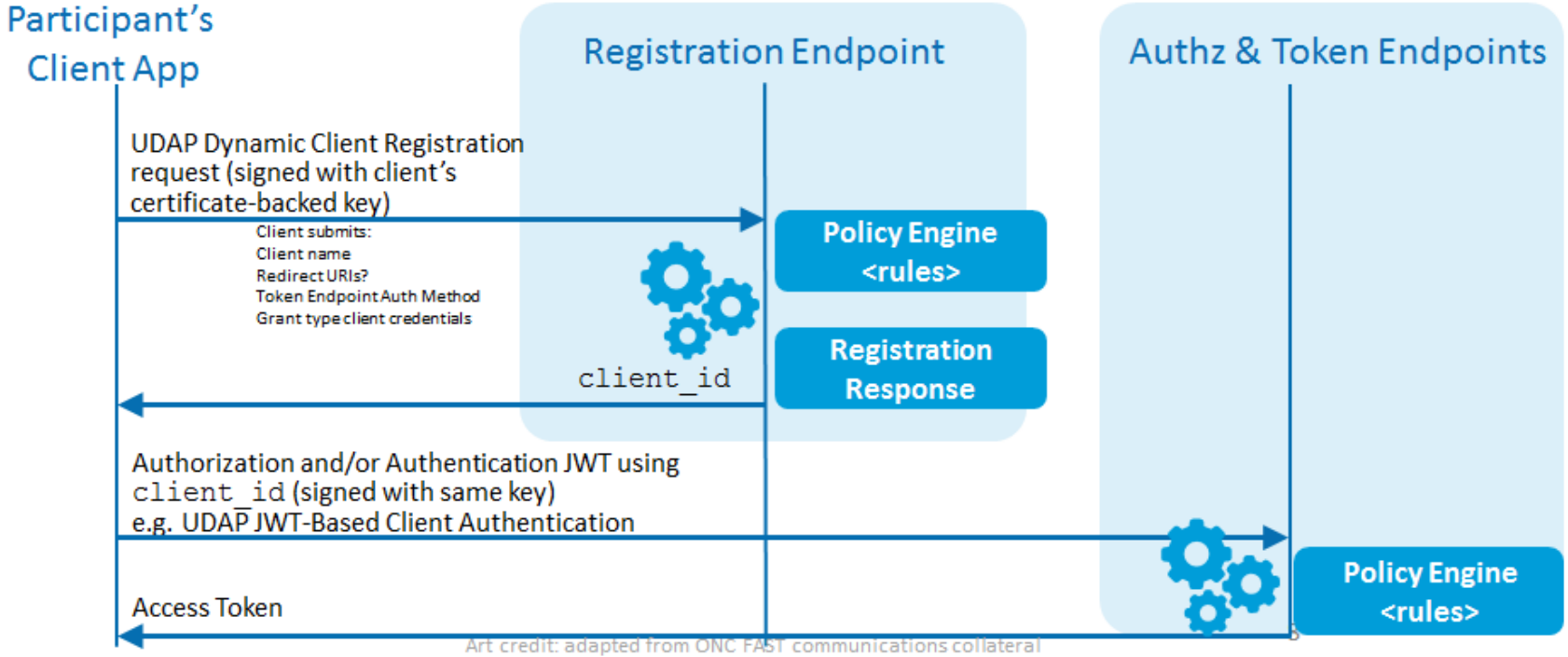


OAuth Sign In Page with UDAP Trusted Dynamic Client Registration

- 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.

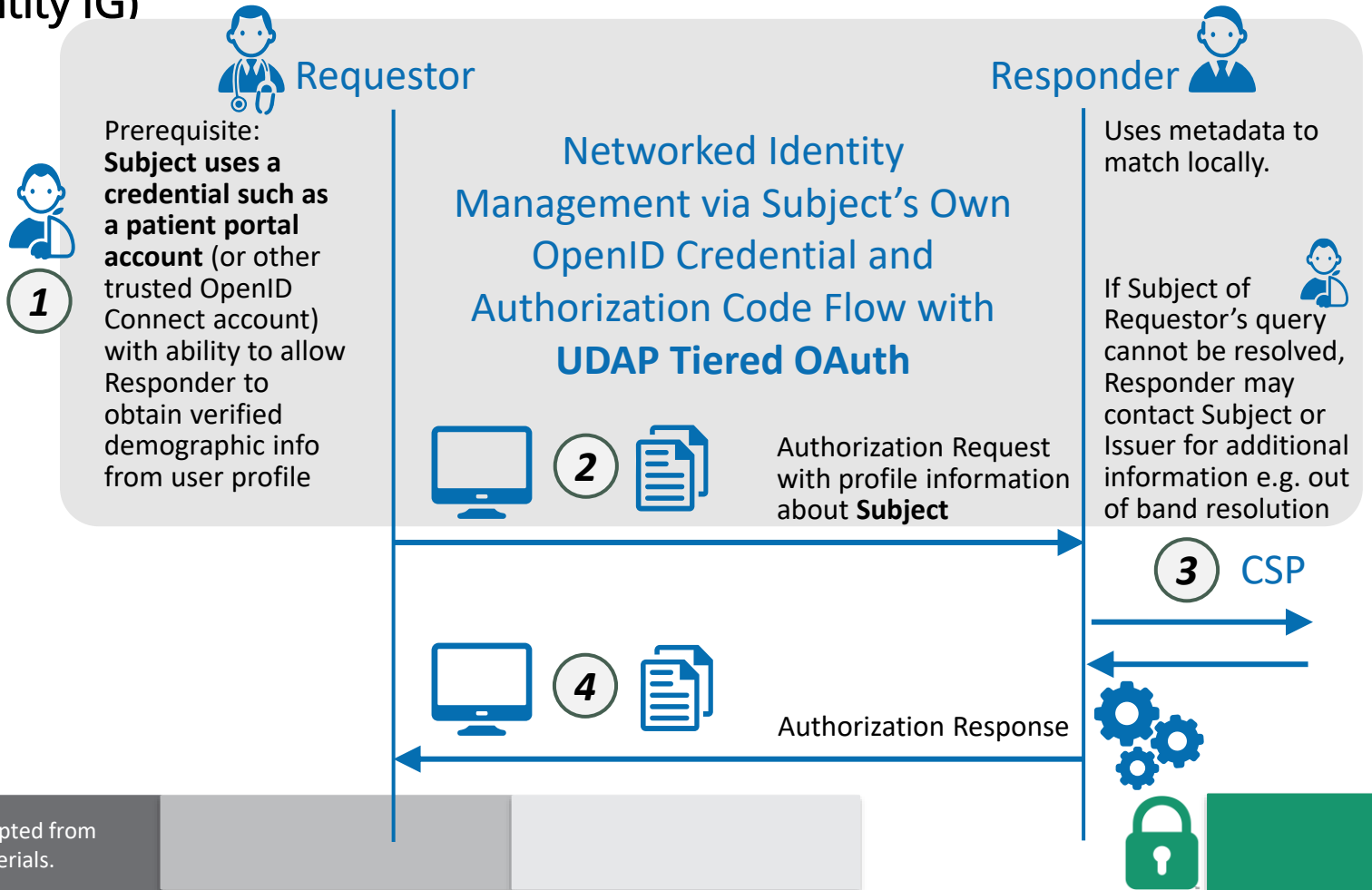


UDAP Dynamic Client Registration & Token Request



Art credit: Adopted from ONC FAST materials.

Frictionless Cross-Organization Matching with Digital Identity-Overview (Identity IG)

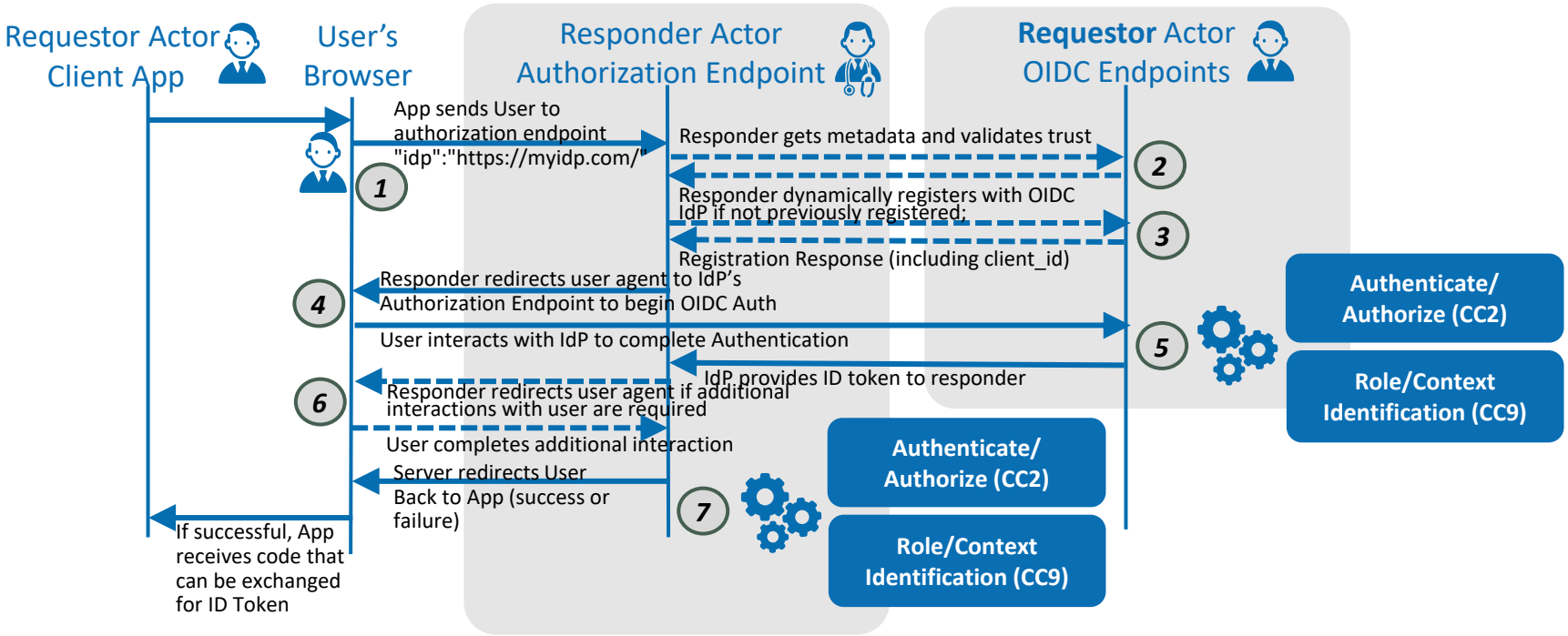


Art credit: Adopted from ONC FAST materials.

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.

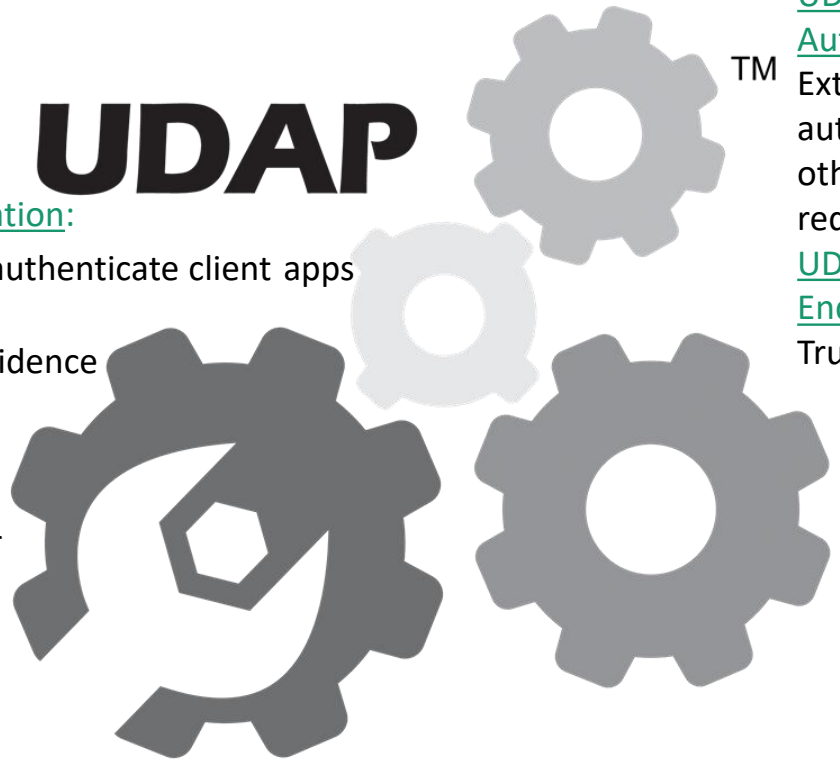
Implementing the UDAP Trusted Ecosystem

UDAP™

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 written into several industry IGs + FAST Security Solution
Basic Authorization Code Flow
Trusted Dynamic Registration
JWT-Based Authentication
Exchange via Trust Framework
Assertions, Certifications & Endorsements; Server Metadata Included
Tiered OAuth & Server validation for endpoint confidence & data provenance

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

Thank you!

www.udap.org

collaborate@udap.org

@udapTools

HL7 Interoperable Digital Identity and Patient Matching Implementation Guide – user profile


```
{
  ...
  "iss":"https://generalhospital.example.com/as",
  "sub":"328473298643",
  "identifier":"123e4567-e89b-12d3-a456-426614174000a",
  "amr":"http://udap.org/code/auth/aal2",
  "acr":"http://udap.org/code/id/ial2",
  "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-1
}
```