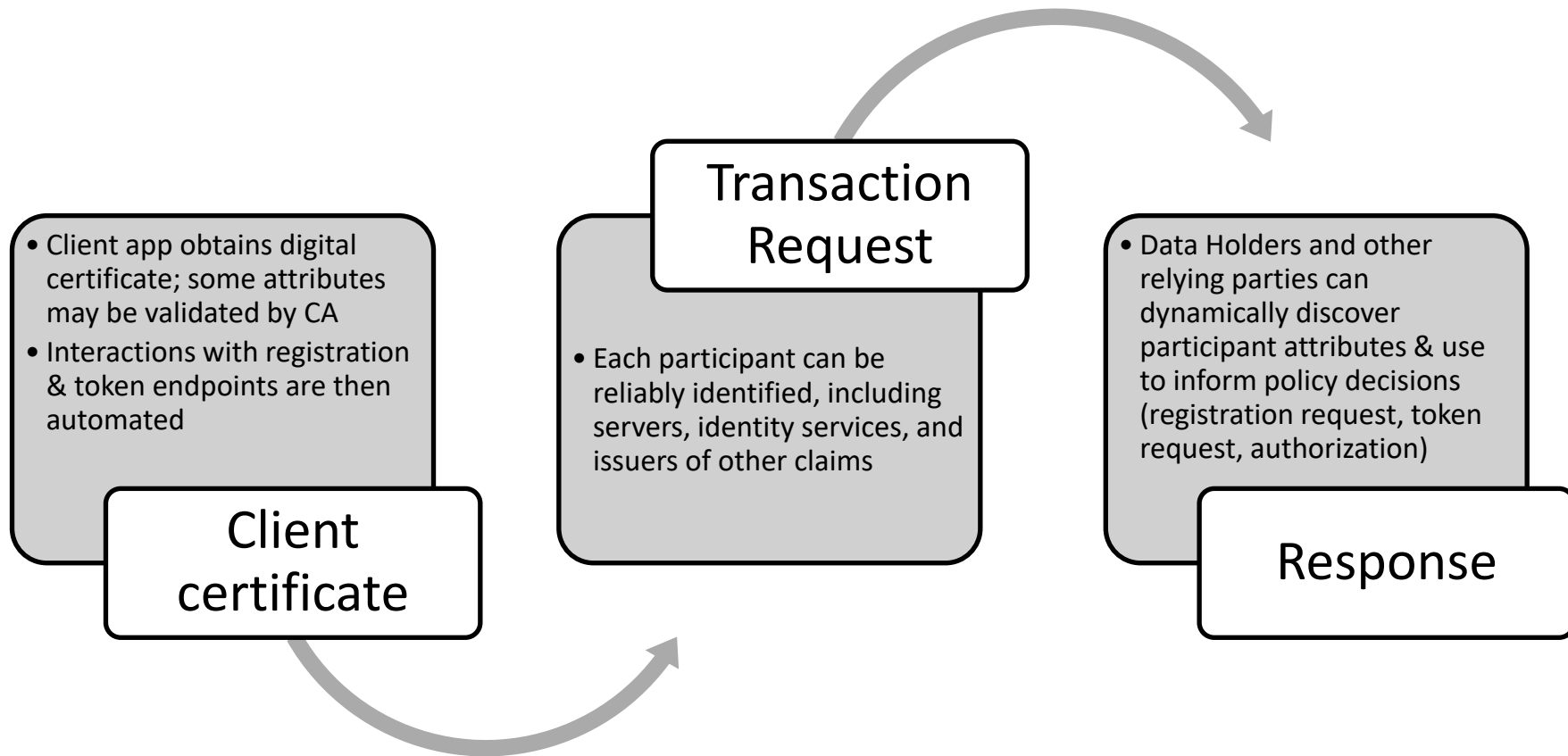


UDAP Technical Overview

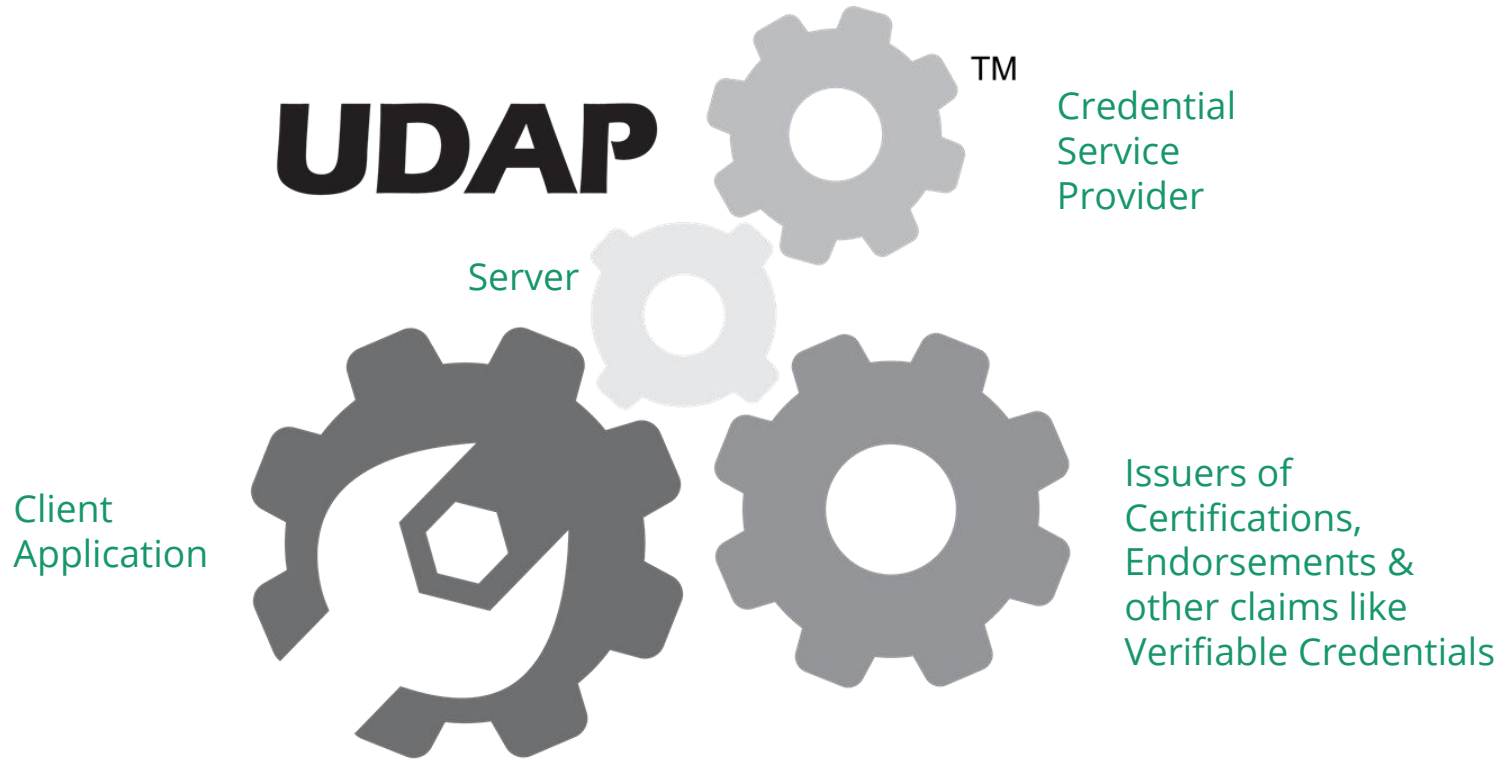
Adding scalability and security to API transactions with trusted certificates

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.

Authorize access to ABC Hospital System

stage.healthtogo.me:8181/oauth/stage/login

ABC Hospital System

Medical Records Network

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, goals
- Any other categories of health information or other data, including categories that become accessible in the future

Username:

Password:

Deny Authorize

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 (self-asserted)

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™
© 2021 EMR Direct



UDAP Dynamic Client Registration & Token Request

Participant's Client App

Registration Endpoint

Authz & Token Endpoints

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

Policy Engine
<rules>

Registration Response

client_id

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

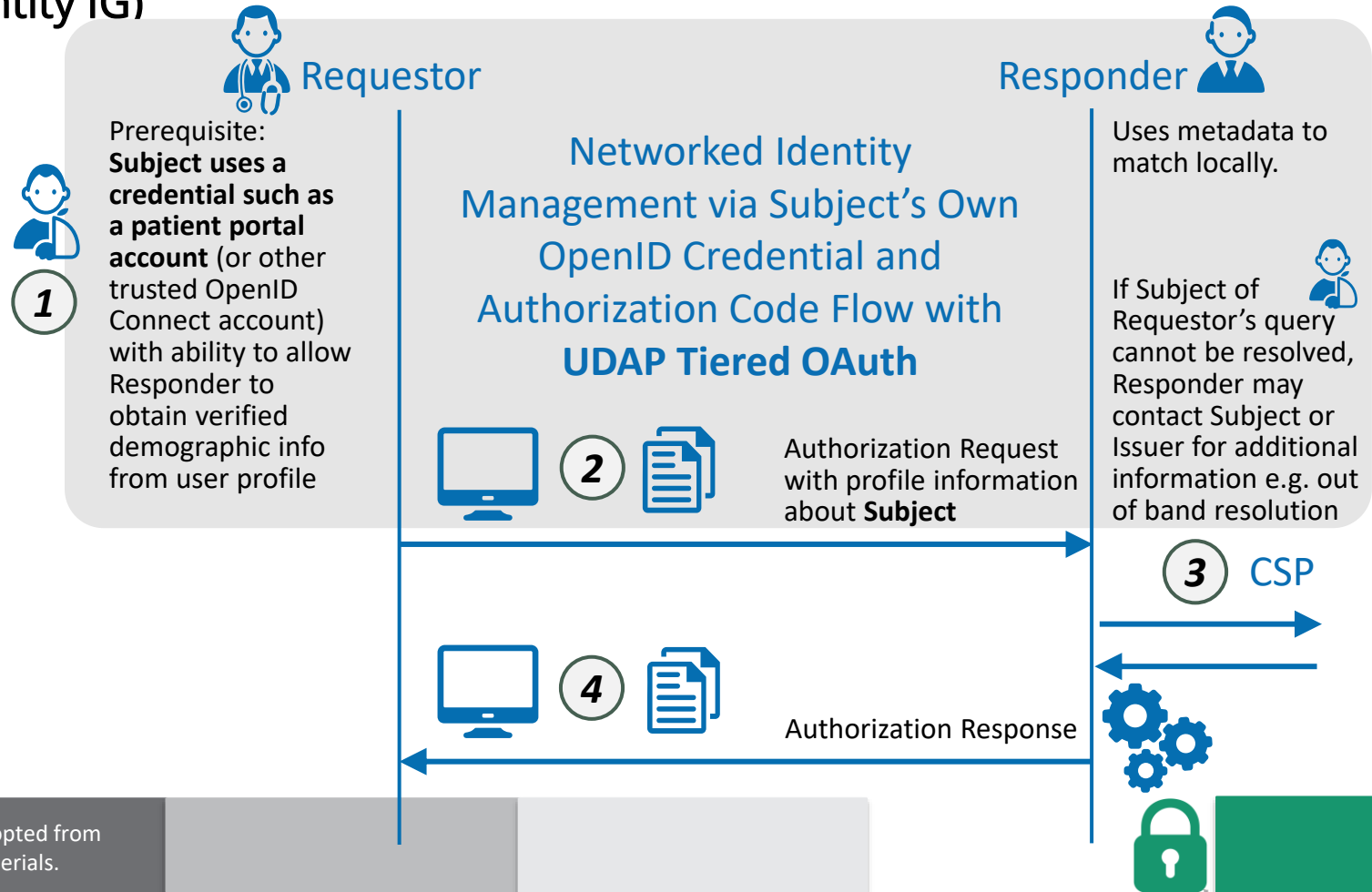
Policy Engine
<rules>

Access Token

Art credit: adapted from ONC FAST communications collateral



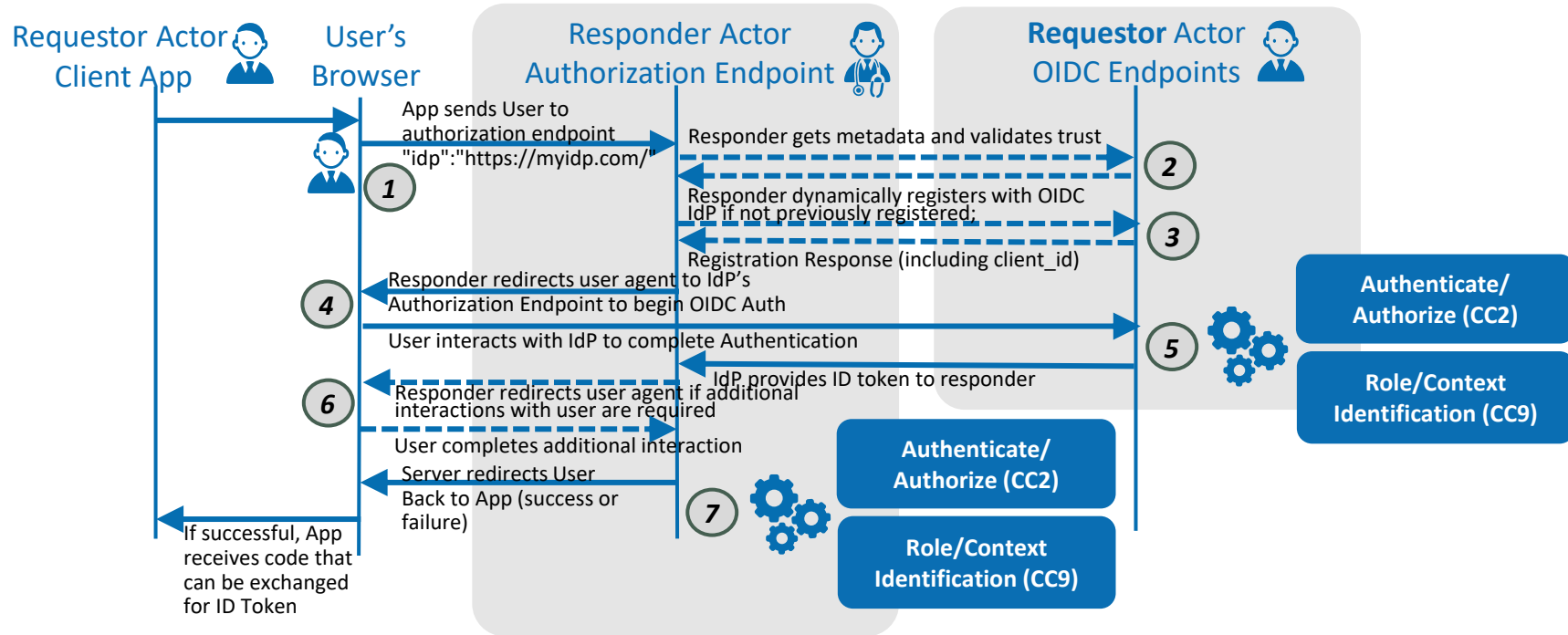
Frictionless Cross-Organization Matching with Digital Identity-Overview (Identity IG)



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)



Implementing the UDAP Trusted Ecosystem

UDAP

TM

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

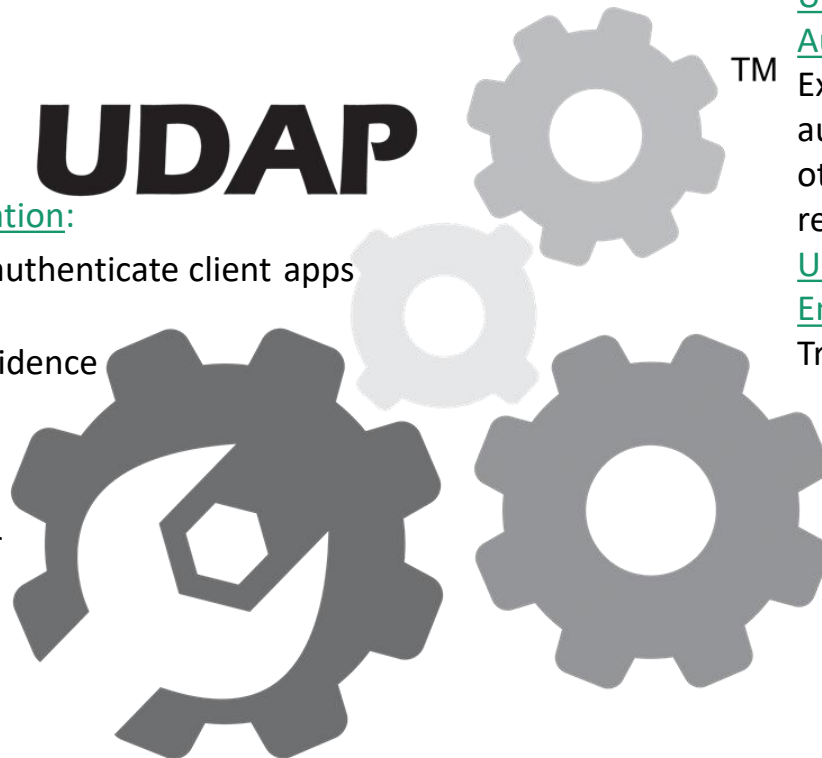
UDAP Certifications &

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



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-a456-42661417400a",  
  "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" }  
}
```

