

# TDRAAP GLIDE PATH Levels of Trusted Dynamic Registration and Authentication



Referral Code 1000

Star Levels- Indicating Level of Security Capability	Description	Benefit of Certified or Accredited Workflow	Industry Effort Level
★	OAuth 2.0 – Authorization code flow with Client ID (and Secret)	Access to data one patient at a time with patient's own credentials	Most difficult to scale (each App must gain Client ID and secret for each different Server)
★★	UDAP Dynamic Client Registration	No client pre-registration needed <sup>1</sup>	Less difficult to scale, some cost savings for clients & servers
★★★	UDAP JWT-Based Authentication	No client credential provisioning needed <sup>2</sup>	Even less difficult to scale
★★★★	UDAP Certifications and Endorsements, Server Metadata & authorization assertions within JWT-Based Authentication <sup>3</sup>	Servers include Server Metadata and indicate validation of Client in UI (if any)	Simpler to scale
★★★★★	Server Claims <sup>4</sup> and UDAP Tiered OAuth	Clients indicate validation in UI (if any); no user pre-registration needed	Simplest to scale, most cost savings for clients, servers & patients

<sup>1</sup> When used with FHIR registration servers capable of UDAP Trusted DCR on the server side.

<sup>2</sup> When used with FHIR authorization servers capable of UDAP JWT-Based Authentication on the server side.

<sup>3</sup> Claims and assertions made by Client applications are validated and/or consumed by Servers. This includes additional Client application characteristics asserted by Endorsers, such as EHNAC and CARIN, e.g., whether a client application is TDRAAP certified or “affirmatively shares” their privacy policy with every user; authorization assertions can be used in B2B patient matching by a privileged client for patient access even without patient credentials.

<sup>4</sup> Claims made by Servers, such as Servers’ use of signed metadata and/or Certifications & Endorsements, are validated by Clients.