TDRAAP GLIDE PATH Levels of Trusted Dynamic Registration and Authentication

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[1]	Less difficult to scale, some cost savings for clients & servers
☆☆☆	UDAP JWT-Based Authentication	No client credential provisioning needed[2]	Even less difficult to scale
☆☆☆☆	UDAP Certifications and Endorsements, Server Metadata & authorization assertions within JWT-Based Authentication[3]	Servers include Server Metadata and indicate validation of Client in UI (if any)	Simpler to scale
☆☆☆☆☆	Server Claims[4] 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

[1] When used with FHIR registration servers capable of UDAP Trusted DCR on the server side.
[2] When used with FHIR authorization servers capable of UDAP JWT-Based Authentication on the server side.
[3] 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.
[4] Claims made by Servers, such as Servers' use of signed metadata and/or Certifications & Endorsements, are validated by Clients.