






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	Network-wide, PKI-based app identity management Frictionless client registration ¹	Less difficult to scale, some cost savings for clients & servers
	UDAP JWT-Based Client Authentication	Streamlined client credential management and network-wide revocation ²	Even less difficult to scale
	UDAP Certifications and Endorsements, Server Metadata & authorization assertions within JWT-Based Client Authentication ³	Confidence in client assertions & other PKI-based claims (purpose, consent, identity) Mitigate man-in-the-middle	Simpler to scale
	Server Claims ⁴ and UDAP Tiered OAuth	Increased confidence in server identity & other claims Fewer, stronger credentials & reduced risk of impersonation	Simplest to scale, most cost savings for clients, servers & patients

¹ When used with FHIR registration servers capable of UDAP Trusted Dynamic Client Registration on the server side.

² When used with FHIR authorization servers capable of UDAP JWT-Based Client 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.