Privacy & Security Standards for Digital Identity

Luis Maas, MD, PhD

CTO, EMR Direct

UDAP Unified Data Access Profiles

EMR Direct
SIMPLIFYING INTEROPERABILITY

Definitions

- Privacy
  - The right to control how your personal information is used or disclosed

- Security
  - The mechanisms used to protect the privacy of your personal information

OAuth 2.0

- An “authorization” protocol
- Most common form: authorization code flow
- Lets you authorize an app to “do something” with data you have rights to access
- Your credentials are not shared with the app
- The app doesn’t need to know who you are

OpenID Connect (OIDC)

- An “authentication” protocol
- Builds on OAuth 2.0
- Lets a relying party (RP) ask for you to be authenticated by an Identity Provider (IdP)
- The IdP provides the RP with an identifier uniquely assigned to you and (possibly) identity attributes like name, DOB, etc.

OpenID Connect (OIDC) – continued

- Lets you prove to the RP that you are the person associated with the identifier
- Lets you decide which identity attributes you want to share with the RP
- Back-channel protects privacy: RP gets data directly from the IdP

Unified Data Access Profiles (UDAP)

- A “trust network” protocol
- Builds on OAuth 2.0 and OpenID Connect
- A number of profiles to scale Open API ecosystems via trust communities
- Not just about user identity, but also the identities of apps, data holders, and IdPs

UDAP Tiered OAuth

- Enables dynamic networks of trusted IdPs
- Data holders can request authentication from your preferred IdP
- Back-channel communication of attributes with your consent with OIDC
- Trust networks can set the bar for identity proofing, authenticators, etc.

Self-Sovereign Identity (SSI)

- Rapidly evolving area of digital identity
- Focus on User-Centric Identity
- Decentralized Identifiers (DIDs) provide mechanisms for authentication and sharing of attributes via Verifiable Credentials
- Since DIDs are URIs, they can also be used as identifiers in UDAP workflows

For more information:

- OAuth 2.0: tools.ietf.org/html/rfc6749
- OIDC: openid.net/specs/openid-connect-core-1_0.html
- UDAP: www.udap.org/
- DIDs: www.w3.org/TR/did-core/

Thank you

- luis@emrdirect.com
- collaborate@udap.org
- @udapTools