MIT FinTech Cybersecurity Summit, January 11, 2018

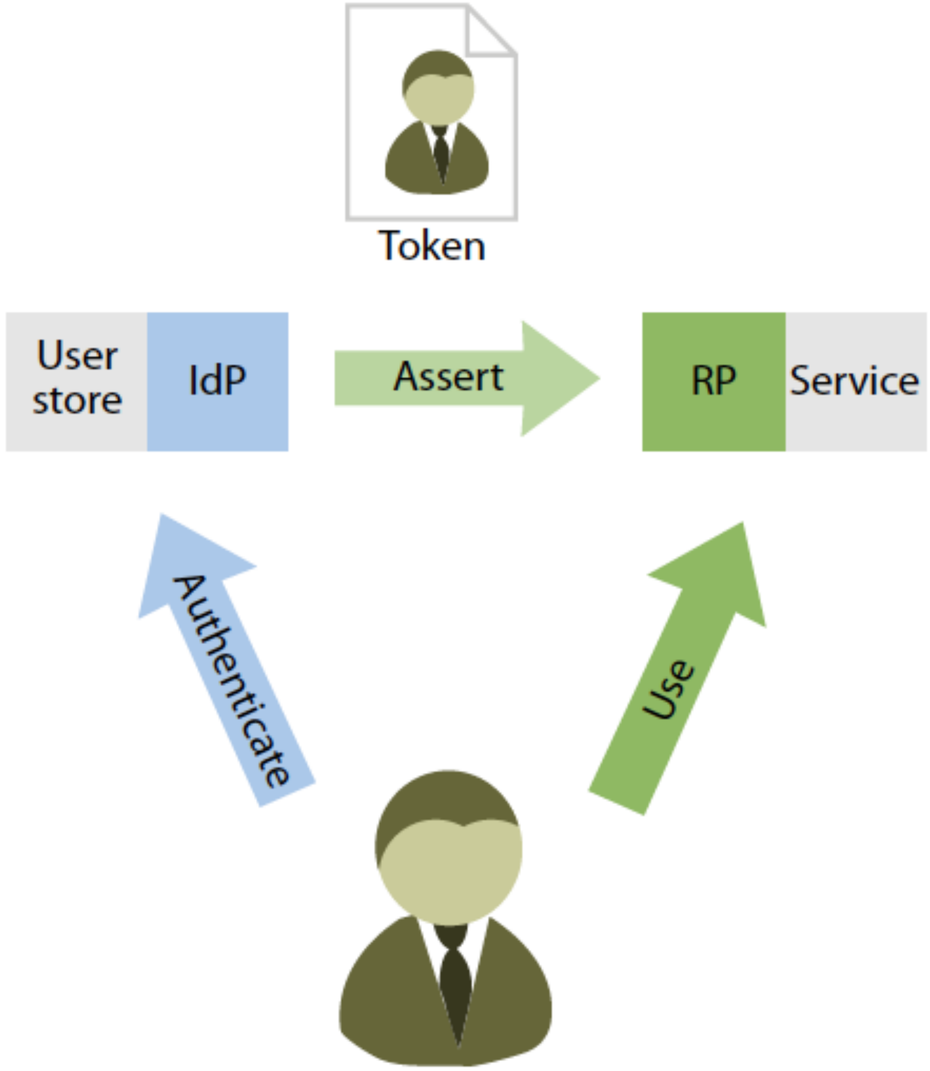
# OPAL: Connecting Identity & Data

**Thomas Hardjono**

MIT Connection Science
MIT Trust::Data Consortium

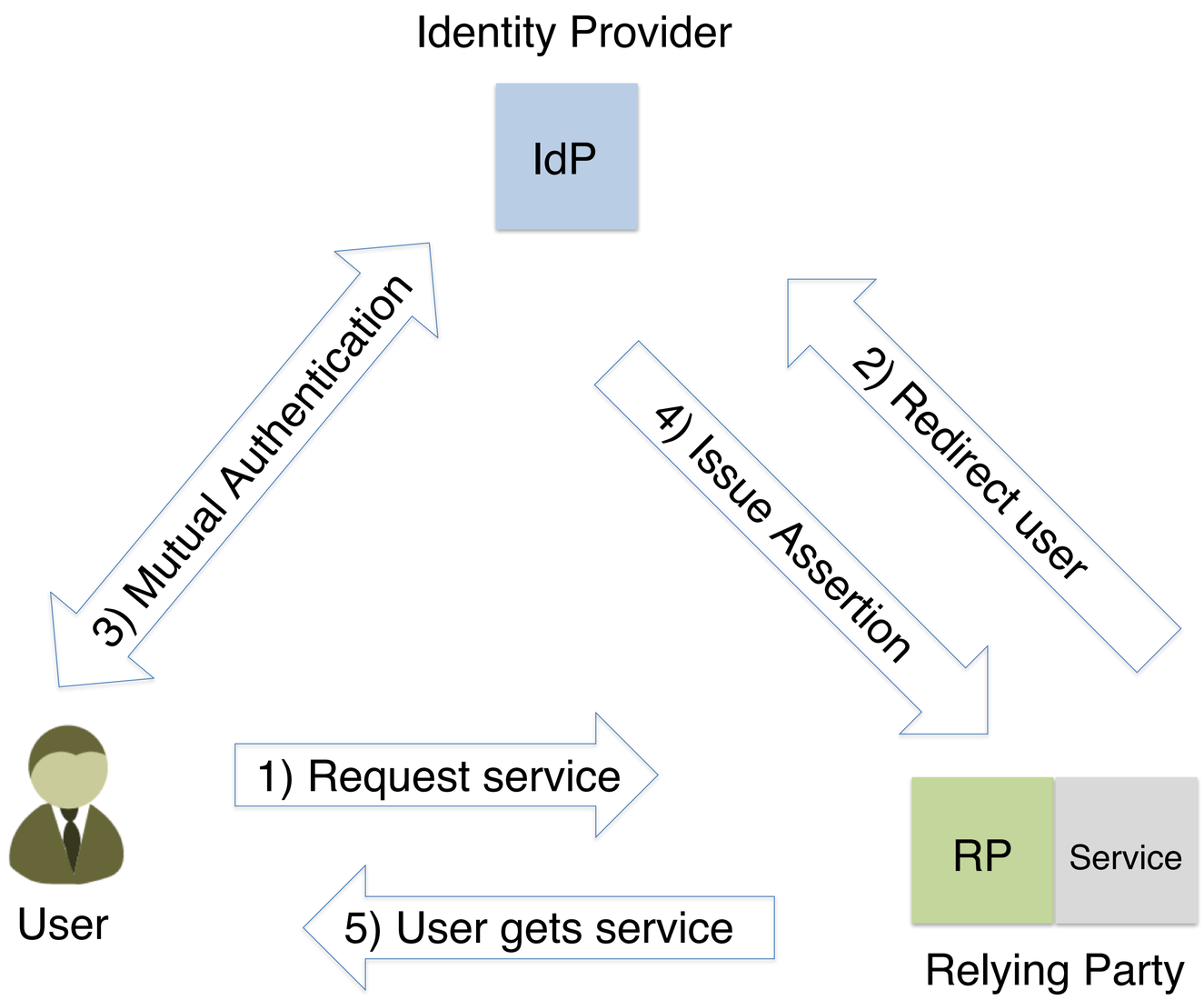
# Identity Providers: What, Who & Why

- Problem of multiple accounts & passwords (late 1990s)
- Problem of repeated re-entering of passwords
- Solution: Authenticate once to "Identity Provider" (IdP)
- IdP issues Assertion or Token
- User wields Assertion or Token to desired Service Provider



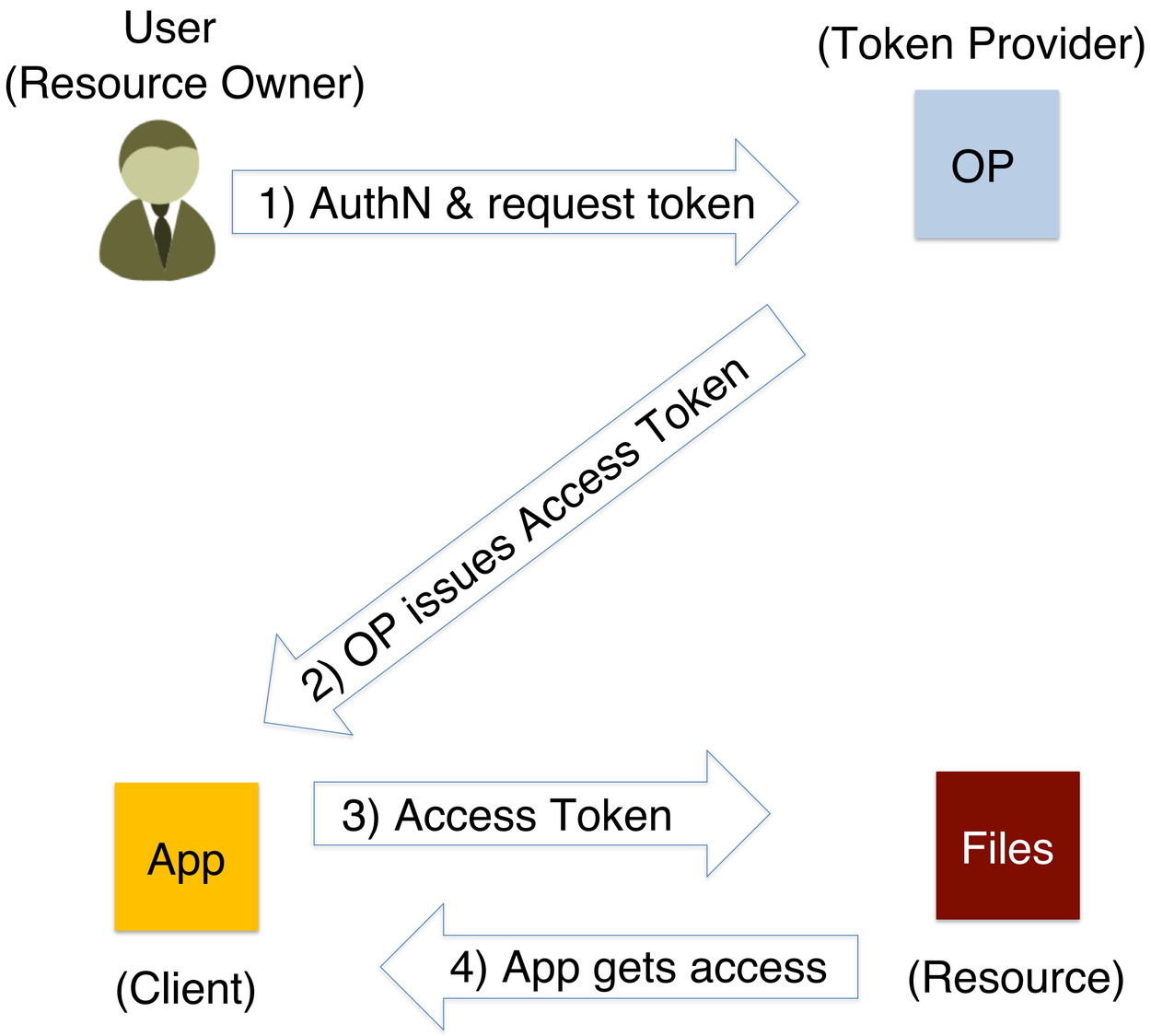

Source: Venn of Federated Identity, Forrester, 2011

# Security Assertions Mark-Up Language (2003)




- Avoid multiple logins
- User authenticates once only to IdP
- Browser use-case (“front channel”)
- Session duration (user is present)
- Services “relies” on IdP for true assertions

# Mobile Apps: OAuth & OpenID-Connect 1.0 (2011)




- Delegated model
- User authenticates to OpenID Provider (OP)
- Token issued to Client (3rd party app)
- App holds token for long time
- Refresh tokens

# But Identity Providers don't have rich user data

MIT Connection Science

- Same attributes collected (repeatedly)
- Fixed information

**"It's a data problem"**

| | |
|---|---|
| Name | |
| Street Address | |
| City | |
| State | Enter Text |
| Zip/Postal | |
| Province | |
| Country | Enter Text |
| Phone | |
| Email | |
| Preferred Communication | Postal Mail<br>Phone<br>E-mail |

**Authorize Card Ops to use your account?**

Sign In | Cancel

**This application will be able to:**

- Read Tweets from your timeline.
- See who you follow, and follow new people.
- Update your profile.
- Post Tweets for you.

**Will not be able to:**

- Access your direct messages.
- See your Twitter password.

Email

Create a password

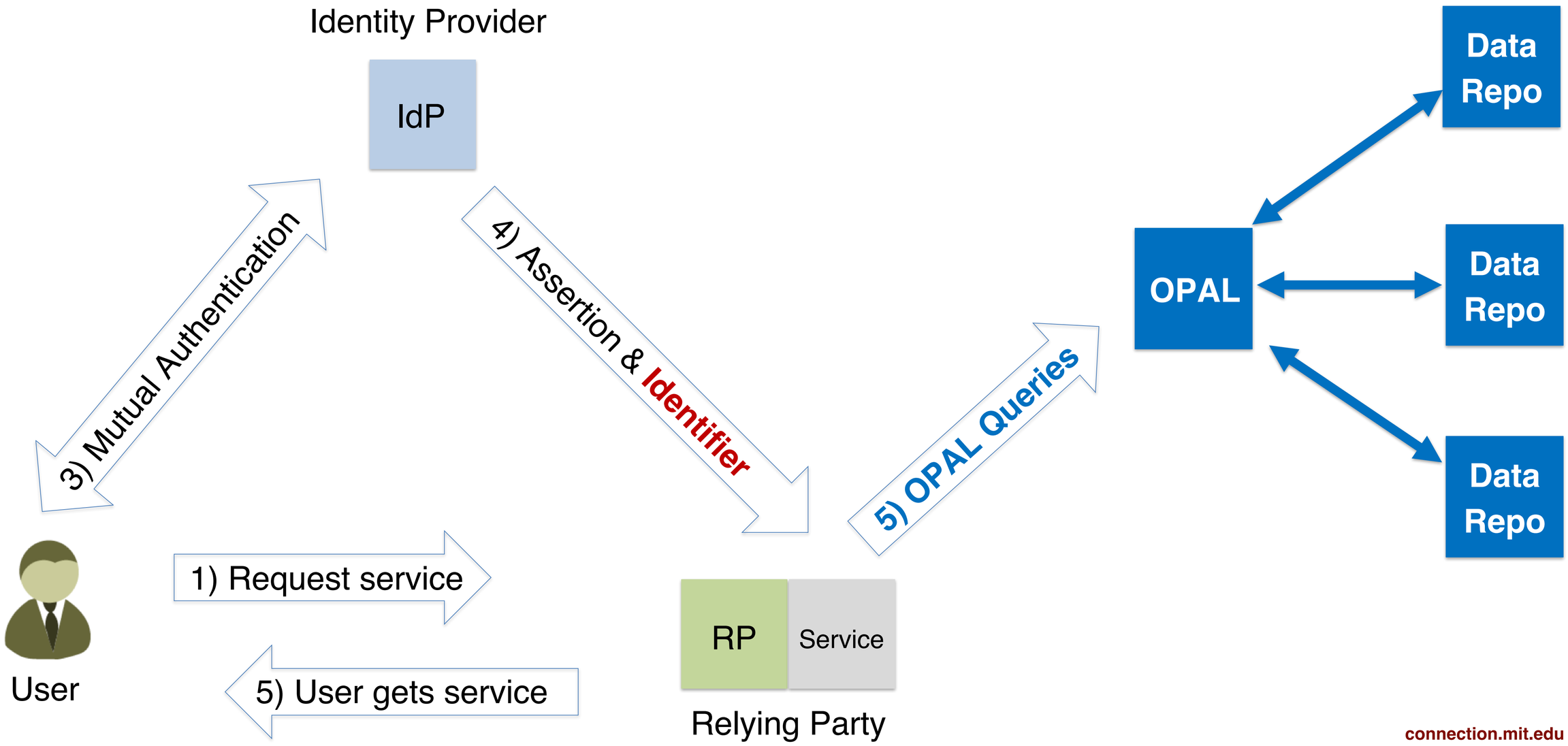
Continue

OR

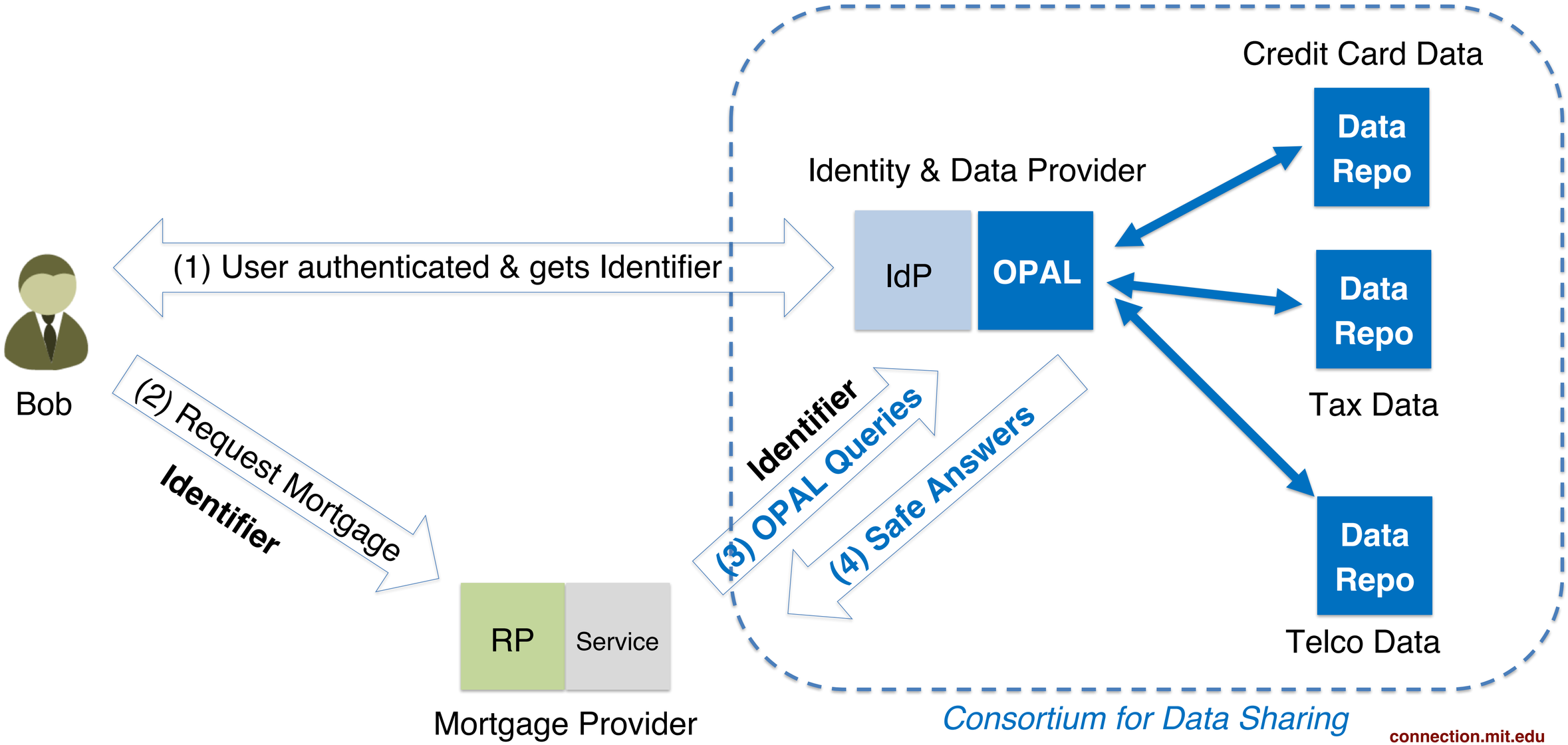
Continue with Facebook

Continue with Google

# Extend the Model: Sharing Insights using OPAL



# Example: User obtaining Mortgage

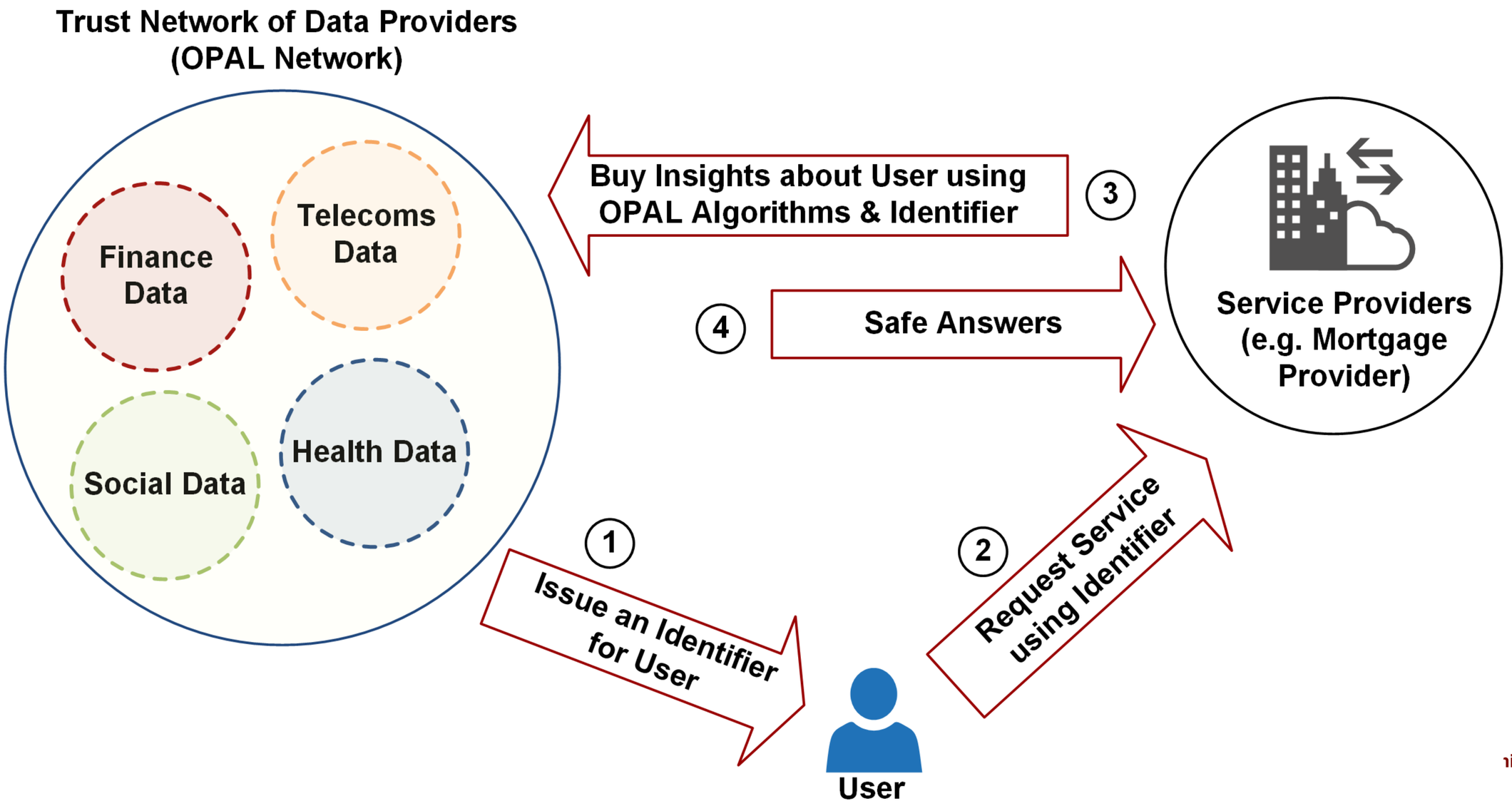


# What's gained

- **Service Providers obtain better insights about users & customers**
- **Improved risk management**
- **Raw data stays where it is**
- **User's privacy maintained (safe answers)**
- **Regulatory compliance**

- Broader insights across industry verticals
- Information derived using algorithms belongs to data owners
- Incentives to create better algorithms
- Market for algorithms
- AI and Machine Learning

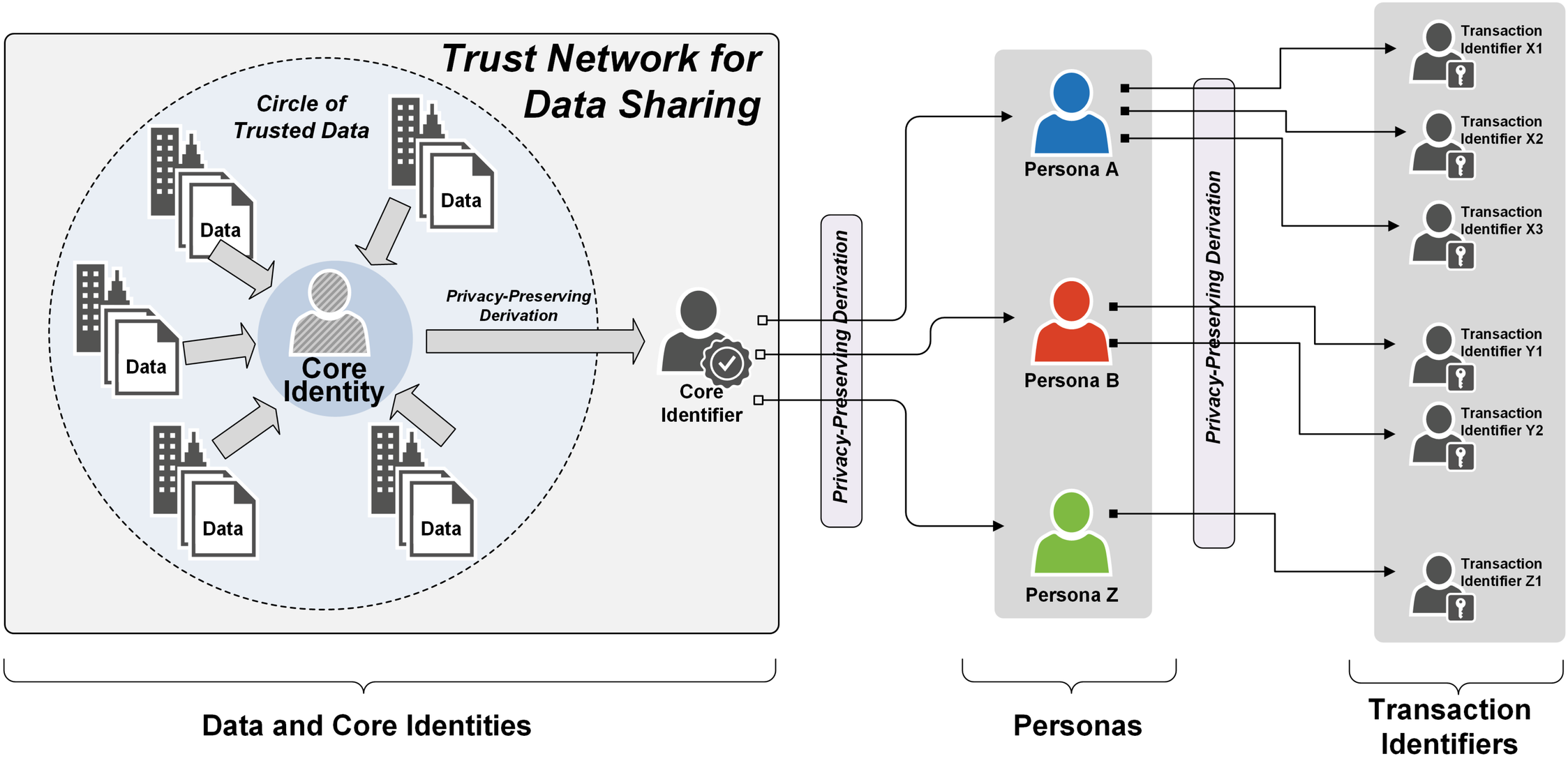
# Share Algorithms & Insights, not raw data



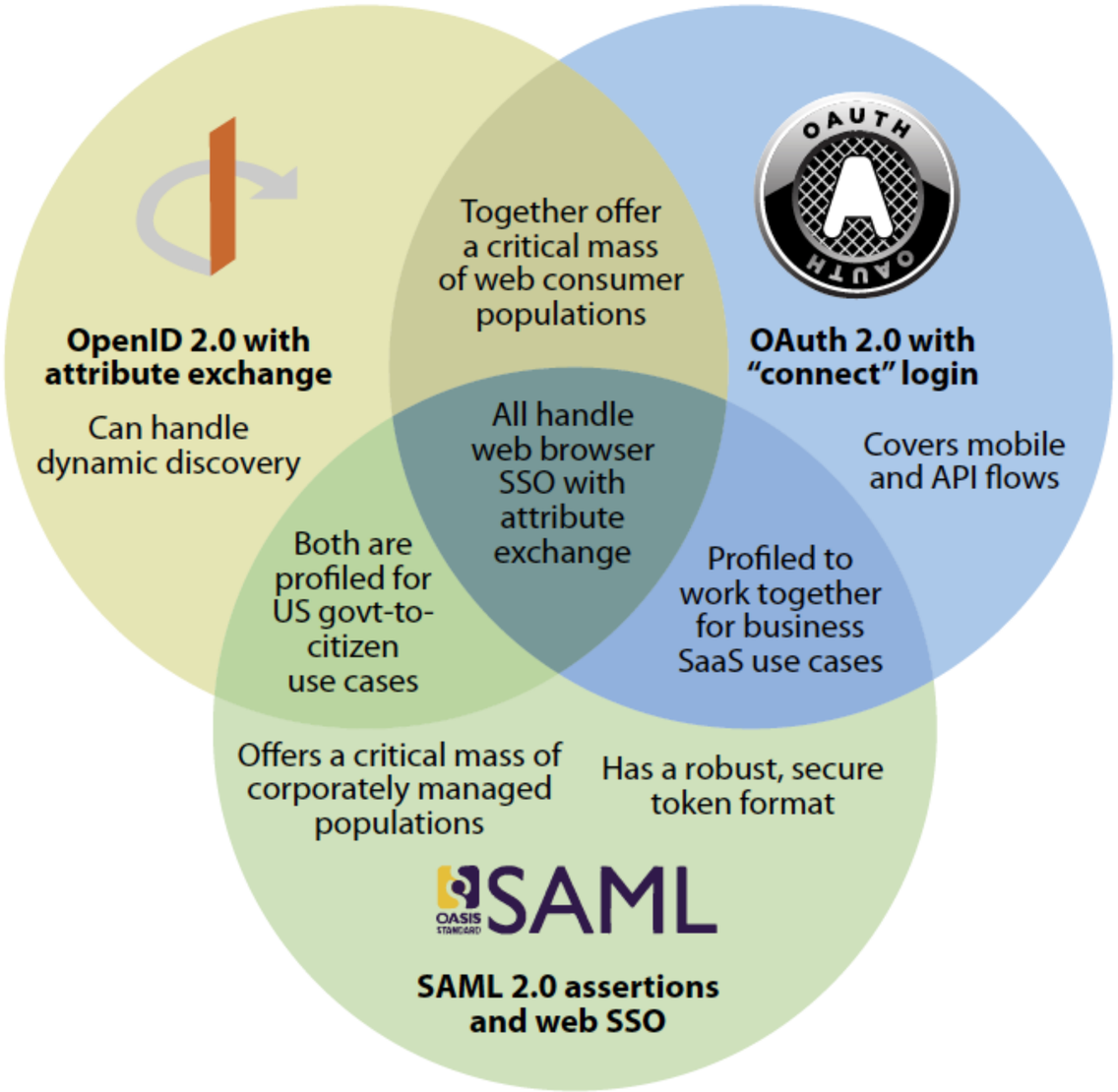
# Questions

# Core Identities, Personas & Transaction Identifiers

MIT Connection Science



# Identity Standards




Source: Eve Maler, UMA WG, Kantara Initiative, 2011

- **SAML2.0**: universal language for B2B identity federation
- **OAuth2.0**: "token-based" authorization for Web Applications, Mobile Apps and RESTful APIs
- **OpenID-Connect**: Attribute Exchange using OAuth2.0 model
- **UMA1.0**: User-centric consent management (over OAuth2.0)