Personal Digital Agent Protocol (pdap)

HotRFC
November 5, 2023

pdap@ietf.org
Enabling a shift from proprietary platforms to personal agents

- Replace forced platform association with one’s choice of community.
- My agent is interoperable by vendors and service providers.
- I can switch the host of my agent anytime. No lock-in.
- My agent’s policies are portable across host communities.
  - Swarm and federated personal AI agents can be supported.
Foundational Principle

Universal Human Right of Freedom of Association and Assembly

- Individual choice of hosting and support communities for one’s digital agent.
- Self-hosting is supported for those that have the skill and interest.
Platform Issues and Regulatory Responses

● **US: FTC vs. Amazon**
  ○ Bundling of Search and Logistics - drives up cost for vendors
  ○ Most-favored-pricing clauses drive up cost for customers

● **EU: Payment Services Directive PSD-2**
  ○ Opens interface between payment services and banks
  ○ Increased competition for both payment services and banks

● **EU: Digital Services Act**
  ○ Customer lock-in and lack of transparency and customer agency
  ○ Very Large Online Platforms (VLOP) and Very Large Online Search Engines (VLOSE)

● **India: Aadhaar, UPI, India Stack, beckn protocol**
  ○ Avoid US / EU style platform oligopolies
  ○ Support essential digital tools as a public good (Aadhaar, India Stack)
  ○ Enable customers and vendors to choose their agents (UPI, beckn protocol)
Personal Digital Agent

- Self-Sovereign (independent of any jurisdiction or federation)
- Community-Hosted (self-hosted option for pure self-sovereignty)
- Semi-autonomous
- Intelligent (adaptable, learning, context-aware, conversational)
- General across all types of vendors, service providers and jurisdictions
- Accepted by most service providers and resource servers
  - Standardized
  - Fair
  - Cost-effective
  - Secure
Scope of a Personal Digital Agent Protocol

● Separate choice of Authorization Server (as agent) from Resource Server (as vendor)
  ○ IETF GNAP - **Last Call** - multiple implementations available

● Standardize Request Presentation and Authorization Tokens
  ○ Authorization and Revocation Capabilities - TBD - Consider [https://github.com/ucan-wg/spec](https://github.com/ucan-wg/spec)

● Standardize the Service Endpoint for a personal digital agent Authorization Server
  ○ Support both URIs and DIDs

● Scope of the Authorization Server Policy Management Interface
  ○ TBD - Consider CEDAR [https://www.cedarpolicy.com/en](https://www.cedarpolicy.com/en)
A-Chooses Host Community

B-Updates Policies

C-Registers Agent Address

Owner

Policies

Agent

Requesting Party Client

Resource Server

GNAP

1>Request

2<Token

3>Token

4<Resource
Steps toward a Personal Digital Agent Standard

● 2015-on: Kantara UMA 2 Protocol Standard
  ○ OAuth-based
  ○ “Open World” Authorization Server
● 2020-on: IETF GNAP Protocol Standard
  ○ Not OAuth-based
  ○ Open world user request state machine
● 2022: W3C Verifiable Credentials Data Model Standard
  ○ Validation and Verification as a commodity service
  ○ Supports open world, decentralized, and self-sovereign flows
● 2023: Personal Digital Agent Discussion Group
  ○ Define the scope of a vendor standard for interoperable personal agents
  ○ Excellent vendor and customer experience without platform lock-in
  ○ https://docs.google.com/document/d/19GU6L1QxaVslfrom9iBKq9T2qV9y0zttRmtnQuPireMMU/edit
● 2024: IETF Standard Workgroup Established
Join our mail list

https://www.ietf.org/mailman/listinfo/pdap

These slides and older notes at:

https://docs.google.com/document/d/19GU6L1QxaVslfm9iBKg9T2qV9y0zttRmtlQuPireMMU/edit

Suggest vendors and implementers to participate.

agropper@healthurl.com

Thank you.