Technology and Implementation Challenges Behind Decentralized Identity

Kristina Yasuda, Microsoft

Decentralized Identity is expected to provide users with more privacy and control over their identity. In this presentation, use-cases, technical building blocks, sample architecture, and implementation challenges including interoperability and trust frameworks will be discussed. Two main components of decentralized identity are Decentralized Identifiers (DIDs) and Verifiable Credentials (VCs) standardized in W3C. Since DIDs and VCs are data models, another important component is a transport protocol such as Self-Issued OpenID Provider (SIOP) being standardized in OpenID Foundation, or QR codes. Concrete use-cases and implementation challenges of decentralized identity will be examined, as a sample using architecture of Microsoft's decentralized identity service, which is built using ION DID method, JWT-based VCs and SIOP. Two major challenges to achieve a trusted, larger-scale adoption of decentralized identity are 1/ interoperability between two credential formats of JSON and JSON-LD and two main signature formats of JWT and LD-proofs, and 2/ establishment of trusted frameworks that define how trust among stakeholders is established and audited.